DECODE: JURNAL PENDIDIKAN TEKNOLOGI INFORMASI
P-ISSN: 2775-2984 | E-ISSN: 2775-1813
Vol. 5, No 3, November 2025, Hal: 839-851
Doi: http://dx.doi.org/10.51454/decode.v5i3.1348
https://journal.umkendari.ac.id/index.php/decode

Deteksi dan Respon Insiden Terotomatisasi Menggunakan Kerangka Kerja NIST dengan Metode Robust Random Cut Forest dan Random Forest Regressor

Rorim Irvano Prahara[1], Budi Prasetya[1], Rudi Rusdiah[1]
[1]Program Studi Magister Ilmu Komputer, Universitas Budi Luhur, Indonesia.

Artikel Info

Kata Kunci:

Deteksi anomali;
Pembelajaran mesin;
Hutan acak;
Kerangka NIST;

Keywords:

Anomaly detection;
Machine learning;
Random forest;
NIST framework

Riwayat Artikel:

Submitted: 13 September 2025
Accepted: 01 Oktober 2025
Published: 01 Oktober 2025

Abstrak: Meningkatnya ancaman serangan siber dan kebocoran data menuntut organisasi menerapkan pendekatan keamanan yang lebih canggih dan proaktif. Sistem deteksi berbasis tanda tangan dinilai tidak lagi memadai karena kurang mampu mengenali serangan baru maupun varian modifikasi. Di sisi lain, implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mempertegas kewajiban organisasi untuk melindungi data melalui sistem deteksi dan respons insiden yang cepat serta andal. Penelitian ini bertujuan merancang sistem deteksi dan respons insiden siber terotomatisasi dengan memadukan machine learning untuk deteksi anomali dan klasifikasi serangan. Metode yang digunakan menggabungkan Robust Random Cut Forest (RRCF) untuk deteksi anomali unsupervised pada data streaming dan Random Forest Regressor (RFR) untuk pemodelan prediktif, menciptakan pendekatan hybrid yang lebih akurat. Untuk klasifikasi serangan digunakan Random Forest Classifier (RFC). Seluruh rancangan mengacu pada kerangka kerja NIST Cybersecurity Framework dan diintegrasikan dengan platform SIEM Wazuh guna memungkinkan peringatan dini dan respons otomatis. Hasil pengujian menunjukkan RFC mencapai kinerja optimal pada dataset UNSW-NB15, CIC-IDS-2017, dan data nyata, bahkan memperoleh skor sempurna dalam beberapa skenario. Sementara itu, kombinasi RRCF dan RFR terbukti efektif mendeteksi anomali real-time tanpa false positive. Kesimpulannya, sistem yang dibangun responsif, adaptif, akurat, serta mendukung kepatuhan regulasi UU PDP, sehingga berkontribusi nyata bagi penguatan keamanan siber organisasi di era digital.

Abstract: *The increasing threat of cyberattacks and data breaches demands organizations to adopt more sophisticated and proactive cybersecurity approaches. Signature-based detection systems are no longer sufficient due to their inability to identify new or modified attack variants. On the other hand, the implementation of Law Number 27 of 2022 on Personal Data Protection (UU PDP) reinforces the legal obligation of organizations to protect data through fast and reliable detection and incident response systems. This study aims to design an automated cyber incident detection and response system by integrating machine learning for anomaly detection and attack classification. The method combines Robust Random Cut Forest (RRCF) for unsupervised anomaly detection in streaming data and Random Forest Regressor (RFR) for predictive modeling, creating a hybrid approach that enhances accuracy. For attack classification, the Random Forest Classifier (RFC) is employed. The entire design follows the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is integrated with the Wazuh SIEM platform to enable early warning*

and automated response. Experimental results demonstrate that the RFC achieves outstanding performance on the UNSW-NB15, CIC-IDS-2017, and real network datasets, even reaching perfect scores in several scenarios. Meanwhile, the hybrid RRCF and RFR approach proves highly effective in real-time anomaly detection without false positives. In conclusion, the proposed system is responsive, adaptive, highly accurate, and compliant with the PDP Law, providing significant contributions to strengthening proactive cybersecurity in the digital era.

Corresponding Author:
Rorim Irvano Prahara
Email: rorimirvano@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transaksi digital yang cepat, menciptakan big data (Sunarto et al., 2024) sekaligus meningkatkan kerentanan terhadap ancaman siber. Maraknya kasus kebocoran dan penyalahgunaan data di sektor e-commerce, perbankan, dan fintech (Lutrianto & Riswaldi, 2025) menunjukkan urgensi dari masalah ini. Data (BSSN, 2023) memperkuat kondisi ini dengan mencatat lebih dari 403 juta anomali trafik dan 1,6 juta data exposure di Indonesia pada tahun 2023, yang didominasi oleh ancaman serius seperti Generic Trojan RAT, APT, ransomware, dan Data Breach. Fakta ini menegaskan bahwa organisasi membutuhkan sistem deteksi dan respons insiden (SDIR) yang tidak hanya cepat dan efektif tetapi juga adaptif untuk melindungi aset dan mencegah pelanggaran data, terutama dengan telah diundangkannya Undang-Undang Perlindungan Data Pribadi (UU PDP) (Pemerintah Republik Indonesia, 2022).

