IMPLEMENTASI HYBRID MACHINE LEARNING IDPS MENGGUNAKAN ALGORITMA RANDOM FOREST UNTUK DETEKSI SERANGAN PORT SCANNING

Zehra Alfarizi, Sugiyatno*
Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer El Rahma Yogyakarta
Jalan Sisingamangaraja No.76, Brotokusuman, Kec. Mergangsan, Kota Yogyakarta, D.I.Yogyakarta 55671
enoyat@gmail.com

ABSTRAK

Keamanan jaringan komputer terus menghadapi berbagai ancaman, salah satunya aktivitas *port scanning* yang sering digunakan sebagai tahap awal sebelum serangan lanjutan. Permasalahan yang terjadi pada sistem keamanan konvensional adalah keterbatasan dalam mendeteksi serangan secara akurat serta lambatnya proses mitigasi terhadap serangan yang berlangsung secara *real-time*. Penelitian ini bertujuan untuk mengembangkan sistem *Hybrid Intrusion Detection and Prevention System* (IDPS) yang mampu mendeteksi sekaligus melakukan tindakan pencegahan secara otomatis. Metode yang digunakan meliputi proses *preprocessing* dataset CIC-IDS2017, pembangunan model Random Forest sebagai metode klasifikasi, serta integrasi *rule-based logic* untuk validasi dan pemblokiran IP. Hasil pengujian menunjukkan bahwa sistem mampu mencapai akurasi sebesar 99,60% dengan nilai *precision* dan *recall* sebesar 0,98 pada kelas *malicious*, serta mampu merespons serangan dengan cepat melalui mekanisme pemblokiran otomatis.

Kata Kunci: *IDPS, CIC-IDS2017, Random Forest, Hybrid Logic, Port Scanning.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah meningkatkan ketergantungan berbagai institusi terhadap sistem jaringan komputer dalam mendukung aktivitas operasional sehari-hari. Seiring dengan meningkatnya penggunaan teknologi tersebut, ancaman terhadap keamanan jaringan juga terus berkembang, salah satunya melalui aktivitas *Port Scanning* yang umum digunakan sebagai tahap awal dalam proses pengintaian sebelum dilakukan serangan lanjutan[1]. Aktivitas ini dapat dimanfaatkan oleh penyerang untuk memperoleh informasi mengenai port dan layanan yang aktif pada suatu server sebelum melakukan eksploitasi lebih lanjut.

Namun, sistem keamanan konvensional yang masih mengandalkan metode deteksi berbasis tanda tangan (signature-based) memiliki keterbatasan dalam mengenali pola serangan baru yang belum terdaftar pada basis data ancaman [2], sehingga kurang efektif dalam menghadapi perkembangan teknik serangan yang semakin dinamis. Selain itu, beberapa penelitian sebelumnya masih berfokus pada proses deteksi serangan tanpa mengintegrasikan mekanisme mitigasi otomatis secara langsung setelah ancaman teridentifikasi, sehingga proses penanganan masih memerlukan intervensi administrator secara manual.

Dalam penelitian ini, pemanfaatan dataset CIC-IDS2017 digunakan karena mampu menyajikan profil lalu lintas jaringan yang lebih representatif dan aktual dibandingkan dataset historis seperti KDD'99 atau NSL-KDD [3]. Algoritma Random Forest dipilih karena mampu mengolah data dengan banyak fitur dan memiliki performa klasifikasi yang stabil melalui pendekatan *ensemble learning* [4]. Oleh karena itu, penelitian ini mengusulkan implementasi *Hybrid Intrusion Detection and Prevention System* (IDPS) dengan mengintegrasikan Random Forest dan *Rule-Based Logic* untuk mendeteksi serta melakukan mitigasi otomatis terhadap serangan *Port Scanning* secara *real-time*.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk membangun sistem keamanan jaringan yang mampu mendeteksi sekaligus menangani aktivitas serangan secara otomatis dalam kondisi *real-time*. Sistem yang dikembangkan menggabungkan algoritma Random Forest sebagai metode klasifikasi dengan *rule-based logic* untuk memastikan karakteristik serangan sebelum dilakukan tindakan pemblokiran. Dengan pendekatan ini, diharapkan proses deteksi dan penanganan serangan dapat berjalan lebih cepat tanpa bergantung pada intervensi manual dari administrator.

