Network Intrusion Detection System Using Convolutional Neural Network And Random Forests Classifiers

SISTEM DETEKSI INTRUSI JARINGAN MENGGUNAKAN JARINGAN SYARAF TIRUAN DAN PENGKLASIFIKASI HUTAN ACAK

Viky Luffiandi Rismawan[1], Elkaf Rahmawan Pramudya[2]
[1,2]Universitas Dian Nuswantoro, Jl. Imam Bonjol No.207, Semarang
vikyrismawan26@gmail.com[1], elkaf.rahmawan@dsn.dinus.ac.id[2],

Abstract *- Network Intrusion Detection Systems (NIDS) play a crucial role in protecting networks from various forms of cyberattacks. However, conventional signature-based methods often fail to detect new or unknown threats and are prone to generating high false positive rates. This study proposes a hybrid approach combining Convolutional Neural Network (CNN) and Random Forest (RF) to develop a more adaptive and accurate intrusion detection system. CNN is employed to extract features from raw network traffic data, while RF serves as the primary classifier. The UNSW-NB15 dataset is used for training and testing the model. Evaluation results show that the hybrid model achieves an accuracy of 93.0%, average precision of 94%, recall of 90%, F1-score of 92%, and a false positive rate of 19.2%. These results demonstrate that the CNN–RF hybrid approach effectively improves intrusion detection performance and offers a promising solution for modern network security systems.*

Keywords *- CNN, cyber security ensemble method, network intrusion detection system, random forest.*

Abstrak - Sistem deteksi intrusi jaringan (Network Intrusion Detection System/NIDS) berperan penting dalam menjaga keamanan jaringan dari berbagai serangan siber. Namun, metode konvensional berbasis signature memiliki keterbatasan dalam mendeteksi serangan baru dan rentan menghasilkan tingkat false positive yang tinggi. Penelitian ini mengusulkan pendekatan hybrid dengan menggabungkan *Convolutional Neural Network* (CNN) dan *Random Forest* (RF) untuk membangun sistem deteksi intrusi yang lebih adaptif dan akurat. CNN digunakan untuk mengekstraksi fitur dari data mentah lalu lintas jaringan, sementara RF digunakan sebagai pengklasifikasi utama. Dataset UNSW-NB15 digunakan untuk pelatihan dan pengujian model. Hasil evaluasi menunjukkan bahwa model hybrid ini mampu mencapai akurasi sebesar 93,0%, precision rata-rata 94%, recall 90%, F1-score 92%, serta *false positive rate* sebesar 19,2%. Hasil ini menunjukkan bahwa pendekatan hybrid CNN–RF efektif dalam meningkatkan performa deteksi intrusi dan dapat menjadi solusi yang menjanjikan dalam sistem keamanan jaringan modern.

Kata Kunci - *CNN, keamanan siber, metode ensemble, random forest, sistem deteksi intrusi jaringan*.

I. PENDAHULUAN

Di era modern saat ini, jaringan komputer memainkan peran vital dalam mendukung kemudahan pertukaran data antar perangkat. Namun, proses ini tidak terlepas dari potensi ancaman, khususnya dalam aspek keamanan informasi. Untuk meminimalkan risiko tersebut, implementasi sistem keamanan siber menjadi sangat krusial. Keamanan siber mencakup seperangkat strategi dan teknologi yang dirancang untuk melindungi infrastruktur jaringan dari serangan yang bersifat merusak maupun tidak dikenal, seperti melalui pemanfaatan perangkat lunak antivirus, firewall, serta berbagai metode perlindungan lainnya[1]. Seiring dengan pesatnya transformasi digital, keamanan jaringan tidak hanya menjadi kebutuhan mendasar, tetapi juga tantangan utama dalam menjaga integritas dan kerahasiaan sistem informasi dari akses ilegal dan aktivitas berbahaya [2].

Salah satu upaya mitigasi terhadap ancaman ini adalah penerapan *Network Intrusion Detection System* (NIDS), yang bertugas memantau lalu lintas jaringan dan mendeteksi aktivitas mencurigakan secara real-time [3]. Sistem deteksi intrusi konvensional umumnya berbasis signature (*signature-based detection*), yang mengandalkan pola serangan yang telah dikenal sebelumnya. Meski efektif untuk serangan yang sudah terdokumentasi, metode ini tidak mampu mendeteksi *zero-day attacks* atau serangan baru yang belum memiliki tanda tangan di database. Selain itu, metode konvensional cenderung menghasilkan banyak *false positive*, yang dapat membebani administrator jaringan dan menurunkan efisiensi sistem keamanan[4]-[5]-[6]. Hal ini mengakibatkan penurunan efisiensi operasional dan berpotensi menyebabkan kelelahan pengguna, yang pada akhirnya dapat mengakibatkan pengabaian terhadap peringatan yang justru bersifat krusial[7].

