Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2785-2794
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.4.5239

Identification and Classification of Cyber Attacks on ELDIRU UNSOED using Random Forest Algorithm

Justicio Caesario*[1], Nofiyati[2], Dwi Kurnia Wibowo[3]

[1,2,3]Informatics, Universitas Jenderal Soedirman, Indonesia

Email: [1]justicio.caesario@mhs.unsoed.ac.id

Received : Aug 5, 2025; Revised : Aug 24, 2025; Accepted : Aug 27, 2025; Published : Aug 28, 2025

Abstract

Academic information systems, such as Eldiru Unsoed, function as vital digital assets vulnerable to cyberattacks, while conventional rule-based Web Application Firewalls exhibit detection weaknesses. Empirical testing in this study shows that the standard ModSecurity with Core Rule Set (CRS) system achieves a recall of only 5.34%, meaning it fails to identify the majority of actual attacks and creates a significant security gap. To address this problem, this research designs a detection system based on the Random Forest algorithm using Nginx server log data, validated with the public CSIC 2010 dataset. The model was developed by engineering hybrid features that include lexical analysis, CRS rule context, and N-grams to classify web traffic. Evaluation results show the proposed Machine Learning-Random Forest (ML-RF) model successfully increases recall from 5.34% to 72.00% and the F1-Score from 10.10% to 80.00%. This improvement in metrics, while maintaining a precision of 91.00%, proves that machine learning integration yields a more balanced and reliable cybersecurity defense mechanism. This research underscores the importance of implementing MLOps workflows for continuous model calibration and retraining to maintain detection effectiveness against evolving threats.

Keywords : *Cyber Security, Machine Learning, Random Forest, Web Application, Web Application Firewall*

1. INTRODUCTION

Keamanan siber telah menjadi aspek fundamental dalam era digital untuk melindungi sistem komputer, jaringan, dan data dari berbagai ancaman siber guna menjaga kerahasiaan, integritas, dan ketersediaan informasi [1], [2]. Seiring meningkatnya ketergantungan pada teknologi digital di berbagai sektor, termasuk institusi pendidikan, penerapan keamanan siber yang efektif menjadi semakin krusial [3], [4]. Sistem Informasi Akademik (SIA) seperti Eldiru di Universitas Jenderal Soedirman merupakan aset digital vital yang menyimpan data sensitif mahasiswa dan dosen [5], sehingga keamanan dan ketersediaannya harus menjadi prioritas utama [6].

Seiring dengan meluasnya pemakaian internet, risiko terhadap ancaman seperti peretasan, *malware*, dan pencurian identitas juga turut meningkat [7]. Kondisi ini menuntut adanya mekanisme pertahanan yang kuat pada lapisan aplikasi web [8]. Implementasi *Web Application Firewall* (WAF) menjadi salah satu strategi pertahanan standar untuk memonitor, memfilter, dan memblokir data berbahaya yang masuk ke aplikasi web [9], [10]. Di banyak lingkungan produksi, WAF yang umum digunakan adalah ModSecurity dengan *OWASP Core Rule Set* (CRS), yang berfungsi sebagai lapisan pertahanan pertama [11], [12].

Dalam konteks operasional, keandalan SIA seperti Eldiru sangat krusial. Gangguan yang disebabkan oleh serangan siber tidak hanya berpotensi menimbulkan kerugian finansial, tetapi juga dapat menyebabkan penurunan reputasi institusi serta disrupsi pada kegiatan akademik yang fundamental [13], [14]. Oleh karena itu, efektivitas sistem keamanan yang diimplementasikan harus

dievaluasi secara berkelanjutan untuk memastikan kemampuannya dalam menghadapi lanskap ancaman yang terus berevolusi [15].

Meskipun demikian, salah satu tantangan utama pada sistem pertahanan standar adalah ketergantungannya pada aturan statis yang kaku [16], [17]. Sistem berbasis aturan seperti ModSecurity-CRS seringkali kesulitan dalam mengenali variasi serangan baru atau teknik penyamaran (*obfuscation*) [18], [19], sehingga banyak serangan dapat lolos tanpa terdeteksi [20]. Pengujian empiris yang dilakukan dalam penelitian ini mengidentifikasi kelemahan fatal tersebut: sistem ModSecurity-CRS standar terbukti hanya memiliki tingkat recall sebesar 5.34%, yang berarti sistem ini gagal mengidentifikasi lebih dari 94% serangan aktual dan menciptakan celah keamanan yang sangat signifikan.

