Jurnal Sistem Cerdas dan Rekayasa (JSCR)

Volume 8 , Nomor 1, April 2026

Website Jurnal : ojs.widyakartika.ac.id/index.php/jscr

Analisis Pengaruh Feature Decontamination terhadap Kinerja Deteksi Ransomware Menggunakan Random Forest

Sriyanto[1], Zuriati[2], Zarnelly[3], Yuri Fitrian[4]

[1]Jurusan Teknik Informatika, Institut Informatika dan Bisnis Darmajaya, Bandar Lampung, Indonesia, Email (sriyanto@darmajaya.ac.id)
[2]Jurusan Teknologi Informasi, Politeknik Negeri Lampung, Bandar Lampung, Indonesia, Email (zuriati_mi@polinela.ac.id)
[3]Jurusan Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia, Email (zarnelly@uin-suska.ac.id)
[4]Jurusan Sistem Informasi, STMIK Pringsewu, Pringsewu, Indonesia, Email (yurifitrian99@gmail.com)

STATUS ARTIKEL

Dikirim 7 Mei 2026
Direvisi 18 Mei 2026
Diterima 18 Mei 2026

Kata Kunci:
Data Leakage, Feature Decontamination, Intrusion Detection, Random Forest, Ransomware

A B S T R A K

Studi ini memfokuskan analisis pada dampak dekontaminasi fitur (feature decontamination) terhadap stabilitas model klasifikasi saat mengidentifikasi ransomware menggunakan dataset UNSW-NB15. Isu krusial pada data deteksi intrusi umumnya terletak pada kebocoran data (data leakage) atau kontaminasi fitur, yang berisiko memicu peningkatan performa model secara semu tanpa menggambarkan kapabilitas aslinya di lingkungan nyata. Penelitian ini menggunakan dua skenario eksperimen, yaitu tanpa feature decontamination dan dengan feature decontamination. Tahapan preprocessing meliputi encoding fitur kategorikal, normalisasi menggunakan StandardScaler, serta penyeimbangan data menggunakan SMOTE. Model klasifikasi yang digunakan adalah Random Forest, dipilih karena kemampuannya dalam menangani data tabular. Hasil penelitian menunjukkan bahwa model tanpa feature decontamination menghasilkan performa sempurna dengan nilai akurasi, precision, recall, dan F1-score sebesar 1.000, yang mengindikasikan adanya data leakage. Setelah dilakukan feature decontamination, performa model menjadi lebih realistis dengan akurasi sebesar 0.9028, precision sebesar 0.8820, recall sebesar 0.9506, dan F1-score sebesar 0.9150, serta nilai AUC sebesar 0.9795. Temuan ini menunjukkan bahwa feature decontamination berperan penting dalam meningkatkan validitas evaluasi model dengan menghilangkan bias dari fitur yang terkontaminasi. Dengan demikian, integritas data menjadi faktor kunci dalam pengembangan sistem deteksi ransomware yang andal.

1. PENDAHULUAN

Serangan siber berbasis ransomware menjadi salah satu ancaman paling destruktif saat ini karena kemampuannya mengunci dokumen pengguna lewat mekanisme enkripsi yang diinisiasi oleh peretas. Konsekuensi dari insiden ini tidak sekadar memicu hilangnya akses data krusial, melainkan juga melumpuhkan stabilitas operasional pada ranah industri, instansi pemerintahan, lembaga pendidikan, hingga sektor pelayanan publik (Asbath et al., 2025). Mengingat masifnya dampak yang ditimbulkan, urgensi terhadap perancangan sistem deteksi intrusi (Intrusion Detection System / IDS) semakin meningkat, khususnya platform yang andal dalam mengidentifikasi aktivitas anomali secara responsif dan presisi sebelum kerusakan meluas.

Dalam perkembangannya, implementasi teknologi pembelajaran mesin (machine learning / ML) kian mendominasi arsitektur IDS karena kapabilitasnya dalam mengeksplorasi karakteristik trafik jaringan secara otomatis. Algoritma Random Forest kerap menjadi pilihan utama para peneliti atas pertimbangan efektivitasnya dalam memproses tipe data tabular serta stabilitasnya yang tinggi terhadap fluktuasi data (Inayah et al., 2024; Kiswanto et al., 2025).

Guna mengoptimalkan proses pembelajaran algoritma, rangkaian rekayasa data awal—seperti konversi variabel kategorikal, standardisasi nilai, dan manipulasi sebaran kelas lewat SMOTE—sering kali diintegrasikan. Penerapan teknik SMOTE terbukti efektif meminimalkan bias pada kelas minoritas melalui penyeimbangan distribusi data, yang pada gilirannya memperkokoh konsistensi luaran klasifikasi (Zuriati et al., 2025).