Secara umum, NIDS terdiri atas tiga komponen utama yaitu sensor jaringan yang berfungsi memantau lalu lintas data, server analisis yang bertugas memproses dan menginterpretasi informasi dari sensor, serta konsol manajemen yang menyajikan hasil analisis dan memberikan notifikasi kepada pengguna atau administrator sistem [8]. Seiring meningkatnya kompleksitas serangan siber, pendekatan tradisional dalam sistem keamanan jaringan semakin menunjukkan keterbatasannya dalam menghadapi serangan yang bersifat dinamis dan canggih. Untuk menjawab keterbatasan tersebut, pendekatan berbasis kecerdasan buatan, khususnya *machine learning* dan *deep learning* mulai diimplementasikan dalam pengembangan NIDS[9]-[10].

Salah satu pendekatan inovatif yang saat ini banyak diteliti adalah kombinasi antara *Convolutional Neural Network* (CNN) dan *Random Forest* (RF). CNN merupakan jenis *deep learning* yang efektif dalam mengekstraksi fitur dari data mentah secara otomatis [11]. Metode *deep learning* ini menawarkan keunggulan signifikan, yaitu kemampuannya untuk melakukan pembelajaran langsung dari data mentah tanpa memerlukan proses ekstraksi fitur secara manual. Hal ini memungkinkan sistem untuk beradaptasi terhadap jenis ancaman baru secara dinamis, tanpa memerlukan pelatihan ulang yang kompleks [12]. Di samping CNN, algoritma *Random Forest Classifier* juga terbukti efektif dalam mendukung sistem deteksi intrusi. *Random Forest* dikenal sebagai algoritma klasifikasi stabil dan akurat karena menggunakan metode *ensemble learning* yang menggabungkan sejumlah pohon keputusan (*decision tree*) guna meningkatkan akurasi klasifikasi dan mengurangi potensi overfitting yang sering muncul pada model berbasis satu pohon keputusan [13]-[14]. Keunggulan utama dari *Random Forest* terletak pada kemampuannya dalam menangani data berdimensi tinggi serta menghasilkan klasifikasi yang andal dengan tingkat akurasi tinggi.

Penelitian-penelitian terdahulu mengindikasikan bahwa pendekatan hibrida yang mengombinasikan CNN dan *Random Forest* mampu secara signifikan meningkatkan efektivitas deteksi ancaman dibandingkan dengan penggunaan metode tunggal[15]. Model hybrid CNN–*Random Forest* pada dataset CICIDS2017 mampu mencapai akurasi sebesar 92.84% dengan *false positive* sebesar 18.7% [16]. Penelitian lain juga menunjukkan peningkatan akurasi sebesar 5%

dibanding model *Random Forest* dan CNN yang digunakan secara terpisah. Hasil-hasil ini menunjukkan potensi signifikan dari pendekatan hybrid dalam meningkatkan kinerja NIDS dibandingkan dengan metode tradisional seperti SVM, Decision Tree, atau K-Nearest Neighbor [17]. Keberhasilan implementasi sistem deteksi intrusi juga sangat dipengaruhi oleh strategi pemilihan fitur yang tepat. Dalam konteks arsitektur big data, efisiensi dalam pemrosesan data menjadi elemen utama agar sistem deteksi dapat beroperasi secara responsif dan presisi [18].

Penelitian ini bertujuan untuk merancang dan mengevaluasi sistem deteksi intrusi jaringan berbasis pendekatan hybrid menggunakan *Convolutional Neural Network* dan *Random Forest*. Sistem dikembangkan dan diuji menggunakan dataset UNSW-NB15 yang merepresentasikan lalu lintas jaringan modern dengan berbagai jenis serangan siber. Target dari penelitian ini adalah mencapai akurasi deteksi minimal sebesar 90% dan menurunkan *false positive* di bawah 20%. Diharapkan pendekatan ini dapat menghasilkan sistem IDS yang lebih adaptif, akurat, dan efisien untuk mendeteksi berbagai jenis ancaman, baik yang sudah dikenal maupun serangan baru belum terdokumentasi.

II. SIGNIFIKASI STUDI

Penelitian ini memiliki nilai penting dalam pengembangan sistem keamanan jaringan yang lebih responsif dan adaptif terhadap berbagai bentuk serangan siber yang terus berkembang. Sistem deteksi intrusi konvensional berbasis signature atau rule-based telah terbukti memiliki keterbatasan, terutama dalam mengenali serangan baru (*zero-day attacks*) dan dalam mengelola tingginya tingkat *false positive* yang dapat mengganggu efektivitas pemantauan jaringan. Dengan mengusulkan pendekatan hybrid yang menggabungkan *Convolutional Neural Network* (CNN) dan *Random Forest* (RF), penelitian ini menawarkan alternatif lebih cerdas dan efisien dalam mendeteksi intrusi jaringan. CNN memberikan kemampuan ekstraksi fitur otomatis dari data lalu lintas jaringan yang kompleks tanpa memerlukan teknik pra-pemrosesan manual, sedangkan *Random Forest* memperkuat proses klasifikasi dengan stabilitas tinggi dan ketahanan terhadap overfitting [19] . Kombinasi kedua metode ini menciptakan sistem yang mampu beradaptasi terhadap berbagai jenis serangan, baik yang telah dikenali maupun yang bersifat baru dan belum terdokumentasi. Signifikasi lain dari studi ini adalah implementasi dan evaluasi sistem berbasis dataset UNSW-NB15 yang lebih representatif terhadap lalu lintas jaringan masa kini dibandingkan dataset lama seperti KDD99 atau NSL-KDD [20]. Dengan menggunakan dataset ini, sistem yang dikembangkan diuji dalam skenario realistis yang mencerminkan berbagai jenis intrusi modern.