2. TINJAUAN PUSTAKA

2.1. Intrusion Detection and Prevention System (IDPS)

Intrusion Detection and Prevention System (IDPS) merupakan sistem keamanan jaringan yang berfungsi untuk memantau lalu lintas data dan mendeteksi aktivitas mencurigakan yang berpotensi mengancam keamanan jaringan [2]. Berbeda dengan Intrusion Detection System (IDS) yang hanya melakukan deteksi, IDPS memiliki kemampuan untuk memberikan respons secara otomatis ketika serangan teridentifikasi, seperti memutus koneksi atau memblokir alamat IP penyerang [5]. Dengan adanya mekanisme tersebut, IDPS dapat membantu mengurangi risiko kerusakan sistem sebelum serangan berkembang lebih lanjut.

Efektivitas IDPS dalam mendeteksi ancaman sangat dipengaruhi oleh metode deteksi yang digunakan. Salah satu pendekatan yang banyak

diterapkan adalah metode berbasis anomali (*anomaly-based)*, yaitu teknik yang memanfaatkan model machine learning untuk mempelajari pola trafik normal dan mengenali aktivitas yang menyimpang dari pola tersebut [6]. Pendekatan ini memungkinkan sistem mendeteksi serangan baru atau serangan yang belum terdaftar dalam basis data ancaman. Dalam implementasinya, IDPS umumnya dikombinasikan dengan mekanisme firewall atau pemblokiran otomatis agar sistem tidak hanya mampu mendeteksi, tetapi juga dapat melakukan tindakan pencegahan secara *real-time*.

2.2. Random Forest dalam Deteksi Serangan Jaringan

Random Forest merupakan algoritma Machine Learning berbasis *ensemble learning* yang menggabungkan banyak decision tree untuk menghasilkan prediksi yang lebih stabil dan akurat. Setiap pohon keputusan dibangun menggunakan subset data dan fitur yang dipilih secara acak, sehingga mengurangi risiko overfitting yang sering terjadi pada single decision tree [4]. Dalam bidang keamanan jaringan, Random Forest banyak digunakan karena mampu menangani dataset berdimensi tinggi dengan jumlah fitur yang besar, seperti pada dataset *CIC-IDS2017* yang memiliki banyak fitur [7]. Selain itu, algoritma ini memiliki performa yang baik dalam menangani data yang bersifat non-linear dan kompleks [6].

Beberapa penelitian sebelumnya menunjukkan bahwa algoritma Random Forest memiliki performa yang baik dalam mendeteksi serangan jaringan. Wang dan Avrianto [1] melaporkan bahwa pendekatan hybrid yang menggabungkan Random Forest dengan metode lain mampu meningkatkan akurasi deteksi intrusi secara signifikan. Selain itu, pendekatan berbasis *anomaly-based* juga dinilai efektif dalam mengenali pola serangan baru yang belum terdapat dalam basis data ancaman [6].

Namun, sebagian besar penelitian tersebut masih berfokus pada proses deteksi tanpa disertai mekanisme mitigasi otomatis setelah serangan teridentifikasi. Hal ini menyebabkan sistem masih memerlukan intervensi manual dalam menangani ancaman yang terjadi. Oleh karena itu, penelitian ini mengusulkan pendekatan hybrid dengan mengintegrasikan Random Forest dan *rule-based logic* untuk meningkatkan efektivitas deteksi sekaligus memungkinkan tindakan pencegahan secara otomatis dalam kondisi *real-time*.

2.3. Dataset CIC-IDS2017

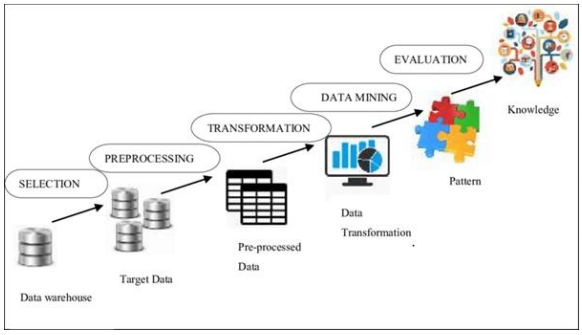
Dataset *CIC-IDS2017* dikembangkan oleh Canadian Institute for Cybersecurity (CIC) sebagai dataset evaluasi IDS yang lebih representatif terhadap kondisi jaringan modern. Dataset ini dirancang untuk mengatasi keterbatasan dataset lama seperti KDD'99 dan NSL-KDD yang dianggap sudah tidak relevan dengan pola serangan terkini . *CIC-IDS2017* mencakup berbagai jenis serangan seperti *DDoS, Brute Force, Port Scanning, Botnet, dan Web Attack*, serta menyediakan fitur statistik jaringan yang diekstraksi menggunakan CICFlowMeter [8]. Keunggulan dataset ini terletak pada keberagaman skenario serangan dan representasi trafik normal yang realistis. Penggunaan dataset ini dalam penelitian bertujuan untuk memastikan bahwa model yang dikembangkan mampu beradaptasi dengan pola serangan yang lebih kompleks dan aktual.