Gambar 1. Anomali Trafik Tahun 2023

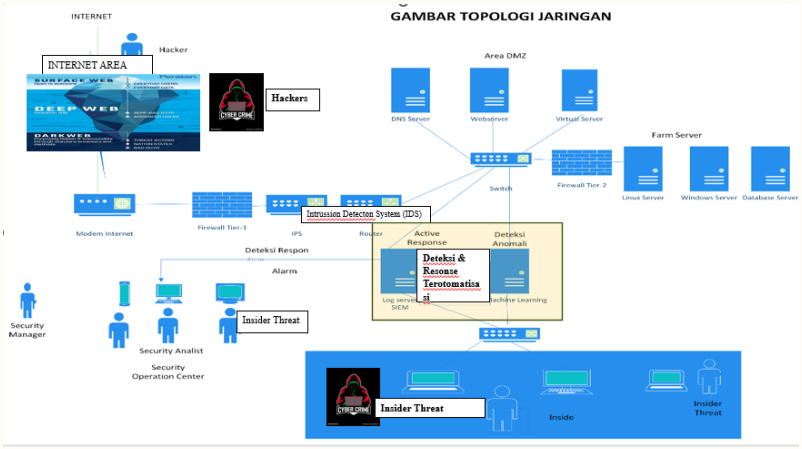
Berbagai penelitian sebelumnya telah mengembangkan solusi machine learning untuk keamanan siber (Avcı & Koca, 2023). (Divekar et al., 2018) dan (Agustina et al., 2024) menggunakan algoritma Random Forest dengan seleksi fitur untuk deteksi intrusi, sementara (Guha et al., 2016) memperkenalkan Robust Random Cut Forest (RRCF) untuk deteksi anomali pada data streaming. (Xuan et al., 2021) juga berkontribusi dengan optimasi model untuk meningkatkan akurasi. Namun, tinjauan literatur menunjukkan bahwa sebagian besar penelitian berfokus pada satu pendekatan (unsupervised atau supervised) dan diuji pada dataset publik yang umum seperti (CIC, 2017; UNSW, 2021) tanpa validasi kuat pada lingkungan industri spesifik. Kesenjangan (gap) ini terletak pada kurangnya integrasi hybrid yang memadukan kedua pendekatan secara sinergis serta evaluasi kinerjanya pada data riil dari sebuah organisasi.

Penelitian ini bertujuan untuk menjembatani gap tersebut dengan merancang sebuah sistem SDIR otomatis yang inovatif. Keunikan penelitian ini terletak pada tiga aspek utama: pertama, penerapan metode hybrid yang mengkombinasikan RRCF (untuk deteksi anomali unsupervised pada data streaming) dan Random Forest Regressor (untuk pemodelan prediktif supervised) guna mencapai

akurasi yang lebih tinggi. Kedua, sistem dirancang sesuai kerangka kerja National Institute of Standards and Technology (NIST) Cybersecurity Framework dan terintegrasi dengan platform SIEM (Wazuh) (Widyatono & Sulistyo, 2023) untuk memungkinkan respons otomatis yang komprehensif. Ketiga, penelitian ini tidak hanya menguji model pada dataset publik tetapi juga memvalidasinya pada dataset internal berupa log server jaringan dari sebuah perusahaan finansial sekuritas di Indonesia, sehingga kontribusinya diharapkan dapat memberikan solusi yang lebih aplikatif dan kontekstual bagi dunia industri.

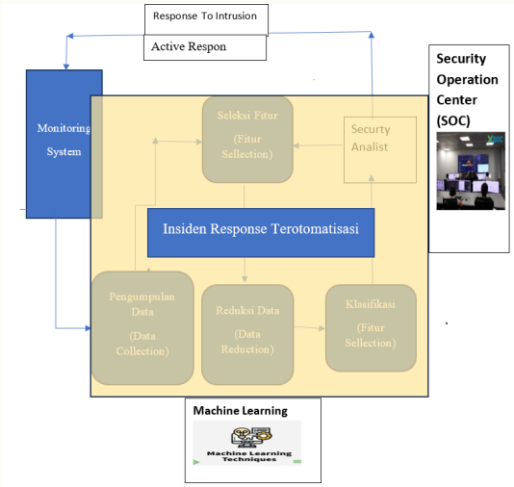
METODE

Berikut ini merupakan metode yang diusulkan oleh penulis terkait Solusi termasuk gambar topologi yang diusulkan dan metode yang akan digunakan. Gambar 2 dibawah ini adalah topologi jaringan yang diusulkan oleh penulis untuk Solusi ini.

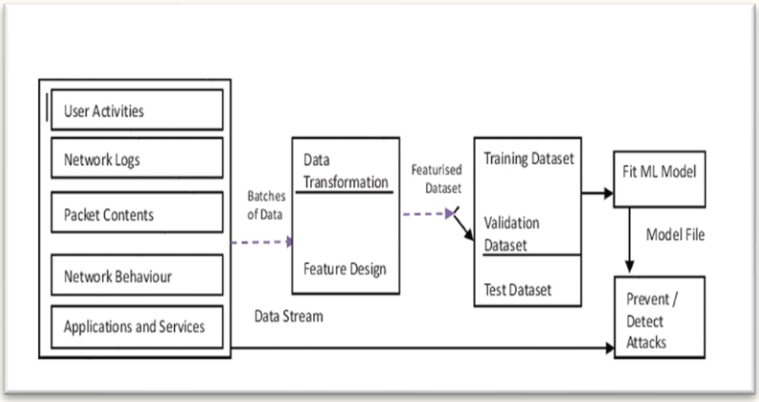


Gambar 2. Gambar Topologi Jaringan

Pengembangan dan optimisasi metode terus dilakukan untuk menghasilkan model Intrusion Detection System (IDS) yang lebih akurat dan efisien (Vourganas & Michala, 2024). Pada penelitian ini, penulis mengusulkan penerapan machine learning (Kostas, 2023)untuk membangun model IDS yang robust. Secara keseluruhan, tahapan penelitian dimulai dari akuisisi data, preprocessing, pembangunan model, hingga evaluasi, yang diilustrasikan dalam diagram alir pada Gambar 3.



Gambar 3. Pembentukan Model deteksi Insiden Respon



Gambar 4. Flow Model deteksi intrusi berbasis Machine Learning.