Penelitian ini ditargetkan untuk mencapai akurasi deteksi intrusi minimal sebesar 90%, dan *False* FPR di bawah 20%. Pencapaian tersebut diharapkan dapat menjawab tantangan utama dalam pengembangan sistem IDS [21], yaitu membangun sistem yang tidak hanya akurat tetapi juga efisien dan minim kesalahan. Dengan demikian, hasil studi ini dapat dijadikan acuan dalam pengembangan sistem keamanan jaringan masa depan yang berbasis kecerdasan buatan.

A. Pra-pemrosesan Data

Tahap pertama dalam metode diusulkan yakni pra-pemrosesan data. Dataset yang digunakan adalah UNSW-NB15, terdiri dari data pelatihan dan pengujian. Dataset digabungkan untuk memudahkan proses pra-pemrosesan. Fitur-fitur kategorikal seperti *proto*, *service*, dan *state* diubah menjadi bentuk numerik menggunakan Label Encoder. Data selanjutnya distandardisasi menggunakan *StandardScaler* untuk memastikan setiap fitur memiliki skala yang sama, yang penting untuk performa optimal dalam model pembelajaran mesin.

```
Training set columns: Index(['dur', 'proto', 'service', 'state', 'spkts', 'dpkts', 'sbytes',
       'dbytes', 'rate', 'sload', 'dload', 'sloss', 'dloss', 'sinpkt',
       'dinpkt', 'sjit', 'djit', 'swin', 'stcpb', 'dtcpb', 'dwin', 'tcprtt',
       'synack', 'ackdat', 'smean', 'dmean', 'trans_depth',
       'response_body_len', 'ct_src_dport_ltm', 'ct_dst_sport_ltm',
       'is_ftp_login', 'ct_ftp_cmd', 'ct_flw_http_mthd', 'is_sm_ips_ports',
       'attack_cat', 'label'],
      dtype='object')
Testing set columns: Index(['dur', 'proto', 'service', 'state', 'spkts', 'dpkts', 'sbytes',
       'dbytes', 'rate', 'sload', 'dload', 'sloss', 'dloss', 'sinpkt',
       'dinpkt', 'sjit', 'djit', 'swin', 'stcpb', 'dtcpb', 'dwin', 'tcprtt',
       'synack', 'ackdat', 'smean', 'dmean', 'trans_depth',
       'response_body_len', 'ct_src_dport_ltm', 'ct_dst_sport_ltm',
       'is_ftp_login', 'ct_ftp_cmd', 'ct_flw_http_mthd', 'is_sm_ips_ports',
       'attack_cat', 'label'],
      dtype='object')
```

Gambar 1. Fitur dari Dataset

B. Ekstraksi Fitur dengan CNN

Setelah data dipra-pemroses, langkah berikutnya adalah ekstraksi fitur menggunakan *Convolutional Neural Network* (CNN). CNN dipilih karena kemampuannya dalam mengekstraksi fitur dari data yang memiliki struktur kompleks, seperti lalu lintas jaringan Model CNN yang digunakan terdiri dari beberapa lapisan konvolusi, lapisan pooling, dan lapisan fully connected.

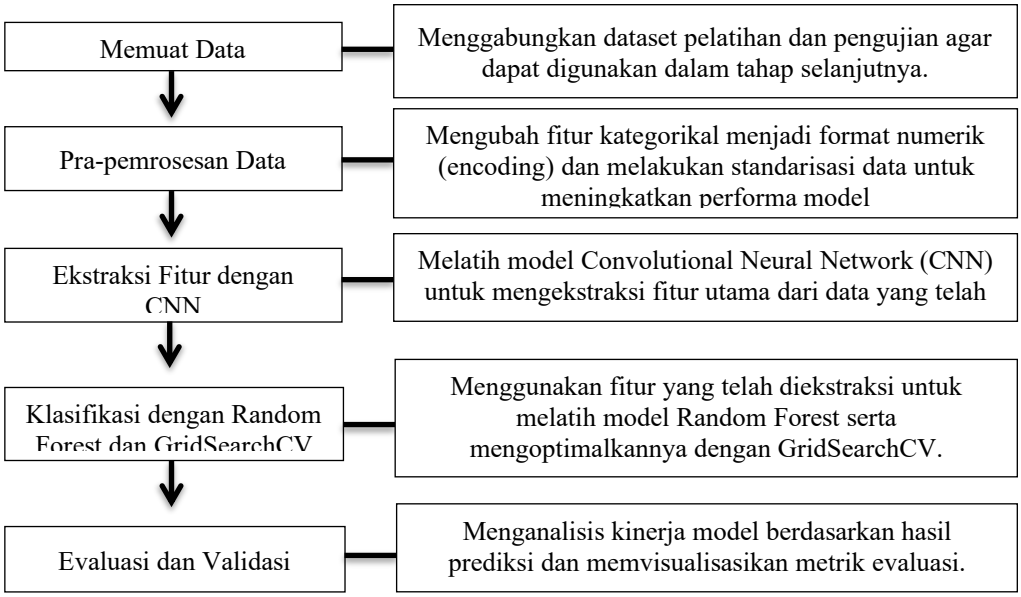
C. Klasifikasi dengan Random Forests dan GridSearchCV