2.4. Rule-Based Logic dalam Sistem Hybrid

Rule-based logic merupakan pendekatan berbasis aturan deterministik yang digunakan untuk mengidentifikasi pola tertentu berdasarkan parameter yang telah ditentukan sebelumnya. Dalam sistem keamanan jaringan, *Rule-Based logic* sering digunakan untuk mendeteksi pola spesifik seperti lonjakan koneksi dalam waktu singkat atau percobaan login berulang. Pendekatan ini memiliki keunggulan dalam hal kecepatan eksekusi dan transparansi keputusan karena setiap tindakan didasarkan pada aturan yang jelas[9]. Namun, rule-based memiliki keterbatasan dalam mendeteksi pola serangan baru yang belum didefinisikan dalam aturan .

Pada penelitian ini, *Rule-Based logic* digunakan sebagai tahap validasi setelah proses klasifikasi dilakukan oleh model Random Forest. Pendekatan ini diterapkan agar sistem tidak hanya mampu mendeteksi anomali, tetapi juga dapat memastikan karakteristik serangan sebelum melakukan tindakan mitigasi secara otomatis. Dengan demikian, kombinasi antara Random Forest dan *Rule-Based logic* diharapkan dapat meningkatkan akurasi deteksi serta menjaga efektivitas proses mitigasi pada sistem keamanan jaringan.

3. METODE PENELITIAN



Gambar 1. Tahapan *Knowledge Discovery in Database* (KDD)

Metode yang digunakan dalam penelitian ini adalah *Knowledge Discovery in Database* (KDD), yaitu pendekatan yang digunakan untuk menggali informasi dari kumpulan data melalui beberapa tahapan pengolahan secara sistematis. Pada penelitian ini, metode KDD diterapkan untuk mengolah data trafik jaringan sehingga diperoleh pola yang dapat digunakan dalam membedakan aktivitas normal dan aktivitas serangan *Port Scanning*, Hasil dari proses

tersebut kemudian digunakan sebagai dasar dalam pengembangan sistem deteksi dan mitigasi ancaman secara otomatis. Tahapan dalam metode KDD terdiri atas *data selection*, *preprocessing*, *transformation*, *data mining*, dan *evaluation* [10]. Adapun alur tahapan metode KDD pada penelitian ini ditunjukkan pada Gambar 1.

3.1. Data Selection

Tahap awal dalam metode KDD adalah proses seleksi data, yaitu memilih data yang relevan untuk digunakan dalam penelitian. Pada penelitian ini, data yang digunakan berasal dari dataset *CIC-IDS2017* dengan fokus pada trafik normal (*benign*) dan trafik serangan *Port Scanning*. Pemilihan kategori data tersebut dilakukan untuk menyesuaikan dengan tujuan penelitian, yaitu membangun model klasifikasi yang mampu membedakan trafik normal dan aktivitas serangan pemindaian port.

3.2. Preprocessing

Pembersihan data bertujuan untuk menyingkirkan record yang tidak valid, seperti data kosong atau nilai tak terhingga (*infinity*) pada durasi trafik. Langkah ini juga mencakup eliminasi fitur-fitur yang tidak memberikan pengaruh besar terhadap hasil klasifikasi akhir. Melalui proses ini, kualitas data yang digunakan dalam pelatihan model dapat terjaga sehingga algoritma Random Forest mampu melakukan klasifikasi secara lebih optimal tanpa dipengaruhi oleh data yang tidak valid.

3.3. Transformation

Transformasi dilakukan untuk menyesuaikan format data agar dapat diproses oleh sistem. Pada tahap ini, data kategorikal diubah ke dalam bentuk numerik melalui proses *encoding* sehingga dapat dikenali oleh model *machine learning*. Selain itu, dilakukan pula normalisasi data dan pemilihan fitur (*feature selection*) terhadap atribut yang dianggap paling relevan, seperti *Destination Port* dan *Packet Length*, guna meningkatkan efektivitas model dalam mendeteksi pola serangan jaringan.