Berbagai literatur ilmiah mengonfirmasi bahwa pendekatan ensemble learning, khususnya Random Forest, mampu mendongkrak performa fungsional IDS melalui kombinasi prediktor jamak demi mengekstraksi nilai akurasi dan recall yang lebih superior (Dong et al., 2021; Kasongo & Sun, 2020; Zhang et al., 2022). Eksperimen taktis Random Forest dalam ranah keamanan digital juga menunjukkan rekam jejak yang solid pada pelbagai studi kasus, termasuk mitigasi serangan pada arsitektur firewall, ekosistem Internet of Things (IoT), hingga anomali DoS di lingkungan Software-Defined Network (Arief et al., 2017; Pirtama, 2024). Kendati demikian, tingginya indikator performa yang ditunjukkan oleh pemodelan ML tidak serta-merta merepresentasikan kapabilitas deteksi yang sesungguhnya di lapangan. Anomali ini umumnya berakar dari fenomena feature contamination atau kebocoran data (data leakage), sebuah kondisi di mana variabel tertentu secara eksplisit maupun implisit merekam informasi yang terikat dengan label target. Akibatnya, sistem dapat menghasilkan akurasi mutlak tanpa benar-benar mengenali pola serangan siber yang substansial.

Eksistensi data leakage dalam ekosistem pembelajaran mesin dilaporkan memicu bias berupa hasil evaluasi yang kelewat optimistis, sehingga tidak sanggup mencerminkan performa operasional pada skenario riil (Kaufman et al., 2012). Selaras dengan hal tersebut, Bouke & Abdullah (2023) mempertegas bahwa kebocoran pola (pattern leakage) pada fase pra-proses berisiko mendegradasi reliabilitas IDS akibat pemanfaatan detail informasi yang semestinya disembunyikan selama fase pelatihan model. Di sisi lain, dataset UNSW-NB15 jamak diadopsi dalam studi keamanan siber lantaran dirancang khusus untuk merefleksikan karakteristik lalu lintas jaringan kontemporer (Moustafa & Slay, 2015). Namun demikian, beberapa atribut pada dataset tersebut berpotensi memberikan informasi yang terlalu berkaitan dengan label sehingga dapat mempermudah proses klasifikasi secara tidak realistis. Kondisi ini dapat menyebabkan hasil evaluasi model menjadi bias dan kurang mampu menggambarkan performa sebenarnya ketika diterapkan pada data nyata.

Tren riset terdahulu cenderung berfokus pada eskalasi metrik performa lewat adopsi algoritma yang semakin kompleks, termasuk pemanfaatan arsitektur deep learning, tanpa mengevaluasi aspek integritas fitur yang dilibatkan dalam fase training. Pola pendekatan seperti ini rawan melahirkan konklusi yang menyesatkan, sebab tingginya akurasi yang diperoleh belum tentu merepresentasikan kecerdasan model dalam menerjemahkan anomali trafik (Buczak & Guven, 2016). Padahal, beberapa kajian ilmiah telah membuktikan bahwa efisiensi operasional dan stabilitas sistem deteksi intrusi dapat ditingkatkan secara signifikan melalui tata kelola atribut serta seleksi fitur yang relevan (Basuki & Bachtiar, 2021; Riza, 2023).

Berangkat dari kesenjangan tersebut, penelitian ini diinisiasi untuk menganalisis pengaruh feature decontamination terhadap validitas kinerja deteksi ransomware memanfaatkan arsitektur Random Forest. Berbeda dari studi konvensional yang memosisikan penyaringan atribut sekadar sebagai bagian dari rutinitas pra-proses, penelitian ini menjadikan dekontaminasi fitur sebagai objek evaluasi sentral untuk menakar dampaknya terhadap objektivitas performa model. Pengujian dikembangkan melalui komparasi dua skenario utama, yaitu pemanfaatan parameter data secara utuh tanpa pembersihan versus implementasi fitur yang telah disterilkan dari potensi data leakage.

Penerapan model Random Forest secara konsisten pada kedua skenario sengaja dilakukan guna menjamin bahwa fluktuasi performa yang terjadi murni dipicu oleh rekayasa karakteristik fitur, bukan karena diferensiasi algoritma klasifikasi. Melalui pendekatan ini, studi diharapkan mampu menyajikan pemahaman komprehensif mengenai pentingnya aspek integritas data dalam perancangan platform deteksi ransomware berbasis pembelajaran mesin, sekaligus menyodorkan parameter evaluasi model yang lebih realistis dan dapat dipertanggungjawabkan.

2. METODE

2.1 Dataset

Dataset yang digunakan pada penelitian ini adalah UNSW-NB15, yaitu dataset publik yang dikembangkan untuk penelitian sistem deteksi intrusi jaringan (Moustafa & Slay, 2015). Dataset tersebut memuat berbagai jenis lalu lintas jaringan yang terdiri atas aktivitas normal maupun beberapa kategori serangan siber, termasuk ransomware. UNSW-NB15 telah menyediakan data pelatihan (training set) dan data pengujian (testing set) secara terpisah sehingga proses evaluasi model dapat dilakukan secara konsisten tanpa perlu melakukan pembagian data ulang.