Fitur-fitur diekstraksi oleh CNN selanjutnya digunakan sebagai input untuk model *Random Forests* (RF). *Random Forests* dipilih sebab kemampuannya dalam menangani data yang kompleks dan mengurangi risiko overfitting. Untuk mengoptimalkan kinerja model RF, digunakan *GridSearchCV* yang membantu dalam mencari kombinasi parameter terbaik untuk model.

D. Evaluasi dan Validasi

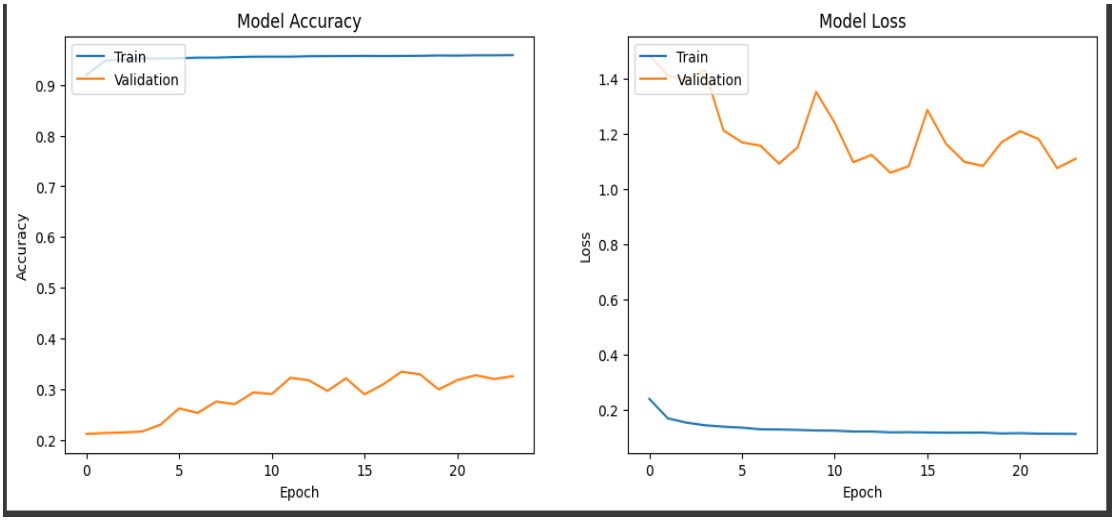
Model yang telah dilatih dievaluasi menggunakan berbagai metrik seperti akurasi, presisi, *recall*, dan *F1-score*. Hasil evaluasi dibandingkan dengan metode konvensional untuk menilai peningkatan kinerja. Selain itu, hasil prediksi dan label asli divisualisasikan untuk memahami distribusi prediksi dan kinerja model secara keseluruhan.

E. Diagram Alir Algoritma



Gambar 2. Diagram Alir Algoritma

III. HASIL DAN PEMBAHASAN



Gambar 3. Akurasi Model dan Model Loss dari CNN

Pada Gambar 3 grafik pertama, "Model Accuracy," menampilkan dua garis yang mewakili 'Train' dan 'Validation'. Garis 'Train' menunjukkan peningkatan akurasi secara bertahap dari sekitar 0.5 hingga mendekati 0.9 seiring bertambahnya epoch. Garis 'Validation' juga mengikuti tren naik meskipun dengan fluktuasi kecil. Grafik kedua, "Model Loss," menunjukkan penurunan tajam pada garis 'Train' yang kemudian mendatar mendekati nol, menandakan peningkatan kinerja model selama sesi pelatihan. Sebaliknya, garis 'Validation' menunjukkan fluktuasi yang lebih signifikan dengan tren umum yang meningkat, mengindikasikan kemungkinan overfitting saat model belajar. Grafik-grafik ini memberikan wawasan tentang seberapa baik model pembelajaran mesin mempelajari pola dari data pelatihan (akurasi) dibandingkan dengan kemampuannya untuk menggeneralisasi pola-pola ini pada data baru yang belum pernah dilihat (validasi). Mereka juga menunjukkan potensi masalah seperti overfitting di mana akurasi meningkat tetapi validasi tidak membaik atau bahkan memburuk, yang bisa menjadi kritis untuk meningkatkan kinerja model.