Untuk mengatasi permasalahan tersebut, diperlukan suatu pendekatan yang lebih objektif, cerdas, dan berbasis data [21], [22]. Penelitian ini mengusulkan penerapan algoritma *Machine Learning* Random Forest sebagai metode untuk membangun sistem deteksi yang lebih andal [23]. Pendekatan ini memanfaatkan log server Nginx sebagai data historis untuk melatih model dalam mengenali pola lalu lintas yang normal dan anomali[24], [25]. Sistem yang diusulkan dirancang dengan merekayasa fitur-fitur hibrida yang mencakup analisis leksikal, konteks dari aturan CRS, dan N-gram untuk mengklasifikasikan lalu lintas web secara akurat.

Tujuan utama dari penelitian ini adalah merancang, mengimplementasikan, dan mengevaluasi sebuah sistem deteksi hibrida (ModSec-RF) yang secara signifikan lebih efektif dan seimbang dibandingkan dengan implementasi ModSecurity-CRS standar. Dengan sistem berbasis *machine learning* ini, diharapkan mekanisme pertahanan siber pada sistem Eldiru mampu memberikan deteksi yang lebih andal terhadap ancaman modern yang dinamis. Pada akhirnya, pendekatan ini diharapkan dapat memperkuat postur keamanan aset digital institusi di tengah lanskap ancaman siber yang terus berkembang.

2. METHOD

Penelitian ini menerapkan pendekatan metodologi yang sistematis untuk merancang, membangun, dan mengevaluasi sistem deteksi serangan siber hibrida, dengan kerangka kerja yang mengacu pada panduan dari *National Institute of Standards and Technology* (NIST) [26]. Pengembangan model deteksi dilakukan menggunakan algoritma *ensemble learning Random Forest* yang dirancang untuk mengklasifikasikan lalu lintas web berdasarkan fitur-fitur yang diekstraksi dari log server.

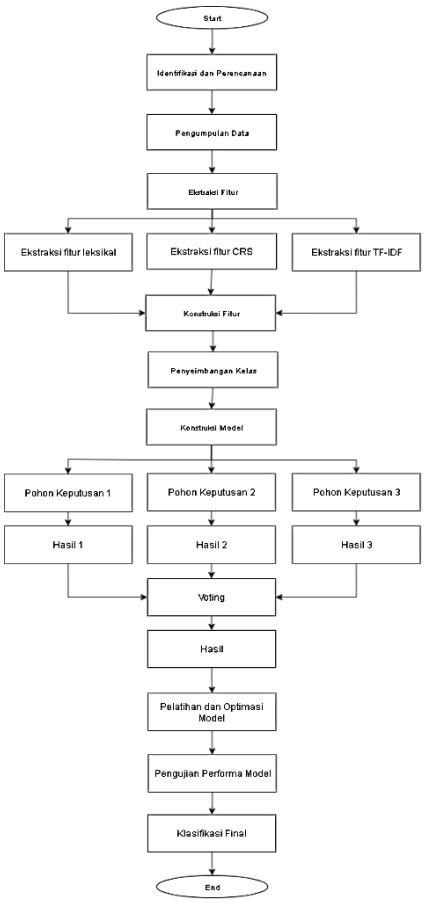
2.1. Metodologi Penelitian

Metodologi penelitian ini disusun secara sistematis dengan mengacu pada kerangka kerja NIST SP 800-53 Rev. 5, sebuah standar yang menyediakan katalog kontrol keamanan dan privasi komprehensif yang sering diadopsi dalam praktik industri, khususnya pada keluarga kontrol SI-4 (*System and Communications Protections*). Proses ini terdiri dari enam tahapan utama yang dirancang secara berurutan untuk memastikan hasil yang valid dan dapat direproduksi, seperti yang diilustrasikan pada Gambar 1.

Gambar 1 diatas menyajikan diagram alur metodologi penelitian secara visual. Proses diawali dengan tahap Identifikasi dan Perencanaan, di mana kelemahan fundamental pada WAF berbasis aturan dianalisis sebagai justifikasi masalah.

Tahap selanjutnya adalah Pengumpulan Data, yang meliputi agregasi log server Nginx dan dataset publik. Setelah data terkumpul, proses dilanjutkan dengan Rekayasa Fitur untuk mentransformasi data mentah menjadi format numerik.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2785-2794
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.4.5239



Gambar 1. Diagram alur penelitian

Proses ini berlanjut secara sekuensial ke Konstruksi Model, Evaluasi dan Perbandingan, hingga tahap akhir yaitu Implementasi, Analisis, dan Klasifikasi pada data riil.