3.4. Data Mining

Dataset yang telah melalui proses preprocessing dibagi menjadi data latih dan data uji menggunakan metode train-test split dengan komposisi 70% data training dan 30% data testing. Data training digunakan untuk melatih model agar mampu mengenali pola trafik normal maupun trafik serangan, sedangkan data testing digunakan untuk menguji kemampuan model terhadap data yang belum pernah diproses sebelumnya. Pembagian data tersebut dilakukan agar hasil pengujian dapat memberikan gambaran performa model secara lebih objektif terhadap data baru.

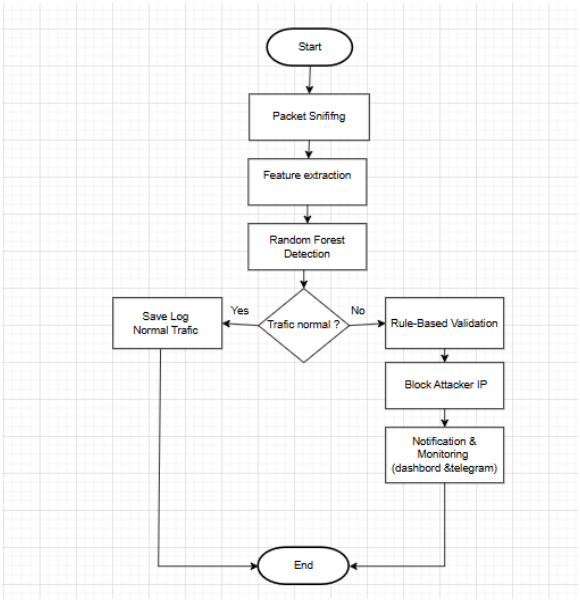
$$\hat{y}(x) = mode\{T_{b(x)}\}_{b=1}^{B} \quad (1)$$

Rumus tersebut menjelaskan bahwa hasil klasifikasi Random Forest diambil dari prediksi yang paling sering muncul dari seluruh pohon keputusan yang terbentuk. Cara kerja ini membuat hasil keputusan model lebih stabil dibandingkan jika hanya menggunakan satu pohon keputusan. Pada penelitian ini, model dibangun menggunakan algoritma Random Forest dengan jumlah estimator sebanyak 100 *decision tree*. Nilai *random state* ditetapkan sebesar 42 agar proses pelatihan tetap menghasilkan keluaran yang konsisten pada setiap pengujian. Setelah model selesai dilatih, pengujian dilakukan menggunakan data testing untuk memperoleh nilai *Accuracy*, *Precision*, *Recall*, *dan F1-score* sebagai ukuran kemampuan model dalam membedakan trafik normal dan trafik serangan.

3.5. Evaluation

Tahap evaluasi dilakukan untuk mengukur performa model menggunakan parameter Confusion Matrix. Melalui metode ini diperoleh nilai akurasi, precision, recall, dan F1-score sebagai indikator kemampuan model dalam melakukan klasifikasi trafik jaringan. Selain evaluasi statistik, sistem juga diuji melalui simulasi serangan secara langsung untuk mengukur kecepatan mitigasi, efektivitas mekanisme pemblokiran IP, serta keberhasilan pengiriman notifikasi melalui Telegram Bot API secara *real-time*.

3.6. Desain Sistem



Gambar 2. Flowchart Arsitektur Sistem Hybrid IDPS

Penelitian ini dilakukan dengan merancang sistem Hybrid Intrusion Detection and Prevention System (IDPS) yang mengintegrasikan algoritma Random Forest dengan mekanisme *rule-based validation* untuk mendeteksi aktivitas serangan *Port Scanning* pada jaringan secara *real-time*. Konsep hybrid pada sistem ini diterapkan dengan memanfaatkan Random Forest untuk melakukan klasifikasi awal terhadap trafik jaringan, kemudian hasil deteksi tersebut dilanjutkan ke proses validasi menggunakan *Rule-Based Logic* sebelum sistem melakukan tindakan mitigasi secara otomatis. Sistem

dirancang untuk melakukan monitoring trafik jaringan, analisis pola trafik, serta tindakan pencegahan terhadap ancaman yang berhasil terdeteksi.