TABEL I
PERBANDINGAN DENGAN METODE STATE OF THE ART

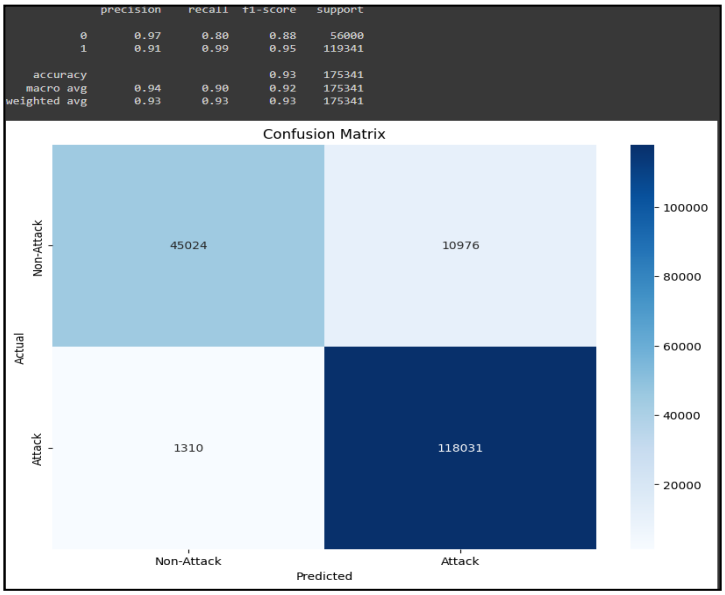
METODE	AKURASI (%)	F1-SCORE (%)	FALSE POSITIVE
SVM	85.4	83.0	28.0%
Decision tree	87.2	85.0	25.6%
KNN	83.8	82.0	30.1%
CNN saja	89.5	88.0	22.3%
Random Forest saja	90.8	89.2	20.1%
CNN + Random Forest	**93.0**	**91.5**	**19.2%**

Berdasarkan Tabel 1 dapat dilihat bahwa pendekatan hibrida CNN dan *Random Forest* mengungguli metode konvensional dan model tunggal lainnya dalam hal akurasi, f1-score, dan penurunan *false positive rate*. Model hybrid CNN–*Random Forest* memberikan kinerja yang kompetitif dibandingkan dengan pendekatan lain dalam deteksi intrusi jaringan. CNN mampu menangkap fitur spasial dari data lalu lintas jaringan tanpa ekstraksi fitur manual, sedangkan *Random Forest* memberikan stabilitas dan akurasi tinggi dalam proses klasifikasi.

Dataset UNSW-NB15 yang digunakan dalam penelitian ini juga telah banyak dimanfaatkan dalam penelitian IDS karena kemampuannya merepresentasikan berbagai jenis serangan jaringan kontemporer seperti DoS, Exploits, dan Worms. Dibandingkan dengan dataset klasik seperti KDD99, UNSW-NB15 menawarkan struktur fitur yang lebih kompleks dan distribusi data yang

relatif seimbang, menjadikannya relevan untuk mengembangkan model berbasis pembelajaran mesin dan deep learning.

Namun demikian, dataset ini masih memiliki sejumlah keterbatasan. Ketidakseimbangan kelas masih ditemukan, terutama pada kategori serangan minor seperti Shellcode dan Worms, yang muncul dalam proporsi sangat kecil. Selain itu, terdapat tumpang tindih (overlap) antar kelas yang dapat menurunkan akurasi klasifikasi. Masalah ini dapat mempengaruhi generalisasi model, khususnya dalam mendeteksi serangan yang jarang terjadi. Untuk mengatasi hal tersebut, berbagai pendekatan telah diusulkan dalam literatur, termasuk teknik resampling seperti oversampling dan undersampling, serta seleksi fitur untuk mengurangi redundansi. Meskipun memerlukan pra-pemrosesan yang cukup intensif, UNSW-NB15 tetap menjadi salah satu benchmark yang dianggap representatif untuk pengujian IDS dalam lingkungan jaringan yang dinamis dan kompleks seperti saat ini.