a. Identifikasi dan Perencanaan: Berfokus pada analisis masalah tingginya false negative pada WAF berbasis aturan, selaras dengan kerangka perencanaan pemantauan NIST SP 800-53, SI-4.
b. Pengumpulan Data: Meliputi pengumpulan log Nginx Eldiru dan dataset publik untuk validasi, yang mengimplementasikan kontrol NIST SP 800-53, SI-4(5).
c. Rekayasa Fitur: Merupakan proses transformasi data log mentah menjadi format numerik terstruktur untuk dianalisis oleh algoritma, sesuai dengan prinsip NIST SP 800-53, SI-4(2).
d. Konstruksi Model: Mencakup pelabelan, penyeimbangan kelas, serta pelatihan dan optimasi model Random Forest sebagai kelanjutan dari implementasi NIST SP 800-53, SI-4(2).
e. Evaluasi dan Perbandingan: Merupakan pengujian kuantitatif untuk membandingkan performa model ModSec-RF dengan sistem standar ModSecurity-CRS, selaras dengan kontrol NIST SP 800-53, SI-4(14).
f. Implementasi, Analisis, dan Klasifikasi: Adalah tahap akhir penerapan model pada data riil Eldiru yang tidak berlabel untuk mendemonstrasikan kapabilitas sistem dan menganalisis temuan.

2.2. Algoritma Random Forest

Random Forest adalah algoritma *ensemble learning* yang menggunakan metode pemisahan biner secara rekursif untuk mencapai simpul terminal dalam struktur pohon, berdasarkan pada pohon klasifikasi dan pohon regresi [27]. Algoritma ini bekerja dengan membangun sejumlah besar pohon keputusan pada saat pelatihan [28]. Untuk melakukan klasifikasi, hasil akhir ditentukan melalui pemungutan suara mayoritas dari semua prediksi pohon keputusan individu yang telah dibangun [29].

P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.4.5239

Setiap pohon dalam Random Forest dilatih pada sampel data yang dipilih secara acak dengan penggantian (*bootstrap sample*) dari *dataset* pelatihan[30]. Selain itu, pada setiap pemisahan simpul (*node split*), algoritma hanya mempertimbangkan sebagian kecil fitur yang dipilih secara acak[31]. Pendekatan ganda ini (*randomisasi* pada level data dan fitur) berfungsi untuk mengurangi varians model dan mencegah overfitting [32], yang merupakan masalah umum pada algoritma pohon keputusan tunggal [33]. Algoritma ini dipilih karena beberapa kelebihannya, seperti kemampuan untuk menghasilkan tingkat kesalahan yang relatif rendah[34], kinerja klasifikasi yang optimal [35], efisiensi dalam menangani data pelatihan dalam jumlah besar [36], serta efektif dalam memperkirakan data yang hilang[37].

3. RESULT

Bagian ini menyajikan hasil yang diperoleh dari seluruh tahapan penelitian secara sistematis. Setiap sub-bagian di bawah ini menguraikan temuan dan hasil implementasi dari setiap tahapan metodologi yang telah dijelaskan pada bab sebelumnya, mulai dari identifikasi masalah hingga evaluasi dan analisis akhir. Penyajian hasil mencakup data kuantitatif dari evaluasi komparatif, visualisasi untuk interpretasi model, serta temuan dari penerapan sistem pada data riil.

3.1. Identifikasi dan Perencanaan

Tahap awal mengidentifikasi masalah fundamental pada sistem pertahanan WAF yang ada di sistem Eldiru. Pengujian empiris terhadap implementasi ModSecurity dengan *OWASP Core Rule Set* (CRS) standar menunjukkan tingkat presisi yang tinggi namun dengan tingkat *recall* yang sangat rendah, yaitu hanya 5.34%. Hal ini mengindikasikan bahwa lebih dari 94% serangan yang sebenarnya gagal terdeteksi oleh sistem berbasis aturan. Kelemahan fatal inilah yang menjadi justifikasi utama untuk merancang sebuah solusi hibrida yang mengintegrasikan machine learning untuk meningkatkan kapabilitas deteksi secara signifikan.

3.2. Pengumpulan Data

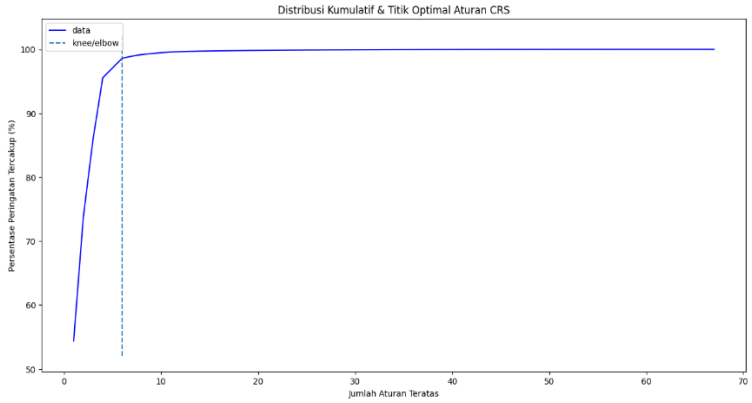
Tahap pengumpulan data diawali dengan akuisisi data primer yang terdiri dari 77.886.413 entri access.log dari server web Nginx sistem Eldiru. Sampel acak sejumlah 10 juta entri diekstraksi dari log ini untuk dilabeli secara otomatis dengan Core Rule Set (CRS). Setiap transaksi yang memicu aturan dicatat dalam audit.log, yang kemudian berfungsi sebagai *dataset* latih (training dataset) utama dalam penelitian ini. Untuk keperluan pengujian dan validasi, *dataset publik* (CSIC 2010 dan ECML/PKDD 2007) juga berhasil diproses dan dipartisi. Proses ini menghasilkan 59.469 baris data yang dialokasikan untuk pengayaan data latih dan 25.488 baris data yang disimpan sebagai data uji simpanan (*holdout set*) untuk evaluasi akhir.