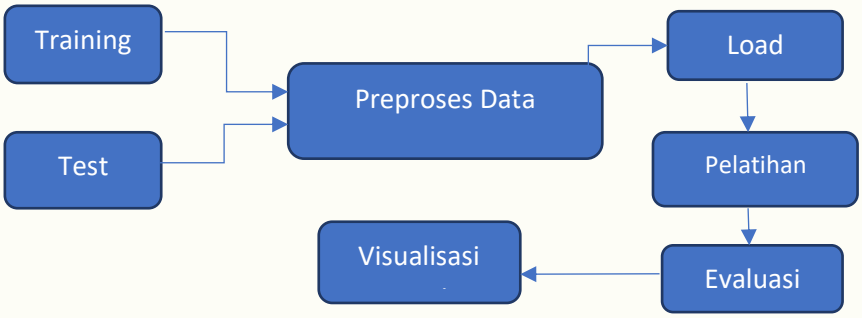
Tahap preprocessing data merupakan langkah krusial sebelum pemodelan. Pada dataset publik (CIC, 2017; UNSW, 2021) dan dataset internal, penanganan nilai null dan duplikat dilakukan terlebih dahulu. Untuk fitur kategorikal, diterapkan one-hot encoding guna mengubah data kategori menjadi format biner yang dapat diproses oleh model matematis. Selanjutnya, seluruh fitur numerik dinormalisasi menggunakan StandardScaler untuk menyamakan skala data, mencegah fitur dengan magnitudo besar mendominasi proses pembelajaran model. Setelah data siap, penelitian ini membangun dua model inti:

1. Model Klasifikasi dengan Random Forest Classifier (RFC): Algoritma RFC dipilih sebagai model utama untuk tugas klasifikasi jenis serangan (Budiman et al., 2021). Pemilihan RFC didasarkan pada kemampuannya yang terbukti dalam menangani data dalam skala besar dengan dimensi tinggi, resisten terhadap overfitting berkat mekanisme bagging-nya, serta mampu mengukur pentingnya setiap fitur (feature importance) yang berguna untuk analisis lebih lanjut (Rafrastaraa et al., 2023). Model ini akan dilatih untuk mengklasifikasikan traffic jaringan ke dalam kategori normal atau berbagai jenis serangan (e.g., DDoS, PortScan, Web Attack pada CIC-IDS-2017 dan 9 kategori pada UNSW-NB15 (Moustafa & Slay, 2016)).
2. Model Deteksi Anomali Hybrid (RRCF + RFR): Untuk deteksi anomali pada data streaming, digunakan pendekatan hybrid yang mengkombinasikan Robust Random Cut Forest (RRCF) untuk analisis unsupervised awal dalam mengidentifikasi outlier, dan Random Forest Regressor (RFR) untuk memodelkan skor error dari RRCF guna meningkatkan akurasi dan mengurangi false positive (Azugo et al., 2024; Xuan et al., 2021).

Dataset yang digunakan terdiri dari:

1. Dataset Publik: CIC-IDS-2017 dan UNSW-NB15, yang merupakan benchmark standar dalam penelitian IDS.
2. Dataset Internal: Kumpulan log server jaringan dari perusahaan finansial sekuritas target penelitian, yang berisi ~15 juta records yang dikumpulkan selama periode tiga bulan. Dataset internal ini dibagi dengan proporsi 80:20, dimana 80% data (~12 juta records) digunakan untuk pelatihan (training) dan validasi model, dan 20% sisanya (~3 juta records) digunakan sebagai data uji (testing) yang sama sekali tidak tersentuh selama proses training untuk menguji performa model yang sebenarnya.

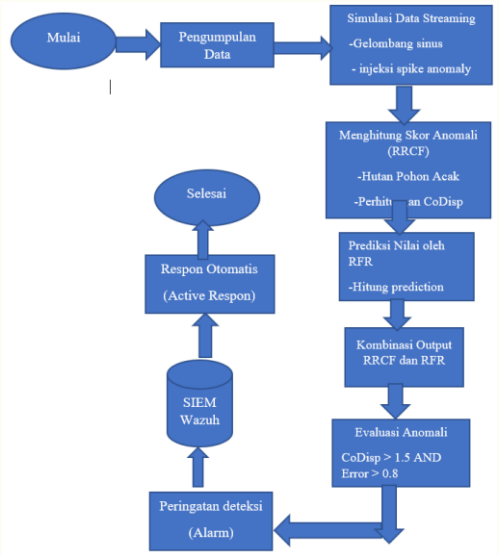
Dengan pendekatan ini, penelitian ini tidak hanya menguji keefektifan model pada data publik tetapi juga memvalidasi kinerjanya pada lingkungan jaringan riil (Hariyanti et al., 2024), sehingga diharapkan dapat memberikan solusi IDS yang lebih aplikatif.



Gambar 5. Metode Machine Learning

Penelitian ini mengembangkan sistem klasifikasi serangan siber menggunakan algoritma Random Forest Classifier (RFC). Pengujian dilakukan pada dua dataset publik terkemuka, CIC-IDS-2017 dan UNSW-NB15, yang berisi lalu lintas jaringan berlabel yang mensimulasikan berbagai serangan modern (seperti DDoS, PortScan, dan 9 kategori lainnya) beserta aktivitas normal. Proses klasifikasi diotomatisasi melalui aplikasi berbasis Streamlit dengan tahapan utama sebagai berikut:

1. Unggah & Preprocessing Data: Pengguna mengunggah file CSV. Sistem kemudian membersihkan data dengan menghapus fitur non-prediktif (seperti IP Address dan Timestamp) untuk mencegah overfitting. Label serangan dikonversi menjadi format biner (0 untuk normal, 1 untuk serangan), dan fitur kategorikal diubah menjadi numerik menggunakan one-hot encoding.
2. Pelatihan Model: Dataset dibagi dengan proporsi 80:20, dimana 80% data digunakan untuk melatih model RFC dan 20% untuk pengujian. Pemilihan RFC didasarkan pada kemampuannya yang robust dalam menangani data besar, resisten terhadap overfitting, dan memberikan akurasi tinggi.
3. Evaluasi & Visualisasi Performa: Model yang telah dilatih dievaluasi dengan metrik standar industri yaitu Akurasi, Presisi, Recall, F1-Score, dan ROC-AUC. Hasil evaluasi ditampilkan dalam bentuk visualisasi intuitif seperti Confusion Matrix, Grafik Feature Importance, dan ROC Curve untuk memudahkan interpretasi pengguna.