2.2 Desain Eksperimen

Eksperimen pada penelitian ini dirancang dalam dua skenario komparatif, yaitu penggunaan seluruh fitur tanpa proses feature decontamination dan penggunaan fitur yang telah melalui proses feature decontamination. Pada skenario pertama, seluruh fitur dalam dataset digunakan tanpa penghapusan atribut. Sementara itu, pada skenario kedua dilakukan penghapusan fitur yang berpotensi menyebabkan data leakage, termasuk fitur attack_cat, fitur indikator seperti is_ftp_login dan is_sm_ips_ports, serta fitur dengan awalan ct_ yang merepresentasikan statistik koneksi. Kedua skenario menggunakan pipeline preprocessing dan model klasifikasi yang sama untuk memastikan bahwa perbedaan hasil evaluasi hanya disebabkan oleh keberadaan atau penghapusan fitur yang terkontaminasi.

2.3 Praproses Data

Tahapan praproses dilakukan untuk mempersiapkan data sebelum digunakan pada proses pelatihan model klasifikasi. Proses awal dilakukan dengan pemisahan dataset menjadi fitur (X) dan label (y), di mana label digunakan untuk menunjukkan kelas normal dan serangan. Selanjutnya, atribut kategorikal diubah ke dalam bentuk numerik menggunakan Ordinal Encoder. Proses fitting encoder hanya dilakukan pada data pelatihan, kemudian transformasi yang sama diterapkan pada data pengujian agar konsistensi data tetap terjaga. Setelah proses transformasi fitur, dilakukan normalisasi data menggunakan StandardScaler untuk menyamakan rentang nilai antar fitur sehingga proses pembelajaran model menjadi lebih optimal. Parameter normalisasi diperoleh dari data pelatihan dan selanjutnya diterapkan pada data pengujian untuk menghindari terjadinya data leakage selama proses evaluasi model.

Untuk menangani ketidakseimbangan distribusi kelas, digunakan metode SMOTE (Synthetic Minority Over-sampling Technique). SMOTE diterapkan hanya pada data pelatihan sehingga tidak mempengaruhi distribusi data pengujian. Teknik ini digunakan untuk menghasilkan sampel sintetis pada kelas minoritas sehingga distribusi data menjadi lebih seimbang dan proses pembelajaran model dapat berjalan lebih stabil (Zuriati et al., 2025). Selain itu, penggunaan SMOTE pada sistem deteksi intrusi juga telah dilaporkan mampu meningkatkan sensitivitas model terhadap pola serangan yang jumlah datanya lebih sedikit dibandingkan trafik normal.

2.4 Model Klasifikasi

Pada penelitian ini digunakan algoritma Random Forest sebagai model klasifikasi utama. Random Forest merupakan metode ensemble learning yang membangun sejumlah pohon keputusan secara acak, kemudian mengombinasikan hasil prediksi dari seluruh pohon untuk menentukan keputusan akhir. Pendekatan tersebut memungkinkan model menghasilkan klasifikasi yang lebih stabil dan mampu mengurangi risiko overfitting pada data berdimensi tinggi (Dong et al., 2021; Kasongo & Sun, 2020).

Konfigurasi model yang diterapkan meliputi penggunaan 200 pohon keputusan (*n_estimators* = 200), kedalaman maksimum pohon sebesar 15 (*max_depth* = 15), serta nilai random state sebesar 42 untuk menjaga konsistensi eksperimen. Penggunaan jumlah pohon

yang lebih banyak bertujuan meningkatkan kestabilan hasil prediksi dan membantu mengurangi variansi model selama proses klasifikasi.

Melalui mekanisme majority voting, Random Forest menghasilkan keputusan akhir berdasarkan prediksi mayoritas dari seluruh pohon keputusan yang dibangun. Dengan karakteristik tersebut, algoritma ini dinilai sesuai untuk proses deteksi ransomware pada dataset UNSW-NB15 yang memiliki karakteristik lalu lintas jaringan yang kompleks dan beragam.

2.5 Evaluasi Model

Kinerja model pada penelitian ini dianalisis menggunakan beberapa metrik evaluasi untuk mengukur kemampuan klasifikasi pada kedua skenario eksperimen. Evaluasi dilakukan menggunakan accuracy, precision, recall, dan F1-score. Nilai accuracy digunakan untuk melihat tingkat ketepatan prediksi model secara keseluruhan, sedangkan precision digunakan untuk mengukur ketepatan model dalam mengidentifikasi kelas serangan. Selanjutnya, recall digunakan untuk mengetahui kemampuan model dalam mendeteksi seluruh data serangan yang tersedia, sementara F1-score digunakan sebagai ukuran keseimbangan antara precision dan recall.

Selain itu, penelitian ini juga menggunakan kurva ROC dan nilai AUC (Area Under Curve) untuk mengevaluasi kemampuan model dalam membedakan kelas normal dan serangan. Analisis confusion matrix dilakukan untuk melihat distribusi hasil klasifikasi berdasarkan jumlah true positive, true negative, false positive, dan false negative. Di samping evaluasi performa klasifikasi, dilakukan pula analisis feature importance untuk mengetahui tingkat kontribusi masing-masing fitur terhadap proses pengambilan keputusan oleh model Random Forest.