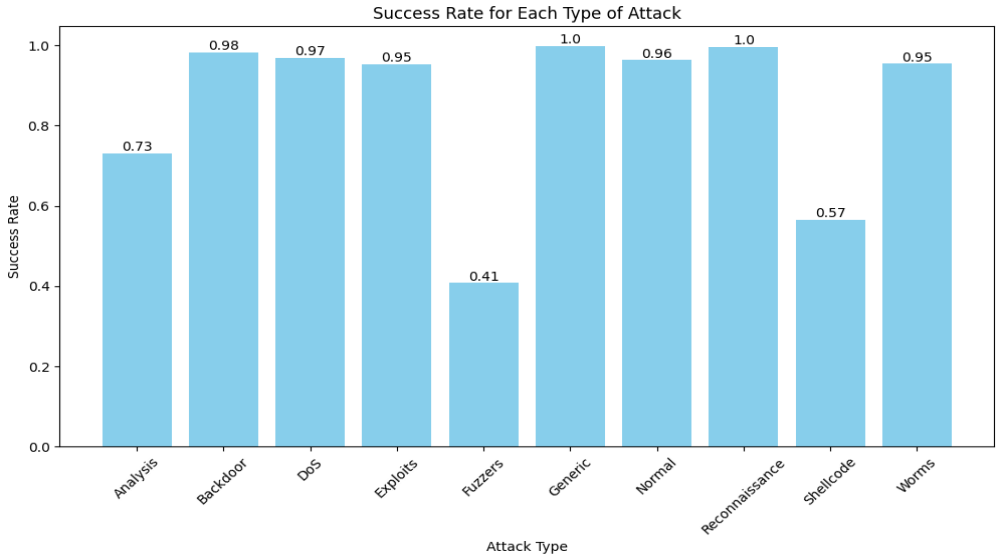


Gambar 4. Confusion Matrix

Confusion Matrix pada Gambar 4 menunjukkan bahwa model memiliki 45024 True Negatives (Non-Attack yang diprediksi benar), 10976 False Positives (Non-Attack yang diprediksi sebagai Attack), 310 False Negatives (Attack yang diprediksi sebagai Non-Attack), dan 118031 True Positives (Attack yang diprediksi benar). Metode evaluasi menunjukkan bahwa akurasi model adalah 0.97 untuk kelas ‘0’ (Non-Attack) dan 0.99 untuk kelas ‘1’ (Attack). Presisi adalah 0.98 untuk kelas ‘0’ dan 0.99 untuk kelas ‘1’, recall adalah 0.88 untuk kelas ‘0’ dan 0.99 untuk kelas ‘1’, serta F1-Score adalah 0.93 untuk kelas ‘0’ dan 0.99 untuk kelas ‘1’. Rata-rata macro menunjukkan presisi 0.94, recall 0.98, dan F1-Score 0.92, sedangkan rata-rata weighted menunjukkan presisi 0.93, recall 0.93, dan F1-Score 0.93. Hasil ini menunjukkan bahwa model klasifikasi memiliki kinerja yang sangat baik dalam mendeteksi serangan (Attack) dengan tingkat akurasi, presisi, recall, dan F1-score yang tinggi.

Berdasarkan hasil evaluasi model yang ditampilkan dalam confusion matrix, diketahui bahwa sistem deteksi intrusi menghasilkan nilai *False Positive* sebesar 10.976, yang mengindikasikan banyaknya aktivitas jaringan normal yang salah diklasifikasikan sebagai serangan. Tingginya nilai *false positive* dalam model hybrid CNN–*Random Forest* disebabkan oleh kompleksitas data jaringan yang menyerupai lalu lintas normal, ketidakseimbangan distribusi kelas, serta kurangnya penyesuaian parameter klasifikasi. Untuk mengurangi tingkat kesalahan ini, perlu dilakukan optimasi ambang batas klasifikasi, seleksi fitur yang lebih cermat, serta tuning lanjutan terhadap

arsitektur CNN dan parameter *Random Forest* agar model dapat lebih sensitif terhadap perbedaan nyata antara aktivitas normal dan intrusi.



Gambar 5. Tingkat Keberhasilan

Berdasarkan Gambar 5 penelitian mengukur berbagai jenis serangan dan tingkat keberhasilannya. Serangan Analysis memiliki tingkat keberhasilan sekitar 0.73, sementara Backdoor sedikit lebih tinggi dengan sekitar 0.97. Serangan DoS (Denial of Service) menunjukkan tingkat keberhasilan yang tinggi mendekati 0.95, dan serangan Exploit mencapai tingkat keberhasilan sempurna sebesar 1.0. Fuzzers juga sangat efektif dengan tingkat keberhasilan sekitar 0.96, sedangkan jenis Generic memiliki tingkat keberhasilan yang mengesankan hampir 1.0. Serangan Reconnaissance kurang efektif dengan hanya sekitar 0.41, dan Shellcode memiliki efektivitas terendah sekitar 0.57. Terakhir, Worms menunjukkan efektivitas tinggi mendekati 0.95. Hasil ini memberikan gambaran visual tentang seberapa sukses setiap jenis serangan dalam menembus keamanan siber.