Gambar 6. Strategi Implementasi RRCF dan RFR

Sistem deteksi anomali real-time dalam penelitian ini mengadopsi pendekatan hybrid yang menggabungkan dua algoritma: Robust Random Cut Forest (RRCF) dan Random Forest Regressor (RFR). Metode ini dirancang untuk secara adaptif dan akurat mengidentifikasi penyimpangan dalam aliran data (data streaming) jaringan. Prinsip kerjanya adalah sebagai berikut:

1. Deteksi Awal dengan RRCF: Algoritma RRCF berperan sebagai detektor unsupervised awal. Ia menganalisis struktur data untuk menghitung CoDisp Score guna mengidentifikasi titik data yang secara struktural menyimpang (outlier), tanpa perlu diawali dengan data berlabel.
2. Konfirmasi dengan RFR: Algoritma RFR berperan untuk mempelajari pola normal data historis dan memprediksi nilai yang diharapkan pada suatu waktu. Dengan membandingkan nilai prediksi (Gruginskie & Vaccaro, 2018) ini dengan nilai aktual dari data stream, sistem menghasilkan prediction error. Error yang sangat tinggi (menyimpang dari pola yang dipelajari) kemudian dikonfirmasi sebagai anomali, sehingga meningkatkan akurasi dan mengurangi false positive.

Dengan pembagian peran ini, RRCF memberikan peringatan dini yang cepat, sementara RFR bertindak sebagai filter pintar untuk mengonfirmasi ancaman yang sesungguhnya, menghasilkan sistem deteksi yang lebih robust. Setelah model melalui tahap evaluasi dan menunjukkan performa yang memadai, langkah selanjutnya adalah mengimplementasikannya dalam lingkungan jaringan nyata untuk melakukan deteksi anomali secara real-time. Implementasi ini melibatkan penerapan model pada data streaming langsung dari jaringan, dimana skor anomali dihitung untuk setiap data point yang masuk. Hasil deteksi tersebut kemudian dapat langsung dimanfaatkan untuk memicu peringatan (alert) atau menjalankan tindakan mitigasi otomatis.

Untuk memastikan kualitas data yang digunakan dalam pelatihan model, penelitian ini menerapkan strategi pengambilan sampel yang cermat guna menangani masalah ketidakseimbangan kelas (class imbalance) yang lazim terjadi pada dataset keamanan siber. Metode utama yang digunakan adalah Stratified Sampling pada dataset UNSW-NB15 dan CIC-IDS-2017. Metode ini menjaga proporsi original antara kelas normal dan anomali dalam setiap subset data (latih, uji, dan validasi), sehingga menjamin model terpapar dengan representasi semua kelas yang proporsional selama pelatihan dan evaluasinya tidak bias. Sebagai pembanding, metode Under-sampling juga dipertimbangkan untuk scenario tertentu yang memprioritaskan efisiensi komputasi dengan mengorbankan sebagian data mayoritas.

Dengan menggabungkan dataset benchmark yang komprehensif dan metodologi sampling yang robust, penelitian ini memastikan bahwa model dilatih pada data yang bervariasi dan representatif, sehingga diharapkan dapat berkinerja baik ketika dihadapkan pada data jaringan yang nyata.

HASIL DAN PEMBAHASAN

Berikut ini merupakan hasil dari simulasi pengujian dan evaluasi sistem deteksi serangan siber berbasis *Random Forest Classifier* untuk klasifikasi lalu lintas jaringan, serta sistem deteksi anomali hybrid menggunakan kombinasi *Robust Random Cut Forest (RRCF)* dan *Random Forest Regressor (RFR*). Evaluasi dilakukan dari aspek performa model, efektivitas deteksi, dan integrasi dengan sistem *SIEM* Wazuh (Bassey et al., 2024). Sistem ini diuji menggunakan dua dataset benchmark populer di bidang keamanan jaringan (Nugroho & Rochmadi, 2024), yaitu CICIDS2017 dan UNSW-NB15 dan dataset nyata dari jaringan internal Perusahaan.

Tabel 1. Lingkungan Perangkat Keras (*Hardware*)

Komponen	**Spesifikasi**
Procesor	Processor Intel Pentium Core I7
RAM	RAM 16 GB
Sistem Operasi	Microsoft Windows 10/11

Tabel 2. Lingkungan Perangkat Lunak (*Software*)

Komponen	**Versi/Detail**
Python 3.10	1.27.2
Scikit-Learn	1.3.2

Matplotlib, Seaborn	visualisasi
RRCF	rrcf v0.4.3 (anomaly detection)
Wazuh	Versi 5.03

Pada penelitian ini system deteksi dirancang dengan dua metode jalur utama yang terdiri dari :

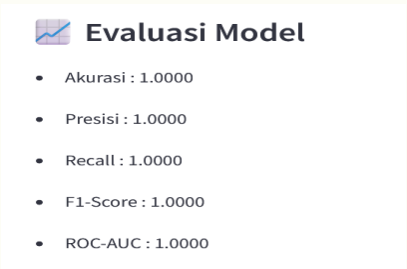
1. Tab1 menjelaskan simulasi Klasifikasi Serangan Siber (berbasis Random Forest Classifier) Digunakan untuk melakukan klasifikasi antara normal (Benign) dan serangan (Atack).
2. Tab2 menjelaskan simulasi Deteksi Anomali Streaming (menggunakan hybrid RRCF + RFR) digunakan untuk mendeteksi anomali pada simulasi aliran data streaming atau adata yang mengalir secara realtime pada jaringan computer (Li & Liu, 2021).
3. Tab3 menjelaskan tentang alur Flowchart integrasi Deteksi anomali (IDS) dengan SIEM Wazuh.

Pada arsitektur jaringan tradisional yang ada pada saat ini terdapat *SIEM* (*Security Information and Event Management*) menggunakan platform wazuh yang mengumpulkan log dari perangkat sekuritu seperti *firewall, IPS, WAF, Antivirus* (Widyatono & Sulistyo, 2023) yang digunakan sebagai system monitoring untuk mendeteksi serangan namun system ini masih berbasis tradisional yang berbasis signature base masih memiliki kelemahan antara lain:

1. Masih sering terjadi false positip ini menjadikan masalah untuk system deteksi monitoring.
2. Pada model signature base sangat tergantung pada database serangan yang sudah pernah ada, system ini mempunyai kelemahan untuk jebis serangan (attack) baru yang belum pernah ada sebelumnya.