3. HASIL DAN PEMBAHASAN

3.1 Kinerja Model Tanpa Feature Decontamination

Berdasarkan pengujian pada skenario pertama yang mengabaikan pembersihan fitur (without feature decontamination), algoritma Random Forest mencatatkan metrik akurasi, presisi, recall, sekaligus F1-score yang menyentuh angka mutlak yaitu 1.000. Capaian statistik ini merepresentasikan tingkat keberhasilan absolut, di mana sistem mampu mengidentifikasi seluruh sampel data pada repositori pengujian secara tepat tanpa kekeliruan klasifikasi sedikit pun. Kendati secara kuantitatif menyajikan hasil yang impresif, fenomena kesempurnaan performa seperti ini dinilai tidak wajar dalam ranah analisis data riil, terutama jika diaplikasikan pada kompilasi data yang memiliki kompleksitas tinggi sekelas UNSW-NB15. Skor sempurna tersebut mengonfirmasi adanya indikasi kuat keterjadian data leakage, sebuah anomali di mana model enkapsulasi memperoleh celah akses terhadap detail informasi yang berkorelasi implisit dengan label target selama fase pembelajaran berlangsung.

Dampaknya, algoritma kehilangan esensi utama untuk menerjemahkan karakteristik fungsional dari anomali lalu lintas jaringan, melainkan sekadar mengeksploitasi keterkaitan semu antara atribut pendukung dengan label klasifikasi. Kondisi tersebut memicu bias penilaian yang kelewat optimistis pada model (overoptimistic evaluation) dan memperbesar risiko kegagalan sistem saat dihadapkan pada objek data asing atau implementasi di lingkungan operasional yang dinamis. Oleh sebab itu, luaran dari skema eksperimen awal ini tidak dapat dijadikan sebagai indikator reliabel dalam mengukur kapabilitas klasifikasi model yang sebenarnya..

3.2 Kinerja Model Dengan Feature Decontamination

Pada tahapan eksperimen kedua, diimplementasikan prosedur feature decontamination dengan mengeliminasi atribut-atribut prediktor yang diidentifikasi memicu bias kebocoran

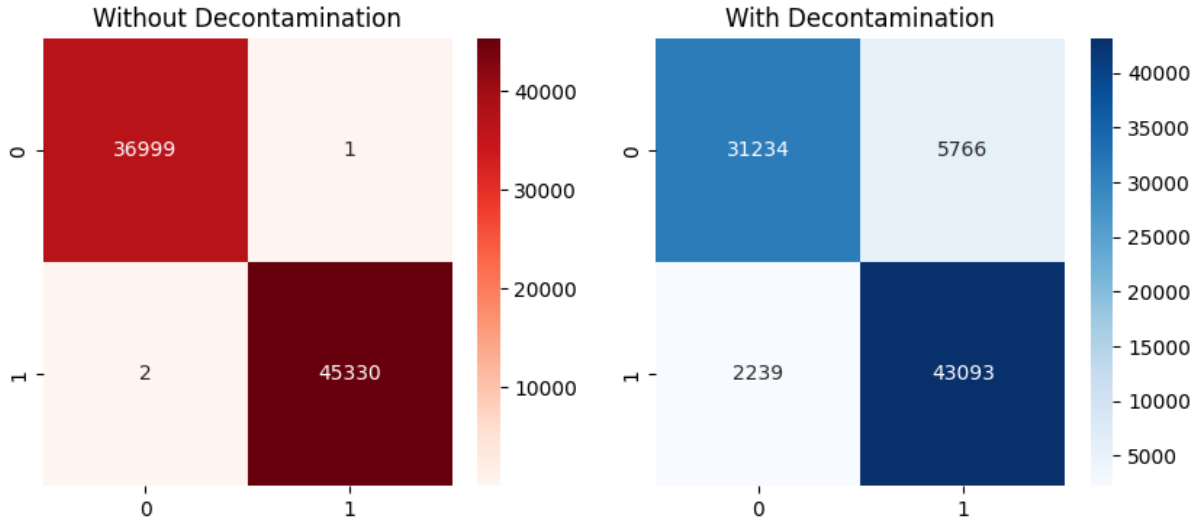
data. Pasca-sterilisasi komponen fitur tersebut, model diproses kembali memanfaatkan jalur pipa pengolahan (pipeline) yang identik dengan skenario pertama. Hasil pengujian menunjukkan adanya pergeseran nilai evaluasi, di mana model mengantongi tingkat akurasi sebesar 0.9028, nilai presisi pada angka 0.8820, skor recall mencapai 0.9506, dan capaian F1-score berada di tingkat 0.9150. Koreksi penurunan parameter performa ini jika dikomparasikan dengan skenario awal mempertegas bahwa kalkulasi pemodelan kini telah terbebas dari intervensi variabel data yang bias.