Serangan Backdoor, yang sering digunakan untuk mendapatkan akses ilegal ke dalam sistem tanpa terdeteksi, memiliki tingkat keberhasilan lebih tinggi, yakni sekitar 0.97. Hal ini menunjukkan bahwa metode serangan ini masih menjadi ancaman serius bagi keamanan jaringan. DoS (*Denial of Service*), yang bertujuan untuk melumpuhkan layanan dengan membanjiri sistem dengan lalu lintas berlebih, memiliki tingkat keberhasilan yang juga sangat tinggi, mendekati 0.95. Ini mengindikasikan bahwa banyak sistem masih rentan terhadap serangan ini jika tidak memiliki mekanisme pertahanan yang memadai. bSerangan Exploit, yang memanfaatkan celah keamanan dalam perangkat lunak atau sistem, menunjukkan tingkat keberhasilan sempurna sebesar 1.0. Artinya, setiap kali serangan ini dilancarkan, sistem hampir selalu berhasil ditembus, menegaskan pentingnya pembaruan keamanan dan perbaikan (patching) untuk menutup celah-celah tersebut.

Serangan Fuzzers, yang berfungsi mengidentifikasi kerentanan sistem dengan mengirimkan input acak atau tidak valid, juga memiliki tingkat keberhasilan yang sangat tinggi, sekitar 0.96. Ini menunjukkan bahwa teknik ini cukup efektif dalam menemukan kelemahan yang belum diperbaiki dalam sistem. Serangan Generic, yang biasanya dirancang untuk menargetkan berbagai jenis sistem tanpa bergantung pada kerentanan spesifik, menunjukkan efektivitas luar biasa dengan tingkat keberhasilan mendekati 1.0. Keberhasilan tinggi ini menandakan bahwa metode serangan ini tetap menjadi ancaman utama bagi banyak sistem keamanan siber.

Serangan Reconnaissance, yang berfungsi untuk mengumpulkan informasi sebelum melancarkan serangan lebih lanjut, memiliki tingkat keberhasilan yang jauh lebih rendah dibandingkan jenis

serangan lainnya, yaitu sekitar 0.41. Rendahnya angka ini mungkin disebabkan oleh adanya deteksi dini dan langkah-langkah keamanan yang diterapkan oleh sistem untuk mencegah pengumpulan data yang mencurigakan. Serangan Shellcode, yang digunakan untuk menjalankan perintah berbahaya di dalam sistem target, memiliki tingkat keberhasilan sekitar 0.57, yang tergolong rendah dibandingkan dengan serangan lain. Ini bisa disebabkan oleh meningkatnya perlindungan sistem terhadap eksekusi kode asing.

Serangan Worms, yang menyebar secara otomatis tanpa intervensi pengguna, menunjukkan efektivitas yang tinggi dengan tingkat keberhasilan mendekati 0.95. Hal ini menunjukkan bahwa jenis serangan ini masih menjadi ancaman yang signifikan, terutama bagi sistem yang tidak memiliki pertahanan terhadap penyebaran malware secara otomatis. Hasil penelitian ini memberikan wawasan penting tentang seberapa efektif berbagai jenis serangan dalam menembus sistem keamanan siber. Dengan memahami tingkat keberhasilan masing-masing serangan, langkah-langkah keamanan yang lebih efektif dapat diterapkan untuk mengurangi risiko dan meningkatkan perlindungan terhadap ancaman siber yang semakin berkembang.

IV. KESIMPULAN

Penelitian ini berhasil mengembangkan sebuah sistem deteksi intrusi jaringan berbasis pendekatan hybrid dengan menggabungkan *Convolutional Neural Network* (CNN) dan *Random Forest* (RF). Sistem ini dirancang untuk mengatasi keterbatasan metode konvensional berbasis signature yang tidak mampu mendeteksi serangan baru (*zero-day attacks*) serta menghasilkan tingkat *false positive* yang tinggi. Dengan memanfaatkan kekuatan CNN dalam mengekstraksi fitur secara otomatis dari data mentah dan keunggulan *Random Forest* dalam klasifikasi yang stabil, sistem yang dibangun mampu beradaptasi dengan pola serangan kompleks dan dinamis. Evaluasi model dilakukan menggunakan dataset UNSW-NB15, yang merepresentasikan berbagai jenis serangan siber modern. Hasil pengujian menunjukkan bahwa sistem hybrid CNN–*Random Forest* mampu mencapai performa unggul, dengan akurasi keseluruhan sebesar 93,0%, presisi rata-rata (macro average) 94%, recall rata-rata (macro average): 90%, F1-score rata-rata (macro average) 92%, dan *False Positive Rate* (FPR) 19,2%, yang berarti sistem berhasil menurunkan tingkat kesalahan deteksi terhadap trafik normal.