3.3. Rekayasa Fitur

Pada tahap ini, data mentah berhasil ditransformasikan menjadi format numerik terstruktur. Seleksi fitur otomatis pada aturan CRS menggunakan "titik siku" (*elbow method*) menghasilkan rekomendasi untuk menggunakan 6 aturan teratas yang paling informatif, yang telah mencakup 98.60% dari total semua peringatan. Hasil dari analisis ini divisualisasikan pada Gambar 2.

Selanjutnya, untuk mengatasi masalah ketidakseimbangan kelas, teknik *RandomUnderSampler* diterapkan. Proses ini berhasil mengubah distribusi kelas pada data latih dari kondisi sangat tidak seimbang (490.406 Normal vs. 97.685 Anomali) menjadi rasio yang lebih seimbang (195.370 Normal vs. 97.685 Anomali), yang krusial untuk mencegah model menjadi bias.

Vol. 6, No. 4, August 2025, Page. 2785-2794
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.4.5239



Gambar 2. Hasil Seleksi Fitur Otomatis Aturan CRS

3.4. Konstruksi Model

Tahap pemodelan berfokus pada pelatihan dan optimasi model *Random Forest*. Proses pencarian hiperparameter menggunakan RandomizedSearchCV berhasil mengidentifikasi konfigurasi model terbaik. Hasil dari proses ini menunjukkan bahwa parameter optimal yang ditemukan adalah n_estimators: 186 dan max_depth: None. Model dengan konfigurasi inilah yang kemudian digunakan untuk semua proses evaluasi dan implementasi selanjutnya.

3.5. Evaluasi dan Perbandingan

Tahap ini merupakan inti dari pembuktian hipotesis penelitian. Performa model ModSec-RF yang diusulkan dibandingkan secara langsung dengan sistem ModSecurity-CRS standar pada 25.488 data uji. Hasil dari perbandingan kuantitatif tersebut disajikan dalam bentuk matriks konfusi pada Tabel 1 dan Tabel 2.

Tabel 1. Matriks Konfusi ModSec-CRS

	Prediksi:Anomali	Prediksi:Valid	Total Aktual
Aktual:Anomali	621 (TP)	11.019 (FN)	11.640
Aktual:Valid	32 (FP)	13.816 (TN)	13.848
Total Prediksi	653	24.835	25.488

Tabel 2. Matriks Konfusi ModSec-RF

	Prediksi:Anomali	Prediksi:Valid	Total Aktual
Aktual:Anomali	8,381 (TP)	3,259 (FN)	11.640
Aktual:Valid	831 (FP)	13.017 (TN)	13.848
Total Prediksi	9212	16.276	25.488

Rekapitulasi metrik kinerja utama dari kedua sistem disajikan pada Tabel 4 . Hasil ini menunjukkan peningkatan performa yang sangat signifikan pada model ML-RF .