Tingginya capaian nilai recall (0.9506) membuktikan bahwa arsitektur yang dibangun tetap mempertahankan sensitivitas yang sangat andal dalam mengenali aktivitas serangan ransomware. Aspek ketajaman deteksi ini sangat krusial dalam ranah keamanan siber, mengingat kegagalan sistem dalam mengenali serangan (false negative) dapat memicu dampak kerusakan sistemik yang fatal pada infrastruktur jaringan. Di lain sisi, sedikit penurunan pada metrik presisi mengonfirmasi munculnya beberapa kesalahan prediksi atas trafik normal sebagai serangan, sebuah konsekuensi logis yang wajar timbul akibat penghapusan parameter kemudahan yang sebelumnya mendominasi proses klasifikasi secara semu.

Secara komprehensif, temuan eksperimental ini memperlihatkan bahwa model klasifikasi tetap mampu mempertahankan efektivitas dan performa yang solid walau komponen fitur yang terpolusi telah disingkirkan. Hasil evaluasi pada skenario kedua ini menyajikan gambaran performa yang jauh lebih objektif serta kredibel untuk merepresentasikan kondisi lapangan yang sesungguhnya.

3.3 Analisis Confusion Matrix

Distribusi hasil klasifikasi pada kedua skenario dapat dilihat pada gambar 3.1.



Gambar 3.1 Confusion Matrix Tanpa dan Dengan Feature Decontamination

Pada skenario tanpa feature decontamination, confusion matrix menunjukkan bahwa seluruh data berhasil diklasifikasikan dengan benar, baik pada kelas normal maupun kelas serangan. Hal ini menghasilkan matriks diagonal sempurna yang mengindikasikan tidak adanya kesalahan klasifikasi. Sebaliknya, pada skenario dengan feature decontamination, terlihat adanya distribusi kesalahan klasifikasi dalam bentuk false positive dan false negative. Meskipun demikian, jumlah kesalahan tersebut masih relatif kecil dibandingkan jumlah total data. Keberadaan kesalahan ini justru menunjukkan bahwa model bekerja secara lebih realistis, karena harus membedakan pola yang lebih kompleks tanpa bantuan fitur yang

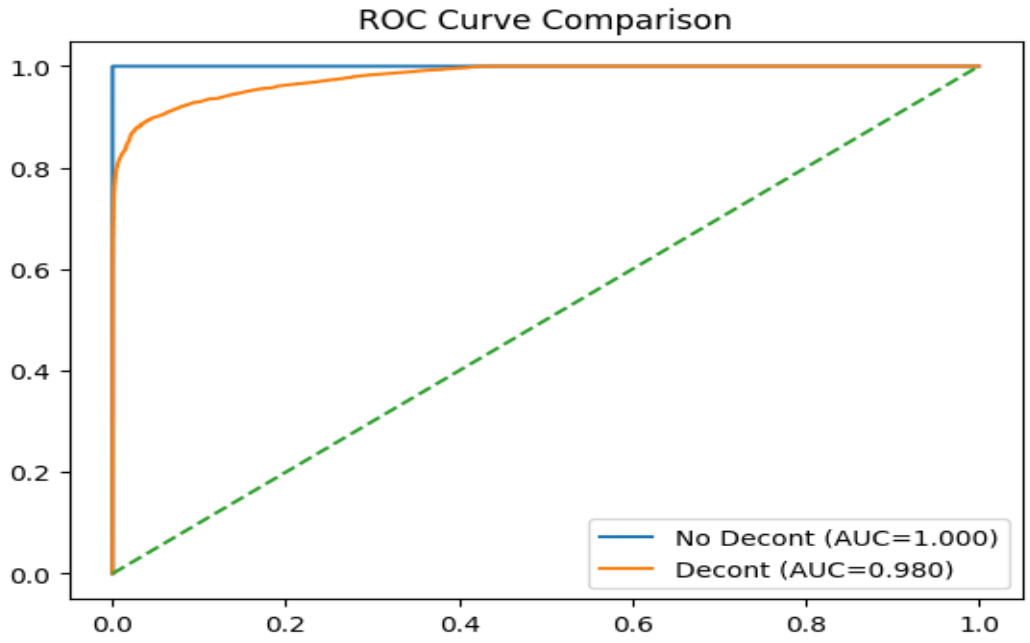
mengandung informasi label. Dengan demikian, confusion matrix pada skenario kedua lebih mencerminkan performa model yang sesungguhnya.

3.4 Analisis Kurva ROC

Perbandingan kemampuan diskriminasi model ditunjukkan pada gambar 3.2. Model tanpa proses feature decontamination menghasilkan kurva ROC yang mendekati garis ideal dengan nilai AUC sebesar 1.000. Hal ini menunjukkan kemampuan klasifikasi yang sangat tinggi, namun kembali mengindikasikan adanya bias akibat data leakage.

Sementara itu, model dengan feature decontamination menghasilkan nilai AUC sebesar 0.9795. Meskipun lebih rendah, nilai ini masih menunjukkan kemampuan diskriminasi yang sangat baik dalam membedakan antara kelas normal dan serangan.