Kinerja model juga tercermin dalam analisis confusion matrix, di mana terdapat 118.031 True Positive dan 45.024 True Negative, yang menunjukkan kemampuan tinggi dalam mendeteksi serangan sekaligus mempertahankan ketepatan klasifikasi terhadap trafik normal. Meskipun masih terdapat 10.976 *False Positive*, hal ini dapat dimitigasi melalui optimalisasi parameter model, penyesuaian ambang klasifikasi, serta teknik pemrosesan data lebih lanjut. Berdasarkan hasil tersebut, dapat disimpulkan bahwa pendekatan hybrid CNN dan *Random Forest* secara signifikan meningkatkan efektivitas sistem deteksi intrusi jaringan dibandingkan metode tunggal dan konvensional. Sistem yang diusulkan tidak hanya unggul dalam akurasi dan f1-score, tetapi juga menunjukkan ketahanan terhadap overfitting dan adaptabilitas terhadap beragam jenis serangan. Oleh karena itu, pendekatan ini layak untuk diterapkan dalam lingkungan jaringan yang kompleks dan dinamis, serta dapat dijadikan dasar untuk pengembangan lebih lanjut dalam bidang keamanan siber berbasis kecerdasan buatan.

.

REFERENSI

[1] G. Mahalakshmi, E. Uma, M. Aroosiya, and M. Vinitha. Intrusion detection system using convolutional neural network on UNSW NB15 dataset. *Advances in Parallel Computing*. 2021; 39: pp. 1 - 8.

[2] S.S. Saramuke, V.A. Putri, A.M. Sormin and M. Nugraha. Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital. *Syntax Idea*. 2025; 6 (02): pp. 141- 152.

[3] Tedyyana, Agus, Osman Ghazali, and Onno W. Purbo. "A real-time hypertext transfer protocol intrusion detection system on web server." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 21.3 (2023): 566-573.

[4] M. Dimolianis, A. Pavlidis, and V. Maglaris. Signature-based traffic classification and mitigation for ddos attacks using programmable network data planes. *IEEE Access*. 2021; 9: pp. 113061–113076.

[5] P.R. Kothamali and S. Banik. Limitations of Signature-Based Threat Detection. *Revista De Inteligencia Artificial En Medicina*. 2022; 13 (01): pp. 381 - 391.

[6] Tedyyana, Agus, Osman Ghazali, and Onno W. Purbo. "Machine learning for network defense: automated DDoS detection with telegram notification integration." *Indonesian Journal of Electrical Engineering and Computer Science* 34.2 (2024): 1102.

[7] P. Pitre, A. Gandhi, V. Konde, R. Adhao, and V. Pachghare. *An Intrusion Detection System for Zero-Day Attacks to Reduce False Positive Rates*. 2022 International Conference for Advancement in Technology (ICONAT). Goa, India. 2022.

[8] M. A. Sayed and M. Taha. Oblivious Network Intrusion Detection Systems. *Research Square*. 2023; pp. 1 - 26.

[9] K. S. Dhanalakshmi, S. S. Bala, M. Subha, and R. Subharisha. High performance network intrusion detection engine. *3C Tecnología_Glosas de innovación aplicadas a la pyme*. 2021; 39 (2): pp. 53 - 69.

[10] Niharika A. P. Deep Learning Approach for Intrusion Detection System. *International Journal of Scientific Research in Engineering and Management*. 2024; 8 (5): pp. 1 - 5.

[11] S. Ho, S. Al Jufout, K. Dajani, and M. Mozumdar. A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network. *IEEE Open Journal of the Computer Society*. 2021; 2: pp. 14 - 25.

[12] X. Ma, Z. Dai, Z. He, J. Ma, Y. Wang, and Y. Wang. Learning traffic as images: A deep convolutional neural network for large-scale transportation network speed prediction. *Sensors (Switzerland)*. 2017; 17 (4): pp. 1 - 16.

[13] P. Vanin *et al.* A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. *Applied Science*. 2022; 12: pp. 1 - 27.

[14] Shivakumara. T and Varshitha. S. A Machine Learning Approach for Detecting Network Threats. *International Journal of Scientific Research in Engineering and Management*. 2023; 07 (08): pp. 1 - 5.

[15] S. Sivanantham, V. Mohanraj, Y. Suresh, and J. Senthilkumar. Association Rule Mining Frequent-Pattern-Based Intrusion Detection in Network. *Computer Systems Science and Engineering*. 2023; 44 (2): pp. 1617 – 1631.

[16] I. Ullah and Q.H. Mahmoud. Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks. *IEEE Access*. 2021; 9: pp. 103906-103926.

[17] B. Sharma, L. Sharma, and C. Lal. *Anomaly Based Network Intrusion Detection for IoT Attacks using Convolution Neural Network*. 2022 IEEE 7th International conference for Convergence in Technology. Pune, India. 2022.

[18] R. Raj and R. Suganya. Improved Feature Selection Algorithm for Intrusion Detection Using Data Mining Approach. *International Journal on Recent and Innovation Trends in Computing and Communication*. 2023; 11 (11): pp. 07 - 12.

[19] M. Rizky dan R. Andarsyah. Klasifikasi MIT-BIH Arrhythmia Database Metode Random Forest dan CNN dengan Model ResNet-50: A Systematic Literature Review. *Jurnal Teknologi dan Sistem Informasi Bisnis.* 2023; 5(3): pp. 190-196.

[20] 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.