Gambar 2 menunjukkan flowchart arsitektur sistem Hybrid IDPS yang dibangun pada penelitian ini. Proses sistem diawali dengan *packet sniffing* menggunakan library Scapy untuk menangkap paket jaringan TCP secara *real-time*. Paket yang berhasil ditangkap kemudian diproses melalui tahap *feature extraction* untuk memperoleh parameter yang dibutuhkan dalam proses deteksi, seperti *source IP*, *destination port*, jumlah *request*, dan jumlah port unik yang diakses.

Data hasil ekstraksi selanjutnya dianalisis menggunakan model Random Forest untuk mengidentifikasi apakah trafik jaringan termasuk kategori normal atau anomali. Apabila trafik teridentifikasi normal, maka aktivitas akan dicatat ke dalam log monitoring sistem. Namun apabila model mendeteksi adanya trafik abnormal, maka proses akan dilanjutkan ke tahap *rule-based validation* guna memastikan pola trafik sesuai dengan karakteristik aktivitas *Port Scanning*.

Jika aktivitas Port Scanning berhasil diidentifikasi, sistem akan secara otomatis melakukan tindakan prevention berupa pemblokiran alamat IP penyerang. Selain itu, sistem juga mengirimkan notifikasi peringatan kepada administrator melalui Telegram Bot API dan menampilkan hasil deteksi ke dashboard monitoring berbasis web guna mempermudah proses pengawasan keamanan jaringan.

4. HASIL DAN PEMBAHASAN

4.1. Evaluasi Performa Model

Evaluasi performa model dilakukan menggunakan data testing yang telah dipisahkan dari data training pada tahap sebelumnya. Pengujian ini bertujuan untuk melihat kemampuan model Random Forest dalam mengklasifikasikan trafik jaringan normal dan trafik serangan pada data yang belum pernah digunakan saat pelatihan. Penilaian model menggunakan metrik *accuracy, precision, recall,* dan *F1-score* berdasarkan *confusion matrix*. Dari hasil pengujian, model memperoleh akurasi sebesar 99,60%.

Tabel 1. Evaluasi Performa Model

Kategori	Precision	Recall	F1-Score	Support
Normal	1,00	1,00	1,00	2688
Attack	0,98	0,98	0,98	312
Accuracy			99,60%	3000

Nilai akurasi sebesar 99,60% menunjukkan bahwa model mampu membedakan trafik normal dan trafik serangan dengan sangat baik. Hasil ini dipengaruhi oleh kemampuan Random Forest dalam membaca pola data yang cukup kompleks serta menggabungkan banyak decision tree untuk menekan kesalahan klasifikasi. Selain itu, dataset CIC-IDS2017 yang memiliki variasi trafik turut membantu model mempelajari karakteristik data secara lebih baik.

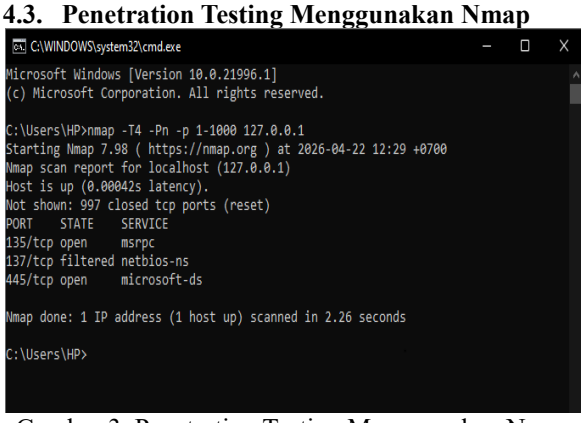
Nilai precision dan recall sebesar 0,98 pada kelas attack menunjukkan bahwa sebagian besar aktivitas serangan berhasil dikenali dengan baik dan kesalahan deteksi terhadap trafik normal tergolong rendah. Hal tersebut menunjukkan bahwa model cukup layak digunakan dalam proses deteksi ancaman jaringan secara real-time. Jika dibandingkan dengan penelitian sebelumnya yang memperoleh akurasi 99,76%[1], Hasil pada penelitian ini masih berada pada tingkat performa yang kompetitif.