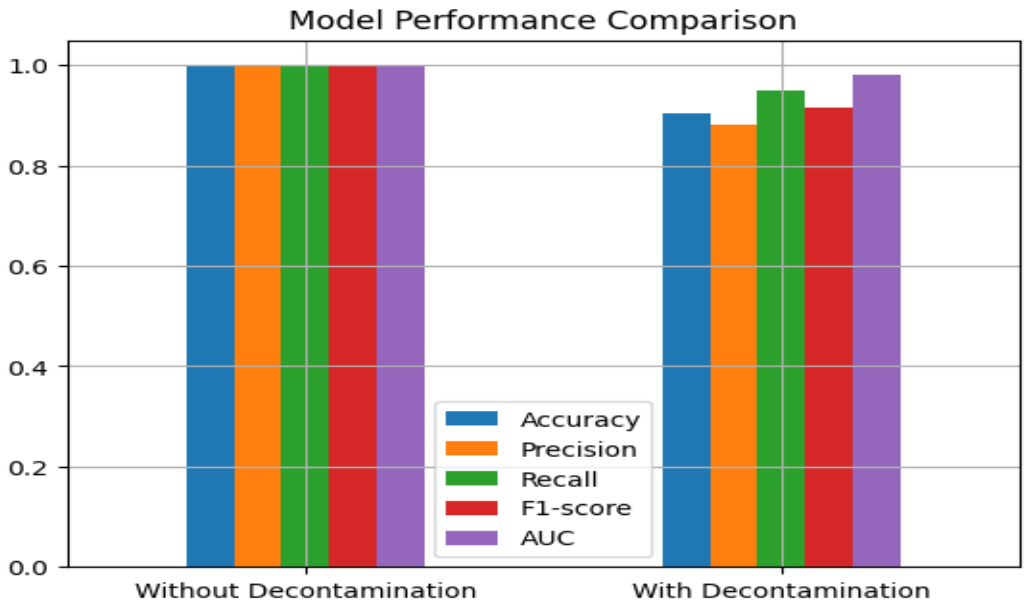
Perbedaan nilai AUC antara kedua skenario menunjukkan bahwa proses decontamination tidak menghilangkan kemampuan model, melainkan menghasilkan evaluasi yang lebih realistis dan dapat dipercaya.



Gambar 3.2 Kurva ROC Perbandingan Model Tanpa dan Dengan Feature Decontamination

3.5 Perbandingan Kinerja Model

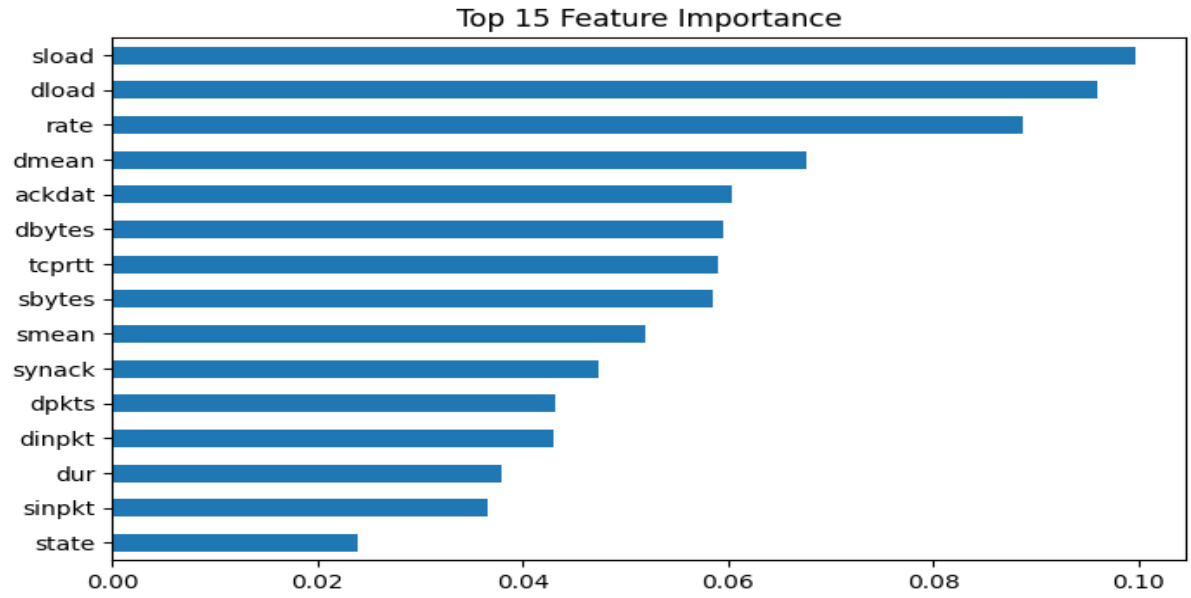
Perbandingan kinerja model pada kedua skenario ditampilkan pada gambar 3.3. Terlihat bahwa seluruh metrik pada skenario tanpa feature decontamination mencapai nilai maksimum. Namun, nilai tersebut tidak mencerminkan kemampuan model yang sebenarnya karena dipengaruhi oleh data leakage. Sebaliknya, pada skenario dengan feature decontamination, nilai metrik mengalami penurunan namun tetap berada pada tingkat yang tinggi. Hal ini menunjukkan bahwa model masih mampu mempertahankan performa yang baik tanpa bergantung pada fitur yang mengandung bias. Perbandingan ini menegaskan bahwa proses feature decontamination berperan penting dalam menghasilkan evaluasi model yang lebih valid.