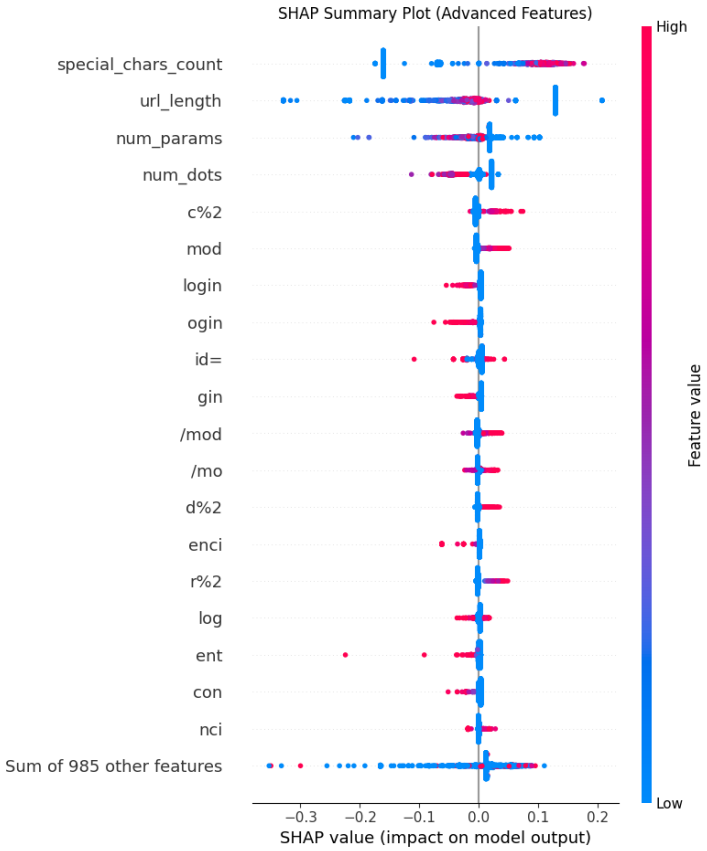
Recall melonjak drastis dari 5.34% menjadi 72.00%, yang berarti model mampu mengidentifikasi sebagian besar serangan yang sebelumnya terlewatkan. Keseimbangan antara *precision* dan *recall* ini tercermin pada F1-Score yang meningkat dari 10.10% menjadi 80.00%, membuktikan bahwa sistem ML-RF secara keseluruhan jauh lebih andal dan efektif.

Vol. 6, No. 4, August 2025, Page. 2785-2794
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.4.5239

Tabel 3. Perbandingan Metrik

Metrik	ModSec-CRS	ML-RF
Precision	95.10%	91.00%
Recall	5.34%	72.00%
F1-Score	10.10%	80.00%
False Positive Rate	0.23%	6.00%
Accuracy	56.64%	84.00%

Untuk memahami dasar pengambilan keputusan model, analisis interpretasi menggunakan SHAP dilakukan dan hasilnya disajikan pada Gambar 3 . Plot ini mengonfirmasi bahwa model mempelajari pola yang relevan, di mana fitur leksikal seperti special_chars_count dan url_length menjadi prediktor paling berpengaruh, sesuai dengan karakteristik umum serangan aplikasi web.



Gambar 3. Visualisasi Plot Ringkasan SHAP

3.6. Implementasi, Analisis, dan Klasifikasi

Pada tahap akhir, model yang telah tervalidasi diterapkan pada sekitar satu juta transaksi unik dari log riil Eldiru. Hasilnya, sistem berhasil mengklasifikasikan 21.430 (2.14%) transaksi sebagai anomali.

Untuk memahami karakteristik anomali yang terdeteksi, dilakukan analisis lebih lanjut. Pertama, anomali yang tidak hanya dideteksi oleh model ML tetapi juga memicu aturan ModSecurity-CRS dipetakan ke dalam kategori serangan spesifik.

Tabel 4. Distribusi Klasifikasi Final pada Data Rill Eldiru

Klasifikasi	Jumlah	Persentase
Normal	978.456	97.86%
Anomali	21.430	2.14%
Total	999.888	100.00%

Proses pemetaan ini dilakukan dengan menganalisis ID aturan CRS yang terpicu, di mana setiap ID aturann memiliki tag yang berkorespondensi langsung dengan kategori dalam OWASP TOP Ten. Sisa anomali lainnya yang tidak memicu aturan CRS dikelompokkan ke dalam kategori ML. Hasil dari klasifikasi mendalam ini disajikan pada Tabel 5.

Tabel 5. Kategori OWASP pada Anomali yang Terdeteksi

Kategori OWASP	Jumlah	Persentase
ML	13.436	62.7%
A01 Broken Access Control	5.542	25.9%
A05 Security Misconfiguration	1.561 |	7.3%
A03 Injection	891	4.1%

4. DISCUSSIONS

Hasil penelitian yang telah disajikan pada bab sebelumnya menunjukkan perbedaan kinerja yang fundamental antara pendekatan deteksi berbasis aturan statis dan pendekatan berbasis *machine learning*. Analisis pada Tabel 3 secara jelas menggarisbawahi kelemahan utama dari sistem ModSecurity-CRS standar, yaitu ketidakseimbangan performa. Tingkat *precision* yang sangat tinggi (95.10%) dicapai dengan mengorbankan *recall* secara drastis, yang hanya mencapai 5.34%. Dalam konteks keamanan siber, metrik *recall* yang rendah mengindikasikan bahwa sistem gagal mengidentifikasi mayoritas ancaman aktual, sehingga menjadikannya tidak efektif sebagai sistem perlindungan yang komprehensif.