Dataset UNSW-NB15 mencakup lalu lintas jaringan yang dikumpulkan melalui penggunaan alat IXIA *PerfectStorm* untuk mensimulasikan aktivitas jaringan normal dan berbagai serangan. Setiap record mewakili satu flow jaringan dan dilengkapi dengan label: normal atau attack. Terdapat total 9 jenis serangan yang direkam, termasuk *Fuzzers, Backdoors, Exploits, Generic, Reconnaissance*, *Shellcode, Worms, DoS, dan Analysis*. Untuk keperluan pelatihan dan evaluasi model, dataset ini dibagi menjadi dua bagian yang telah ditentukan oleh pembuatnya: 1. Training set: 175.341 record, 2. Testing set: 82.332 record. Setiap record dalam dataset memiliki 49 fitur, yang terdiri dari fitur numerik (seperti durasi koneksi, jumlah byte, dan jumlah paket) serta fitur kategorikal (seperti jenis protokol atau arah lalu lintas). Dalam proses pra-pemrosesan, fitur kategorikal dikonversi ke dalam format numerik menggunakan teknik encoding seperti *one-hot encoding* atau label *encoding*, sedangkan fitur numerik dinormalisasi menggunakan teknik seperti min-max scaling atau *z-score* standardization agar seluruh fitur berada pada skala yang seragam.

Berdasarkan pengujian dengan dataset UNSW-NB15, model Random Forest Classifier menunjukkan hasil yang sangat optimal dengan nilai akurasi, presisi, recall, F1-score, dan *ROC-AUC* masing-masing sebesar 1.0000. Hal ini mengindikasikan bahwa model mampu mendeteksi seluruh trafik serangan maupun trafik normal secara sempurna. Meskipun performa ini sangat baik, perlu dilakukan pengujian lanjutan pada data real-time atau data yang berbeda agar memastikan model tidak mengalami overfitting. Integrasi hasil deteksi ke dalam sistem log Wazuh memungkinkan pengawasan aktif terhadap aktivitas mencurigakan sesuai dengan prinsip Detect dalam kerangka kerja NIST CSF serta penerapan prinsip keamanan data pribadi sesuai UU PDP (Pemerintah Republik Indonesia, 2022). Hasil evaluasi model dengan *Random Forest Classifier* menunjukan bahwa:



Gambar 7. Evaluasi Model dengan Random Forest Classifier

Tabel 3. Evaluasi Model

Matrik	Nilai	Penjelasan
Akurasi	1.0000	Semua prediksi tepat. Tidak ada salah klasifikasi.
Presisi	1.0000	Semua yang diklasifikasikan sebagai serangan benar-benar serangan.
Recall	1.0000	Semua serangan berhasil dideteksi tanpa ada yang terlewat.
F1-Score	1.0000	Keseimbangan sempurna antara presisi dan recall.
ROC-UAC	1.0000	Kemampuan model membedakan aRecallntara kelas serangan dan normal sangat baik.

Hasil Confusion Matrix menunjukan bahwa:

Tabel 4. Confusion Matrix

	Predicted Benign	Predicted Attack
Actual Benign	890	0
Hasil Confusion Matrix Actual Attack	0	110

Intepretasi Hasil didapatkan sebagai berikut:

Tabel 5. Interpretasi Hasil

Metrik	Nilai	Penjelasan
True Negative (TN)	890	Benign diklasifikasi sebagai Benign (benar)
False Positive (FP)	0	Benign diklasifikasi sebagai Attack (tidak ada kesalahan)
False Negative (FN)	0	Attack diklasifikasi sebagai Benign (tidak ada serangan yang lolos)
True Positive (TP)	1110	Attack diklasifikasi sebagai Attack (benar)

Simulasi Pengujian streaming anomali dilakukan dengan menyisipkan gangguan periodik ke dalam sinyal data. Sistem deteksi menggunakan metode hybrid antara *Robust Random Cut Forest (RRCF)* dan *Random Forest Regressor (RFR). RRCF* mendeteksi pola struktural yang menyimpang, sementara RFR mengukur seberapa besar prediksi model meleset dari nilai aktual. Kombinasi keduanya memberikan hasil deteksi yang lebih akurat dan minim false positive. sistem dapat mendeteksi seluruh titik injeksi anomali secara tepat dan mengirimkan log sesuai ke Wazuh (Widyatono & Sulistyo, 2023).

Pada tahap simulasi, sistem melakukan deteksi anomali berbasis time-series menggunakan kombinasi algoritma *RRCF (Robust Random Cut Forest)* dan *Random Forest Regressor (RFR)*. Data stream disimulasikan dengan sinyal sinusoidal yang disisipkan lonjakan (spike) sebagai anomali. Deteksi anomali dilakukan dengan dua pendekatan:

1. Skor CoDisp (RRCF) yang mengukur outlierness berdasarkan struktur pohon acak.
2. Error Prediksi (RFR) yang mengukur seberapa jauh prediksi meleset dari kenyataan. Sebuah titik dianggap anomali jika:
   a. Skor CoDisp melebihi threshold 1.5
   b. Error prediksi lebih dari 0.8

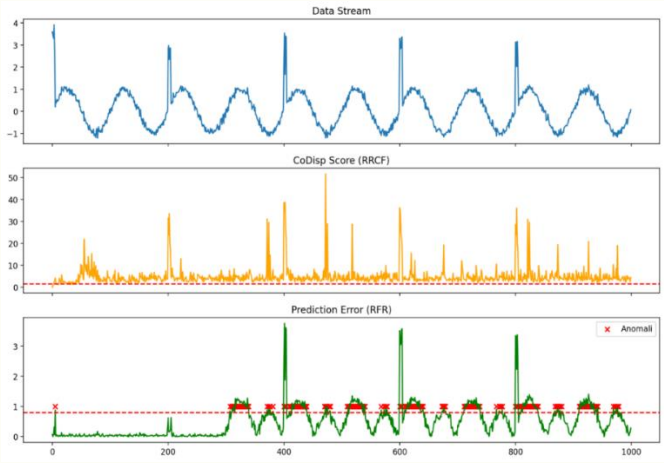
Adapun mekanisme deteksi *Hybrid* RRCF dan RFR dalah sebagai berikut:

Tabel 6. Mekanisme Deteksi Hybrid RRCF dan RFR

Komponen	Tujuan
RRCF	Menilai keanehan struktur data streaming (deteksi outlier struktural).
Random ForestRegressor	Mengukur seberapa besar penyimpangan nilai (error prediksi).