Gambar 3.3 Perbandingan Nilai Accuracy, Precision, Recall, dan F1-score

3.6 Analisis Feature Importance

Kontribusi masing-masing fitur terhadap model ditunjukkan pada gambar 3.4.



Gambar 3.4 Feature Importance pada Model Random Forest Setelah Feature Decontamination

Hasil analisis menunjukkan bahwa fitur seperti sload, dload, rate, dan dmean memiliki pengaruh terbesar dalam proses klasifikasi. Fitur-fitur tersebut berkaitan dengan karakteristik lalu lintas jaringan yang relevan dalam mendeteksi aktivitas ransomware. Setelah proses feature decontamination, model lebih mengandalkan fitur-fitur yang benar-benar informatif dibandingkan fitur yang mengandung informasi implisit terhadap label. Hal ini menunjukkan

bahwa model mampu beradaptasi dan tetap menghasilkan performa yang baik meskipun beberapa fitur dihapus.

3.7 Diskusi dan Implikasi Hasil Penelitian

Berdasarkan hasil eksperimen yang telah dilakukan, proses feature decontamination terbukti memberikan pengaruh terhadap validitas performa model deteksi ransomware. Nilai evaluasi yang sangat tinggi pada skenario tanpa decontamination menunjukkan bahwa model memperoleh keuntungan dari keberadaan fitur yang memiliki keterkaitan kuat dengan label data. Kondisi tersebut menyebabkan model terlihat memiliki performa sempurna, padahal kemampuan generalisasinya belum tentu mampu merepresentasikan kondisi jaringan nyata. Temuan ini sejalan dengan penelitian Kaufman et al. (2012) yang menjelaskan bahwa data leakage dapat menghasilkan estimasi performa yang terlalu optimis pada model machine learning. Selain itu, Bouke dan Abdullah (2023) juga melaporkan bahwa keberadaan pattern leakage pada tahap praproses dapat menurunkan reliabilitas sistem deteksi intrusi karena model memanfaatkan informasi yang seharusnya tidak tersedia selama proses pembelajaran. Setelah fitur yang berpotensi menyebabkan data leakage dihapus, performa model mengalami penurunan menjadi lebih realistis. Kondisi tersebut menunjukkan bahwa model tidak lagi bergantung pada atribut yang secara implisit mengandung informasi terhadap label, tetapi mulai mempelajari karakteristik lalu lintas jaringan secara lebih representatif. Dengan demikian, hasil penelitian ini memperlihatkan bahwa kualitas fitur memiliki pengaruh besar terhadap kemampuan generalisasi model dibandingkan hanya meningkatkan kompleksitas algoritma yang digunakan. Temuan tersebut juga mendukung penelitian sebelumnya yang menyatakan bahwa pengelolaan atribut dan seleksi fitur merupakan bagian penting dalam pengembangan sistem deteksi intrusi yang stabil dan akurat (Riza, 2023).

Meskipun terjadi penurunan performa setelah proses feature decontamination, nilai recall model tetap berada pada kategori tinggi. Hal ini menunjukkan bahwa kemampuan model dalam mengenali pola serangan ransomware masih dapat dipertahankan dengan baik. Dengan kata lain, penghapusan fitur yang terkontaminasi tidak menghilangkan kemampuan utama model dalam mendeteksi aktivitas serangan, tetapi justru membantu menghasilkan evaluasi yang lebih objektif dan dapat dipercaya.

Penelitian ini juga memberikan implikasi penting bagi pengembangan sistem deteksi intrusi berbasis machine learning. Penggunaan dataset tanpa pemeriksaan integritas fitur berpotensi menghasilkan model dengan performa tinggi secara semu yang sulit diterapkan pada lingkungan nyata. Model yang terlihat sangat akurat pada tahap pengujian belum tentu mampu bekerja secara konsisten ketika dihadapkan pada karakteristik lalu lintas jaringan yang berbeda. Oleh sebab itu, proses feature decontamination perlu dipertimbangkan sebagai bagian penting dalam tahapan praproses untuk meningkatkan reliabilitas sistem deteksi ransomware.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa keberhasilan sistem deteksi intrusi tidak hanya dipengaruhi oleh pemilihan algoritma klasifikasi, tetapi juga sangat bergantung pada kualitas data dan integritas fitur yang digunakan selama proses pelatihan. Dengan demikian, evaluasi model yang realistis menjadi faktor penting agar sistem deteksi ransomware yang dikembangkan mampu bekerja lebih andal pada implementasi nyata.

4. KESIMPULAN

Penelitian ini dilakukan untuk menganalisis pengaruh feature decontamination terhadap performa deteksi ransomware menggunakan algoritma Random Forest pada dataset UNSW-NB15. Hasil eksperimen menunjukkan bahwa penggunaan seluruh fitur tanpa proses decontamination menghasilkan performa yang sangat tinggi dengan nilai akurasi, precision, recall, dan F1-score sebesar 1.000. Namun, hasil tersebut mengindikasikan adanya data leakage sehingga performa model tidak sepenuhnya merepresentasikan kemampuan deteksi yang sebenarnya.