4.2. Implementasi Real-Time dan Mitigasi

Pengujian sistem dilakukan untuk mengukur kemampuan deteksi dan respons terhadap serangan secara real-time. Waktu respons dihitung sebagai selisih antara waktu deteksi (T_detect) dan waktu tindakan mitigasi (T_block). Pengujian dilakukan beberapa kali menggunakan skenario serangan yang sama, kemudian diambil nilai rata-rata. Berdasarkan hasil pengujian, diperoleh rata-rata waktu respons sebesar 0,72 detik, yang menunjukkan bahwa sistem mampu merespons serangan dengan cepat melalui mekanisme pemrosesan berbasis memori.

Sistem menerapkan mekanisme *prevention* berupa *logical blocking*, yaitu dengan memasukkan alamat IP penyerang ke dalam daftar blacklist. Setelah IP terblokir, sistem tidak lagi memproses trafik dari IP tersebut sehingga tidak menghasilkan notifikasi ulang pada dashboard maupun Telegram. Meskipun demikian, proses scanning masih dapat dilakukan karena pemblokiran tidak dilakukan pada level firewall sistem operasi, melainkan pada level aplikasi. Pendekatan ini membantu menghindari duplikasi alert sekaligus meningkatkan efisiensi sistem dalam menangani aktivitas serangan.

4.3. Penetration Testing Menggunakan Nmap



Gambar 3. Penetration Testing Menggunakan Nmap melalui Command Prompt

Pengujian penetration testing dilakukan untuk melihat kemampuan sistem dalam mengenali aktivitas pemindaian port pada jaringan. Pada penelitian ini, simulasi serangan menggunakan tools Nmap yang dijalankan dari sisi attacker menuju server target melalui command prompt. Metode tersebut digunakan

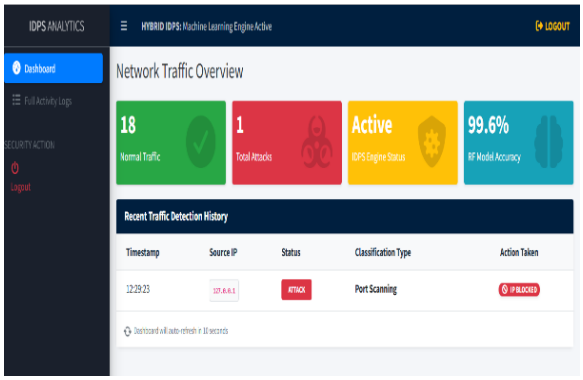
untuk menggambarkan proses reconnaissance, yaitu upaya awal yang umumnya dilakukan penyerang untuk mengetahui port terbuka dan layanan yang aktif pada server.

Dari hasil pengujian, simulasi serangan dilakukan menggunakan perintah nmap -T4 -Pn -p 1-1000 127.0.0.1 untuk melakukan pemindaian terhadap sejumlah port pada server target. Aktivitas tersebut menghasilkan pola akses ke banyak port dalam waktu singkat sehingga dikenali sistem sebagai trafik tidak normal. Setelah scanning terdeteksi, alamat IP sumber secara otomatis dimasukkan ke dalam daftar blokir sementara yang tersimpan pada memori sistem. Hasil ini menunjukkan bahwa mekanisme deteksi dan mitigasi dapat berjalan sesuai rancangan sistem.

4.4. Dashboard Monitoring Real-Time

Untuk membantu proses pemantauan keamanan jaringan, sistem yang dibuat dilengkapi dashboard monitoring berbasis web menggunakan framework Flask. Dashboard menampilkan kondisi trafik jaringan secara real-time berdasarkan hasil klasifikasi model Random Forest, seperti jumlah trafik yang diproses, trafik normal (*benign*), trafik serangan (*malicious*), serta riwayat pemblokiran alamat IP. Tampilan ini memudahkan administrator melihat kondisi jaringan secara langsung tanpa harus memeriksa log secara manual.

Selain sebagai sarana pemantauan, dashboard juga dapat digunakan untuk melihat pola aktivitas serangan pada periode tertentu. Informasi tersebut berguna bagi administrator saat melakukan analisis insiden maupun menentukan tindak lanjut terhadap ancaman yang muncul.