Hybrid Rule	Anomali = CoDisp > 1.5 dan Error > 0.8

Maka dengan pendekatan ini system dapat Menghindari false positive dari RRCF saja dan Mendeteksi perubahan bentuk data & prediksi sekaligus.



Gambar 8. Hybrid Deteksi Anomali

Hasil simulasi menunjukkan bahwa terdapat 292 anomali yang berhasil dideteksi. Seluruh anomali ini kemudian dikirim sebagai log ke Wazuh melalui protokol syslog dengan format pesan: [ALERT] Anomali terdeteksi dari IP 192.168.1.100 pada indeks ke-{n}, Pesan-pesan tersebut dikirim secara real-time dan terekam dalam file log anomali_export.log, serta ditangkap oleh sistem deteksi Wazuh berdasarkan konfigurasi decoder dan rules yang telah diatur sebelumnya. Berikut ini adalah sebagian cuplikan dari log hasil deteksi:

Tabel 7. Log Hasil Deteksi

Indeks	CoDisp Score	Error Prediksi
5	4.15	1.04
205	3.26	0.86
316	3.79	1.07
555	2.11	1.29

Secara umum, skor CoDisp tertinggi mencapai lebih dari 50, dan error prediksi maksimum lebih dari 3.5, menandakan deteksi sangat kuat terhadap anomali dengan deviasi besar dari pola normal. Deteksi ini secara otomatis dipantau oleh Wazuh Active Response, yang dapat memicu tindakan mitigasi seperti blocking IP jika jumlah alert melewati ambang batas (threshold) tertentu.

Pengujian dan Evaluasi dilakukan terhadap model klasifikasi serangan siber menggunakan algoritma Random Forest Classifier dengan input data dari dataset CIC-IDS-2017. Pengujian dibagi berdasarkan jenis serangan, yaitu DDoS, PortScan, dan WebAttack. Hasil pengujian dan evaluasi mencakup metrik-metrik utama seperti akurasi, presisi, recall, F1-score, serta kurva ROC (Receiver Operating Characteristic) dan confusion matrix untuk masing-masing jenis serangan (Bharadiya, 2023). Berikut adalah tabel performa model terhadap ketiga jenis serangan:

Tabel 8. Performance Model terhadap Serangan

Jenis Serangan	Akurasi	Presisi	Recall	F1-Score	ROC-AUC
DDoS	0.9991	0.9974	0.9983	0.9995	
PortScan	0.9995	1.0000	0.9991	0.9996	1.0000
WebAttack	0.9975	1.0000	0.8000	0.8889	

Model menunjukkan tingkat akurasi yang tinggi (99,75%), dengan presisi sempurna (1.0000), yang berarti semua prediksi serangan merupakan serangan yang benar (tanpa false positive). Hal ini sangat penting untuk menghindari alarm palsu yang dapat mengganggu sistem keamanan. Namun demikian, nilai recall sebesar 0.8000 mengindikasikan bahwa terdapat beberapa serangan (sekitar 20%) yang tidak berhasil terdeteksi oleh model (false negative), yang masih menjadi kelemahan yang perlu diperhatikan. Dari sisi evaluasi lainnya, nilai F1-Score sebesar 0.8889 menunjukkan keseimbangan yang cukup baik antara presisi dan recall. Selain itu, ROC-AUC sebesar 0.9976 menegaskan bahwa model memiliki kapabilitas yang sangat tinggi dalam membedakan antara trafik benign dan trafik serangan. Hasil evaluasi juga menunjukkan bahwa:

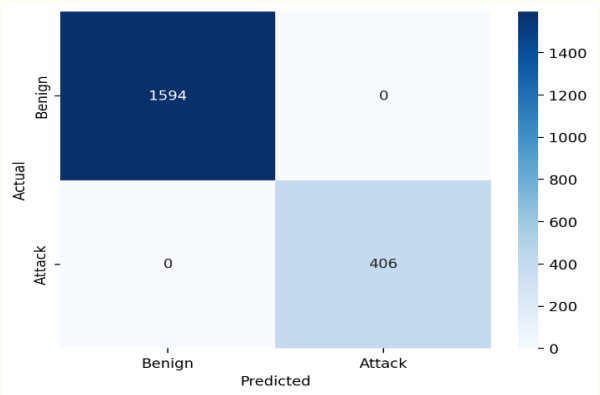
a. Sebanyak 1975 data benign berhasil diklasifikasikan dengan benar (True Negative).
b. Tidak terdapat false positive, yaitu data benign yang salah diklasifikasikan sebagai attack.
c. Terdapat 20 data attack yang berhasil dideteksi oleh model (True Positive).
d. Namun, terdapat 5 data serangan yang tidak terdeteksi dan diklasifikasikan sebagai benign (False Negative).