Sebaliknya, model ModSec-RF yang diusulkan berhasil mengatasi masalah ini dengan mencapai keseimbangan yang jauh lebih baik antara *precision* dan *recall*. Peningkatan *recall* yang masif menjadi 72.00% merupakan pencapaian paling signifikan. Hal tersebut menunjukkan kemampuan model untuk melakukan generalisasi dan mengidentifikasi pola-pola serangan kompleks yang lolos dari deteksi aturan statis. Keseimbangan performa ini divalidasi oleh nilai *F1-Score* yang meningkat secara signifikan dari 10.10% menjadi 80.00%, yang membuktikan bahwa sistem berbasis *machine learning* secara keseluruhan lebih andal dan efektif.

Analisis interpretasi model menggunakan SHAP (Gambar 3) memberikan justifikasi logis terhadap kinerja model dan memastikan bahwa model tidak beroperasi sebagai "kotak hitam". Kontribusi tinggi dari fitur leksikal seperti special_chars_count dan url_length menunjukkan bahwa model telah berhasil mempelajari pola-pola yang secara semantik relevan dengan karakteristik serangan aplikasi web. *Payload* serangan seperti *Cross-Site Scripting* (XSS) dan *SQL Injection* seringkali memanipulasi properti-properti tersebut, sehingga signifikansi fitur ini dalam model mengonfirmasi bahwa proses pembelajaran berjalan dengan baik.

Implementasi model pada data riil menyoroti potensi sekaligus tantangan dalam aplikasi praktis. Dominasi kategori yang hanya dapat terdeteksi oleh model sebesar 62.7% (Tabel 5) menunjukkan kekuatan model dalam mendeteksi anomali yang tidak memiliki *signature* yang jelas untuk memicu aturan CRS. Hal ini dapat diinterpretasikan sebagai keberhasilan dalam mendeteksi aktivitas pemindaian (*scanning*) ataupun serangan. Namun, kategori ini juga dapat mengindikasikan adanya potensi *false positive* terhadap lalu lintas yang sah namun jarang terjadi dan kurang terwakili dalam data latih. Fenomena ini menegaskan bahwa meskipun otomatisasi *machine learning* sangat kuat,

validasi oleh manusia dan kalibrasi berkelanjutan tetap diperlukan dalam lingkungan produksi untuk menyempurnakan ambang batas deteksi. Proses ini melibatkan beberapa langkah praktis seperti analis keamanan secara periodik mengambil sampel dari anomali yang terdeteksi oleh model, analisis verifikasi manual untuk membedakan antara serangan nyata (*true positive*) dan lalu lintas yang sah (*false positive*). Dapat juga dilakukan umpan balik dari hasil verifikasi untuk digunakan sebagai data latih tambahan untuk melatih ulang (*retrain*) model secara berkala. Melalui siklus umpan balik ini, ambang batas deteksi model dapat disempurnakan secara adaptif, sehingga akurasinya meningkat dan tingkat *false positive* dapat ditekan seiring waktu.

5. CONCLUSION

Berdasarkan hasil implementasi dan evaluasi empiris yang telah dipaparkan pada sistem informasi akademik Eldiru Unsoed, penelitian ini menghasilkan beberapa kesimpulan utama. Pertama, penelitian ini berhasil menerapkan sebuah pendekatan deteksi hibrida yang mengombinasikan analisis fitur leksikal, konteks dari aturan OWASP CRS, dan representasi N-gram untuk membangun model klasifikasi Random Forest yang akurat dan dapat diinterpretasikan. Kedua, sistem berbasis machine learning (ML-RF) yang diusulkan menunjukkan performa yang secara signifikan lebih unggul dibandingkan implementasi standar ModSecurity dengan CRS dalam konteks pengamanan aplikasi web Eldiru. Keunggulan tersebut dibuktikan oleh peningkatan *F1-Score* dari 10.10% menjadi 80.00% dan metrik *recall* dari 5.34% menjadi 72.00%, yang menegaskan bahwa pendekatan ini mampu menghasilkan sistem deteksi yang lebih seimbang dan efektif secara keseluruhan. Ketiga, penerapan pada data riil dari log server Eldiru menunjukkan kemampuan model untuk mengidentifikasi ancaman yang lolos dari deteksi berbasis aturan, meskipun dominasi kategori anomali yang hanya terdeteksi oleh *machine learning* menyoroti potensi ambiguitas hasil yang memerlukan validasi lebih lanjut.

Berdasarkan temuan dan keterbatasan yang teridentifikasi selama penelitian, beberapa saran diajukan untuk arah penelitian selanjutnya guna meningkatkan postur keamanan siber sistem Eldiru. Saran tersebut mencakup perlunya melakukan validasi dan kalibrasi secara mendalam terhadap kategori deteksi yang hanya ditemukan oleh model *machine learning* untuk membedakan secara akurat antara ancaman nyata dan *false positive*. Selain itu, direkomendasikan untuk memperluas kapabilitas pemetaan kategori serangan dengan mengintegrasikan sumber data tambahan seperti hasil pemindaian keamanan aplikasi. Terakhir, untuk menjaga relevansi model dalam jangka panjang, disarankan untuk mengimplementasikan alur kerja MLOps (Machine Learning Operations) untuk pelatihan ulang model secara berkala serta memperluas cakupan pengujian untuk mengukur ketahanan model terhadap adversarial attacks. Implementasi saran-saran ini diharapkan dapat memperkuat mekanisme pertahanan Eldiru Unsoed secara berkelanjutan terhadap lanskap ancaman siber yang dinamis.