Setelah dilakukan proses feature decontamination, performa model mengalami penurunan menjadi lebih realistis dengan nilai akurasi sebesar 0.9028, precision sebesar 0.8820, recall sebesar 0.9506, dan F1-score sebesar 0.9150. Meskipun nilai akurasi menurun, model tetap mampu mempertahankan kemampuan deteksi serangan dengan baik, terutama ditunjukkan oleh nilai recall yang tetap tinggi.

Temuan penelitian ini menunjukkan bahwa integritas fitur memiliki pengaruh yang sangat penting terhadap validitas evaluasi model machine learning pada sistem deteksi intrusi. Oleh karena itu, proses feature decontamination perlu diperhatikan untuk mengurangi bias evaluasi dan meningkatkan reliabilitas model ketika diterapkan pada kondisi jaringan nyata. Dengan demikian, penelitian ini menegaskan bahwa kualitas data dan validitas fitur merupakan faktor penting dalam pengembangan sistem deteksi ransomware yang andal dan dapat dipercaya.

5. DAFTAR PUSTAKA

Arief, M., Trisnawan, P. H., Data, M., Studi, P., Informatika, T., Komputer, F. I., & Brawijaya, U. (2017). *Implementasi Sistem Deteksi Serangan Slowloris Pada Arsitektur Jaringan Software-Defined Network*. *1*(1), 1–10.

Asbath, R. G. A., Ilpan, Anugrah, R. P., & Setiawan, A. (2025). Analisis Dampak Ransomware pada Keamanan Data Perusahaan dan Strategi Mitigasinya. *Kumpulan Ilmu Komputer Dan Perubahan Digital*, *1*(1), 17–23.

Basuki, A., & Bachtiar, F. A. (2021). Metode Deteksi Intrusi Menggunakan Algoritme Extreme Learning Machine Dengan Correlation-Based Feature Selection Intrusion Detection. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *8*(1), 103–110. https://doi.org/10.25126/jtiik.202183358

Bouke, M. A., & Abdullah, A. (2023). An empirical study of pattern leakage impact during data preprocessing on machine learning-based intrusion detection models reliability. *Expert Systems With Applications*, *230*(June), 120715. https://doi.org/10.1016/j.eswa.2023.120715

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Dong, R., Shui, Y., & Zhang, Q. (2021). *Intrusion Detection Model Based on Feature Selection and Random Forest the performance of the intrusion detection*. *23*(6), 985–996. https://doi.org/10.6633/IJNS.202111

Inayah, K., Ramli, K., Indonesia, U., Korespondensi, P., Leak, I., Activity, T., Gathering, I., Attack, W. A., & Forest, R. (2024). Analisis Kinerja Intrusion Detection System Berbasis Algoritma Performance Analysis Of Intrusion Detection System Based On Random Forest Algorithm Using Unbalanced Honeynet BSSN. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *4*(11). https://doi.org/10.25126/jtiik1148911

Kasongo, S. M., & Sun, Y. (2020). Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW - NB15 Dataset. *Journal of Big Data*. https://doi.org/10.1186/s40537-020-00379-6

Kaufman, S., Rosset, S., Perlich, C., & Stitelman, O. R. I. (2012). *Leakage in Data Mining : Formulation , Detection , and Avoidance*. *6*(4), 1–21. https://doi.org/10.1145/2382577.2382579

Kiswanto, D., Ramadhani, F., Surbakti, N. M., & Nasution, N. A. (2025). *Pengembangan dan*

Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest. *6*(3). https://doi.org/10.47065/bit.v5i2.2203

Moustafa, N., & Slay, J. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *Military Communications and Information Systems Conference (MilCIS), IEEE*, 1–6. https://doi.org/10.1109/MilCIS.2015.7348942.

Pirtama, A. (2024). Improvement Attack Detection on Internet of Things Using Principal Component Analysis and Random Forest. *Media Journal of General Computer Science*, *1*(January), 14–19. https://doi.org/10.62205/mjgcs.v1i1.8

Rabbani, S. (2023). Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer Prediction of Cyber Attack Categories with Random Forest Classification Algorithm Using Rapidminer. *SMATIKA : STIKI Informatika Jurnal*, *13*(2), 284–293.

Riza, F. (2023). Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging. *Jurnal Sistim Informasi Dan Teknologi*, *5*(1), 7–9. https://doi.org/10.37034/jsisfotek.v5i1.161

Zhang, C., Wang, W., Liu, L., Ren, J., & Wang, L. (2022). Three-Branch Random Forest Intrusion Detection Model. *Mathematics*, *10*(4460), 1–21. https://doi.org/https://doi.org/10.3390/math10234460

Zuriati, Widyawati, D. K., Arifin, O., Saputra, K., Sriyanto, & Ahmad, A. (2025). *Hybrid Machine Learning Approach for Nutrient Deficiency Detection in Lettuce*. *6*(2), 187–204. https://doi.org/10.38043/tiers.v6i2.7143