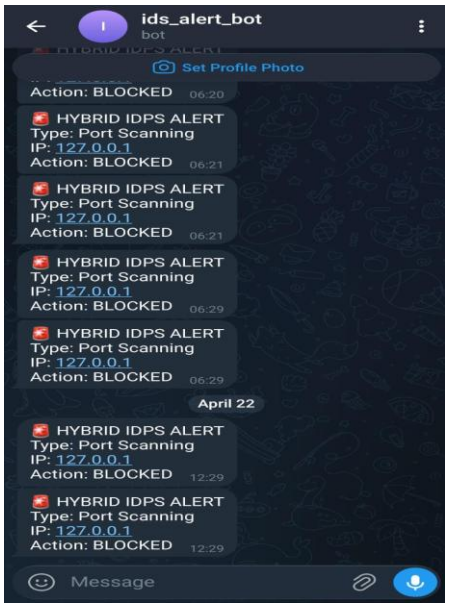
Gambar 4. Tampilan Dashboard Monitoring IDPS Secara Real-Time

Berdasarkan hasil pengujian, dashboard menampilkan satu aktivitas serangan yang dikenali sebagai Port Scanning dengan status tindakan IP Blocked. Rata-rata waktu respons sistem dari proses deteksi hingga mitigasi tercatat sebesar 0,72 detik. Selama pengujian berlangsung, pembaruan data pada dashboard berjalan stabil tanpa memberikan beban yang berarti pada server. Hal ini menunjukkan bahwa sistem monitoring dapat digunakan dengan baik untuk mendukung pengawasan jaringan secara *real-time.*

4.5. Notifikasi Serangan Melalui Telegram

Selain dashboard monitoring, sistem yang dikembangkan juga dilengkapi fitur notifikasi instan melalui Telegram Bot API untuk menyampaikan informasi serangan secara langsung kepada administrator. Fitur ini memudahkan administrator memperoleh pemberitahuan tanpa harus memantau dashboard secara terus-menerus. Ketika model Random Forest mengklasifikasikan trafik sebagai *malicious* dan proses *Rule-Based Logic* mengenali jenis serangan, sistem akan mengirimkan pesan otomatis yang berisi jenis serangan, alamat IP sumber, serta status tindakan mitigasi.

Integrasi notifikasi ini membantu mempercepat respons administrator karena informasi ancaman dapat diterima langsung melalui perangkat seluler. Dengan demikian, proses analisis maupun tindak lanjut terhadap insiden keamanan dapat dilakukan lebih cepat dibandingkan sistem yang hanya menyimpan log tanpa pemberitahuan otomatis.



Gambar 5. Notifikasi Otomatis Serangan Melalui Telegram

Berdasarkan hasil pengujian, notifikasi Telegram berhasil menampilkan informasi serangan berupa *Port Scanning* yang berasal dari alamat IP 127.0.0.1 dengan status tindakan *BLOCKED*. Pesan peringatan diterima sesaat setelah proses deteksi berlangsung, sehingga administrator dapat segera mengetahui adanya ancaman pada jaringan. Hasil tersebut menunjukkan bahwa sistem tidak hanya mampu melakukan deteksi dan mitigasi otomatis, tetapi juga dapat menyampaikan informasi serangan secara cepat dan praktis kepada administrator jaringan.

4.6. Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh komponen yang dikembangkan dapat berjalan sesuai dengan fungsinya. Pengujian mencakup proses deteksi serangan menggunakan

model Random Forest, validasi menggunakan rule-based logic, serta mekanisme pemblokiran IP secara otomatis. Selain itu, pengujian juga dilakukan pada fitur monitoring melalui dashboard dan pengiriman notifikasi menggunakan Telegram.

Berdasarkan hasil pengujian yang telah ditunjukkan pada Gambar 3, Gambar 4, dan Gambar 5, sistem mampu mendeteksi aktivitas port scanning dan memberikan respons berupa pemblokiran IP secara otomatis dengan menyimpan alamat IP penyerang ke dalam memori (RAM) sebagai daftar blokir sementara. Informasi serangan juga dapat ditampilkan pada dashboard serta dikirimkan melalui notifikasi Telegram dengan baik. Selain itu, hasil evaluasi model pada Tabel 1 menunjukkan bahwa sistem memiliki tingkat akurasi yang tinggi dalam mengklasifikasikan trafik jaringan. Hal ini menunjukkan bahwa sistem yang dikembangkan dapat bekerja secara terintegrasi dan mampu mendukung proses keamanan jaringan secara efektif.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa sistem *Hybrid Intrusion Detection* and *Prevention System* (IDPS) berbasis Random Forest dan *Rule-Based Logic* mampu mendeteksi serta menangani ancaman jaringan secara efektif pada kondisi *real-time*. Sistem yang dikembangkan memperoleh tingkat akurasi sebesar 99,60% dengan nilai precision dan recall sebesar 0,98 pada kategori malicious, sehingga mampu membedakan trafik normal dan trafik serangan dengan baik. Selain itu, sistem dapat mengidentifikasi aktivitas serangan seperti *Port Scanning* dan melakukan mitigasi otomatis dengan menyimpan alamat IP penyerang ke dalam memori (RAM) sebagai daftar blokir sementara, dengan rata-rata waktu respons sebesar 0,72 detik. Fitur dashboard monitoring dan notifikasi Telegram juga mendukung proses pemantauan jaringan secara *real-time*. Mekanisme pemblokiran yang diterapkan dalam penelitian ini masih berada pada level aplikasi (*logical blocking*) dan belum terintegrasi dengan firewall sistem operasi. Secara keseluruhan, sistem menunjukkan performa yang baik dalam proses deteksi dan mitigasi, meskipun masih memiliki keterbatasan karena hanya difokuskan pada deteksi *Port Scanning* dengan pendekatan klasifikasi biner. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan sistem ke arah klasifikasi multi-class, penerapan pemblokiran pada level firewall, serta pengujian pada lingkungan jaringan yang lebih kompleks.