CONFLICT OF INTEREST

Penulis menyatakan bahwa tidak terdapat konflik kepentingan, baik antarpenulis maupun dengan objek penelitian dalam artikel ini.

REFERENCES

[1] E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.

[2] R. Ali, A. Ali, F. Iqbal, A. M. Khattak, and S. Aleem, "A Systematic Review of Artificial Intelligence and Machine Learning Techniques for Cyber Security," *Commun. Comput. Inf. Sci.*, vol. 1210 CCIS, no. October, pp. 584–593, 2020, doi: 10.1007/978-981-15-7530-3_44.

Vol. 6, No. 4, August 2025, Page. 2785-2794
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.4.5239

[3] A. K. B. Arnob, R. R. Chowdhury, N. A. Chaiti, S. Saha, and A. Roy, "A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions," *J. Edge Comput.*, vol. 4, no. 1, pp. 73–104, 2025, doi: 10.55056/jec.885.

[4] D. Oktareza, A. Noor, E. Saputra, and ..., "Transformasi Digital 4.0: Inovasi yang Menggerakkan Perubahan Global," *CENDEKIA J. Hukum, Sos. Hum.*, vol. 2, no. 3, pp. 661–672, 2024, [Online]. Available: https://journal.lps2h.com/cendekia/article/view/98%0Ahttps://journal.lps2h.com/cendekia/article/download/98/78

[5] R. Yandra, Mahfudnurnajamuddin, and Suriyanti, "Implementasi Teknologi dalam Manajemen Pemasaran Pendidikan: Tantangan dan Peluang," *J. Educ. Res.*, vol. 5, no. 2, pp. 2008–2024, 2024, doi: 10.37985/jer.v5i2.1071.

[6] M. F. Aska, D. P. Putta, and C. J. M. Sinambela, "Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital," *J. Inf. Inf. Secur.*, vol. 5, no. 2, pp. 187–200, 2024, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty

[7] M. E. Durmu, "Web application firewall based on machine learning models," no. July, 2025, doi: 10.7717/peerj-cs.2975.

[8] R. Z. Muttaqin and D. Sudiana, "Design of Realtime Web Application Firewall on Deep Learning-Based to Improve Web Application Security," *J. Penelit. Pendidik. IPA*, vol. 10, no. 12, pp. 11121–11129, 2025, doi: 10.29303/jppipa.v10i12.8346.

[9] M. O. Musa and T. Victor-Ime, "Improving Internet Firewall Using Machine Learning Techniques," *Am. J. Comput. Sci. Technol.*, no. June, 2023, doi: 10.11648/j.ajcst.20230604.14.

[10] N. A. Widiyono and U. Y. Oktiawati, "Implementasi Web Application Firewall (WAF) pada Aplikasi Fishku Berbasis Google Cloud Armor," *J. Internet Softw. Eng.*, vol. 5, no. 2, pp. 75–85, 2024, doi: 10.22146/jise.v5i2.9980.

[11] A. Rosyida Zain, I. Muhamad, M. Matin, and D. K. Kautsar, "Analisis Implementasi Modsecurity dan Reverse Proxy Untuk Pencegahan Serangan Keamanan DDoS pada Web Server," *SNIV Semin. Nas. Inov. Vokasi*, vol. 2, no. 1, pp. 118–127, 2023.

[12] A. Blozva *et al.*, "IoT devices Integration and Protection in Available Infrastructure of a University Computer Network," *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 8, pp. 1820–1833, 2021.

[13] Z. Y. Gunibala, S. N. Maharani, and S. Pujiningsih, "Dampak Finansial Serangan Siber Terhadap Kinerja Korporasi: Scoping Review," *J. Daya Saing*, vol. 11, no. 2, pp. 493–501, 2025, doi: 10.35446/dayasaing.v11i2.2245.

[14] Faizal, "Pengaruh Serangan Siber Ransomware yang Menyerang Pusat Data Nasional Terhadap Persepsi dan Kepercayaan Masyarakat Kota Semarang pada Kominfo," 2025.

[15] I. Ahmad, Q. E. U. Haq, M. Imran, M. O. Alassafi, and R. A. Alghamdi, "An Efficient Network Intrusion Detection and Classification System," *Mathematics*, vol. 10, no. 3, pp. 1–15, 2022, doi: 10.3390/math10030530.