Nilai-nilai ini mengindikasikan bahwa model memiliki kemampuan klasifikasi yang sangat tinggi, dengan kesalahan klasifikasi yang sangat kecil. Hal ini juga diperkuat oleh ROC Curve yang hampir menyentuh titik sudut kiri atas (0,1), serta nilai F1-Score yang mendekati 1, menunjukkan keseimbangan optimal antara presisi dan recall. Confusion matrix memberikan informasi lebih rinci tentang klasifikasi model terhadap setiap kelas. Matriks ini terdiri dari 2x2 kotak yang menampilkan jumlah prediksi benar dan salah dalam tiap kelas. Visualisasi confusion matrix membantu dalam mengidentifikasi pola kesalahan model, misalnya kecenderungan terhadap false negative yang bisa sangat berbahaya pada sistem deteksi intrusi. Pengujian lanjutan dilakukan dengan menggunakan dataset attack_dataset_100MB_final.csv yang terdiri dari berbagai jenis serangan siber seperti *Brute Force, DoS, Port Scan* (Dasmen et al., 2022), *Web Attack, Botnet, dan Infiltration* (Halder & Ozdemir, 2018). Dataset ini lebih kompleks dan representatif terhadap skenario nyata dalam jaringan, sehingga cocok untuk menguji kemampuan generalisasi model deteksi serangan.

Hasil pengujian menunjukkan bahwa model Random Forest Classifier mampu mengklasifikasikan data dengan tingkat akurasi sempurna. Berikut adalah hasil confusion matrix:

Tabel 9. Hasil Confusion Matrix

	Predicted Benign	**Predicted Attack**
Actual Benign	1594	0
Actual Attack	0	406



Gambar 9. Evaluasi Model

Dari confusion matrix tersebut, dapat diperoleh data sebagai berikut ini :

a. True Positive (TP) = 406 merupakan data *attack* yang diklasifikasikan sebagai serangan (*attack*).
b. True Negative (TN) = 1594 merupakan data benign yang diklasifikasikan sebagai normal (benign).

c. False Positive (FP) = 0 adalah data benign yang salah diklasifikasikan sebagai attack
d. False Negative (FN) = 0 adalah data attack yang salah diklasifikasikan sebagai benign

Sehingga perhitungan Jumlah total data = TP + TN + FP + FN = 406 + 1594 + 0 + 0 = 2000 data.

KESIMPULAN

Berdasarkan hasil pengujian dan analisis, penelitian ini berhasil mengembangkan dan mengimplementasikan sebuah sistem deteksi dan respons insiden siber yang terotomatisasi. Sistem ini memanfaatkan pendekatan hybrid machine learning, menggabungkan Random Forest Classifier (RFC) untuk klasifikasi serangan dan kombinasi Robust Random Cut Forest (RRCF) serta Random Forest Regressor (RFR) untuk deteksi anomali pada data streaming. Secara keseluruhan, dapat disimpulkan bahwa:

1. Kinerja Sistem yang Unggul: Model RFC menunjukkan performa klasifikasi biner yang luar biasa pada dataset CIC-IDS-2017 dan UNSW-NB15, dengan berbagai metrik evaluasi (akurasi, presisi, recall, F1-score) mencapai nilai hampir sempurna (~99%) (Sharafaldin et al., 2019). Hal ini membuktikan kehandalannya dalam membedakan trafik normal dan malicious secara konsisten.
2. Efektivitas Metode Hybrid untuk Deteksi Real-Time: Pendekatan hybrid RRCF dan RFR terbukti efektif dalam meningkatkan akurasi deteksi anomali pada data streaming. Kombinasi analisis struktural (CoDisp score) dan analisis prediktif (prediction error) berhasil mengidentifikasi anomali dengan stabil dan meminimalkan kesalahan deteksi (false positive), menjadikannya solusi yang layak untuk lingkungan operasional.
3. Integrasi dan Respons Otomatis yang Berhasil: Sistem berhasil diintegrasikan dengan platform SIEM Wazuh, menciptakan alur kerja dari deteksi hingga respons otomatis (seperti pemblokiran IP). Integrasi ini tidak hanya mempercepat waktu respons tetapi juga menempatkan sistem dalam kerangka keamanan siber yang komprehensif sesuai dengan fungsi Detect dan Respond dalam NIST Cybersecurity Framework.

Kontribusi Ilmiah dan Novelty, penelitian ini memberikan kontribusi dan kebaruan melalui:

1. Arsitektur Hybrid yang Inovatif: Mengusulkan dan memvalidasi sebuah arsitektur hybrid yang memadukan pendekatan unsupervised (RRCF) dan supervised (RFR, RFC) secara sinergis untuk menangani kedua tugas utama keamanan siber: klasifikasi dan deteksi anomali real-time.
2. Aplikasi dalam Konteks Regulasi: Penelitian ini mengaplikasikan solusi teknis machine learning secara langsung untuk menjawab tantangan kepatuhan terhadap Undang-Undang PDP No. 27 Tahun 2022. Sistem yang dibangun dapat menjadi alat pendukung bagi Data Protection Officer (DPO) dan Pengontrol Data dalam memenuhi kewajiban pelaporan insiden sesuai Pasal 46, khususnya dalam hal menghasilkan bukti log dan laporan tertulis yang cepat dan akurat dalam waktu 3x24 jam setelah terjadinya insiden.

Meskipun menunjukkan hasil yang positif, penelitian ini memiliki beberapa catatan yang perlu diperhatikan, yaitu:

1. Risiko Overfitting pada Model RFC: Akurasi yang sangat tinggi pada dataset uji publik mengindikasikan kemungkinan overfitting. Generalisasi performa model terhadap data jaringan nyata yang lebih dinamis dan beragam perlu diuji lebih lanjut.
2. Keterbatasan Dataset Simulasi Anomali: Pengujian deteksi anomali untuk data streaming masih mengandalkan data simulasi. Validasi pada aliran data jaringan real-time yang sesungguhnya dengan anomali yang lebih kompleks dan bervariasi diperlukan untuk mengonfirmasi keefektifannya di dunia nyata.
3. Cakupan Jenis Serangan: Dataset yang digunakan mungkin tidak mencakup seluruh vektor serangan siber mutakhir, seperti teknik evasion yang secara khusus dirancang untuk menipu model machine learning.