DAFTAR PUSTAKA

[1] R. C. Wang and R. P. Avrianto, "Improving Detection Accuracy of Network Intrusions Using a Hybrid Network Intrusion Detection System Based on Isolation Forest and Random Forest Algorithms," *JUTIF*, vol. 6, no. 6, pp. 5371–5385, 2025.

[2] T. H. Hai, N. T. Khiem, and N. H. Phuc, "Toward an Online DoS/DDoS Classification: An Empirical Study for Network Intrusion Detection Systems," *Journal of Computer Science*, vol. 17, no. 3, pp. 304–318, 2021, doi: 10.3844/JCSSP.2021.304.318.

[3] G. Pradita and A. Pramono, "Implementasi Monitoring Keamanan Jaringan Pada Server Ubuntu Menggunakan Snort Intrusion Detection Prevention System (IDPS) dan Telegram Bot Sebagai Media Notifikasi Di PT SS UTAMA," *Jurnal Mahasiswa Teknik Informatika*, vol. 8, no. 4, 2024.

[4] T. Agustina, M. Masrizal, and I. Irmayanti, "Performance Analysis of Random Forest Algorithm for Network Anomaly Detection using Feature Selection," *Sinkron*, vol. 8, no. 2, Apr. 2024.

[5] T. Purnama *et al.*, "Implementasi Intrusion Detection System (IDS) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp dan telegram Sebagai Media Notifikasi," vol. 14, no. 2, pp. 358–369, 2023, [Online]. Available: http://ejurnal.provisi.ac.id/index.php/JTIKPpage 358

[6] M. Mujiono, D. A. Larasati, M. Hemansyah, and F. Fatimatuzzahra, "Deteksi Anomali dalam Sistem Keamanan Jaringan Menggunakan Teknik Supervised Machine Learning," *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi dan Sistem Komputer*, vol. 9, no. 1, pp. 65–69, May 2025, doi: 10.55886/infokom.v9i1.971.

[7] K. Inayah, K. Ramli, and P. Korespondensi, "Analisis Kinerja Intrusion Detection System Berbasis Algoritma Random Forest Menggunakan Dataset Unbalanced Honeynet," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK),* vol. 9, no. 3, pp. 573-582, 2022, doi: 10.25126/jtiik1148911.

[8] M. Arief Rachmatullah, A. Subagja Firdaus, N. Afaf Ekayana, F. Al-hilal Saepul Bahri, and M. Zauzi, "Analisis Efektivitas Intrusion Detection System (IDS) Untuk Serangan DDOS Menggunakan Komparasi Random Forest dan Decision Tree," *Jurnal Mahasiswa Teknik Informatika*, vol. 10, no. 1, 2026.

[9] H. Setiawan, M. Agus Munandar, and L. W. Astuti, "Penggunaan Metode Signatured Based Dalam Pengenalan Pola Serangan di Jaringan Komputer," vol. 8, no. 3, pp. 517–524, 2021, doi: 10.25126/jtiik.202184200.

[10] K. Gustipartsani, N. Rahaningsih, R. D. Dana, and I. Y. Mustafa, "Data Mining Clustering Menggunakan Algoritma K-MEANS Pada Data Kunjungan Wisatawan di Kabupaten Karawang," *Jurnal Mahasiswa Teknik Informatika*, vol. 7, no. 6, 2023