Oleh karena itu, penelitian selanjutnya disarankan untuk fokus pada: (1) pengumpulan dan penggunaan dataset jaringan riil yang lebih besar dan beragam, (2) eksplorasi teknik regularisasi dan model yang lebih kompleks (seperti Deep Learning) untuk meningkatkan generalisasi, serta (3) pengujian yang lebih rigor terhadap kemampuan deteksi serangan zero-day dan advanced persistent threats (APTs).

DAFTAR PUSTAKA

Agustina, T., Masrizal, M., & Irmayanti, I. (2024). Performance Analysis of Random Forest Algorithm for Network Anomaly Detection using Feature Selection. Sinkron, 8(2), 1116–1124. https://doi.org/10.33395/sinkron.v8i2.13625

Avcı, İ., & Koca, M. (2023). Cybersecurity Attack Detection Model, Using Machine Learning Techniques. Acta Polytechnica Hungarica, 20(7), 29–44. https://doi.org/10.12700/APH.20.7.2023.7.2

Azugo, P., Venter, H., & Nkongolo, M. W. (2024). Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset. https://arxiv.org/abs/2404.12855v1

Bassey, C., Chinda, E. T., & Idowu, S. (2024). Building a Scalable Security Operations Center: A Focus on Open-source Tools. Journal of Engineering Research and Reports, 26(7), 196–209. https://doi.org/10.9734/jerr/2024/v26i71203

Bharadiya, J. (2023). Machine Learning in Cybersecurity: Techniques and Challenges. European Journal of Technology, 7(2), 1–14. https://doi.org/10.47672/ejt.1486

BSSN. (2023). Lanskap Keamanan Siber 2023. https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf

Budiman, S., Sunyoto, A., & Nasiri, A. (2021). Analisa Performa Penggunaan Feature Selection untuk Mendeteksi Intrusion Detection Systems dengan Algoritma Random Forest Classifier. Sistemasi, 10(3), 753. https://doi.org/10.32520/stmsi.v10i3.1550

CIC. (2017). CIC - IDS2017. https://www.unb.ca/cic/datasets/ids-2017.html

Divekar, A., Parekh, M., Savla, V., Mishra, R., & Shirole, M. (2018). Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives. Proceedings on 2018 IEEE 3rd International Conference on Computing, Communication and Security, ICCCS 2018, 1–8. https://doi.org/10.1109/CCCS.2018.8586840

Gruginskie, L. A. dos S., & Vaccaro, G. L. R. (2018). Lawsuit lead time prediction: Comparison of data mining techniques based on categorical response variable. PLoS ONE, 13(6), 1–26. https://doi.org/10.1371/journal.pone.0198122

Guha, S., Mishra, N., Roy, G., & Schrijvers, O. (2016). Robust random cut forest based anomaly detection on streams. 33rd International Conference on Machine Learning, ICML 2016, 6, 3987–3999.

Halder, S., & Ozdemir, S. (2018). Hands-On Machine Learning for Cybersecurity.

Hariyanti, E., Hostiadi, D. P., Anggreni, Yohanes Priyo Atmojo, I Made Darma Susila, & Tangkawarow, I. (2024). Analisis Perbandingan Metode Seleksi Fitur pada Model Klasifikasi Decission Tree untuk Deteksi Serangan di Jaringan Komputer. Jurnal Sistem Dan Informatika (JSI), 18(2), 208–217. https://doi.org/10.30864/jsi.v18i2.615

Kostas, K. (2023). Anomaly infiltration detection in networks using machine learning. International Journal of Mechanical Engineering, 8(August). https://doi.org/10.56452/7-2-552

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lutrianto, I., & Riswaldi, R. (2025). Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia. Greenation International Journal of Law and Social Sciences, 3(2), 345–350. https://doi.org/10.38035/gijlss.v3i2.429.

Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal, 25(1–3), 18–31. https://doi.org/10.1080/19393555.2015.1125974

Nugroho, S., & Rochmadi, T. (2024). Analysis of Information Security Readiness Using the Index KAMI. Decode: Jurnal Pendidikan Teknologi Informasi, 4(3), 881–886. https://doi.org/10.51454/decode.v4i3.602

Pemerintah Republik Indonesia. (2022). Undang Undang Perlindungan Data Pribadi. 016999, 457–483.

Rafrastaraa, F. A., Pramunendar, R. A., Prabowo, D. P., Kartikadarma, E., & Sudibyo, U. (2023). Optimasi Algoritma Random Forest menggunakan Principal Component Analysis untuk Deteksi Malware. Jurnal Teknologi Dan Sistem Informasi Bisnis, 5(3), 217–223. https://doi.org/10.47233/jteksis.v5i3.854

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117(January 2019), 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2019). A Detailed Analysis of the CICIDS2017 Data Set. In Communications in Computer and Information Science (Vol. 977, Issue Cic). Springer International Publishing. https://doi.org/10.1007/978-3-030-25109-3_9

Sunarto, S. A., Maulidina, C. P., & Wijaya, W. V. (2024). Kajian Literatur: Penerapan Big Data dan Artificial Intelligence untuk Perkembangan Bidang Edukasi dan Bisnis. Kinesik, 11(3), 300–312. https://doi.org/10.22487/ejk.v11i3.1366

Torino, P. D. I., & Mennuni, A. M. (2023). Master Degree Thesis An Analysis of SOC Monitoring Systems.

UNSW. (2021). UNSW NB15. https://research.unsw.edu.au/projects/unsw-nb15-dataset

Vourganas, I. J., & Michala, A. L. (2024). Applications of Machine Learning in Cyber Security: A Review. Journal of Cybersecurity and Privacy, 4(4), 972–992. https://doi.org/10.3390/jcp4040045

Widyatono, D. P., & Sulistyo, W. (2023). Pemodelan Instrusion Prevention System Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan Wazuh. Journal of Information Technology Ampera, 4(1), 113–127. https://journal-computing.org/index.php/journal-ita/index

Xuan, C., Do, Thanh, H., & Lam, N. T. (2021). Optimization of network traffic anomaly detection using machine learning. International Journal of Electrical and Computer Engineering, 11(3), 2360–2370. https://doi.org/10.11591/ijece.v11i3.pp2360-2370