[16] L. Demetrio, A. Valenza, G. Costa, and G. Lagorio, "WAF-A-MoLE: Evading web application firewalls through adversarial machine learning," *Proc. ACM Symp. Appl. Comput.*, pp. 1745–1752, 2020, doi: 10.1145/3341105.3373962.

[17] Amirah and F. Karimah, "Preliminary Study for Cyber Intrusion Detection Using Machine Learning Approach," *J. Sist. Inf. dan Tek. Inform.*, vol. 1, no. 1, pp. 28–33, 2023, doi: 10.70356/jafotik.v1i1.4.

[18] G. Floris *et al.*, "ModSec-AdvLearn: Countering Adversarial SQL Injections With Robust Machine Learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 20, pp. 6693–6705, 2025, doi: 10.1109/TIFS.2025.3583234.

[19] V. Lakhno *et al.*, "Experimental Studies of the Features of Using WAF To Protect Internal Services in the Zero Trust Structure," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 3, pp. 705–721, 2022.

[20] Z. Benamor, Z. A. Seghir, M. Djezzar, and M. Hemam, "A comparative study of machine learning algorithms for intrusion detection in IoT networks," *Rev. d'Intelligence Artif.*, vol. 37, no. 3, pp. 567–576, 2023, doi: 10.18280/ria.370305.

Vol. 6, No. 4, August 2025, Page. 2785-2794
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.4.5239

[21] K. H. Hamzah, M. Z. Osman, T. Anthony, M. A. Ismail, Z. Abdullah, and A. Alanda, "Comparative Analysis of Machine Learning Algorithms for Cross-Site Scripting (XSS) Attack Detection," *Int. J. Informatics Vis.*, vol. 8, no. 3–2, pp. 1678–1685, 2024, doi: 10.62527/joiv.8.3-2.3451.

[22] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, vol. 11, no. August, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[23] C. Lu, Y. Cao, and Z. Wang, "Research on Intrusion Detection Based on an Enhanced Random Forest Algorithm," *Appl. Sci.*, vol. 14, no. 2, 2024, doi: 10.3390/app14020714.

[24] A. Yudhistira and Y. Fitrisia, "Monitoring Log Server Dengan Elasticsearch, Logstash Dan Kibana (ELK)," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 124–134, 2023, doi: 10.36341/rabit.v8i1.2975.

[25] Rio Pradana Aji, "Analisis Log Serangan Bruteforce Terhadap Web Server Nginx Pada Dasbor Sistem Pencatatan Log Teroptimasi Menggunakan Metode Investigasi Forensik," *Univ. Islam Indones.*, pp. 4–95, 2022.

[26] NIST SP800-53, "Security and Privacy Controls for Information Systems and Organizations," *NIST Spec. Publ.*, p. 465, 2020, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[27] M. Fahri, "Penerapan Algoritma Random Forest untuk Deteksi Phishing pada Website," *J. Ilm. Teknol. Sist. Inf.*, vol. 6, no. 2, pp. 186–194, 2025, doi: 10.62527/jitsi.6.2.472.

[28] A. D. Purwanto, K. Wikantika, A. Deliar, and S. Darmawan, "Decision Tree and Random Forest Classification Algorithms for Mangrove Forest Mapping in Sembilang National Park, Indonesia," *Remote Sens.*, vol. 15, no. 1, 2023, doi: 10.3390/rs15010016.

[29] S. Amini, M. Saber, H. Rabiei-Dastjerdi, and S. Homayouni, "Urban Land Use and Land Cover Change Analysis Using Random Forest Classification of Landsat Time Series," *Remote Sens.*, vol. 14, no. 11, pp. 1–23, 2022, doi: 10.3390/rs14112654.

[30] J. Svoboda, P. Štych, J. Laštovička, D. Paluba, and N. Kobliuk, "Random Forest Classification of Land Use, Land-Use Change and Forestry (LULUCF) Using Sentinel-2 Data—A Case Study of Czechia," *Remote Sens.*, vol. 14, no. 5, 2022, doi: 10.3390/rs14051189.

[31] M. S. Chowdhury, "Comparison of accuracy and reliability of random forest, support vector machine, artificial neural network and maximum likelihood method in land use/cover classification of urban setting," *Environ. Challenges*, vol. 14, no. October 2023, p. 100800, 2024, doi: 10.1016/j.envc.2023.100800.

[32] E. Fevid, C. Walsh, and L. Russo, "Zero-Day Ransomware Detection via Assembly Language Bytecode Analysis and Random Forest Classification," 2024.

[33] H. Dabiri, V. Farhangi, M. J. Moradi, M. Zadehmohamad, and M. Karakouzian, "Applications of Decision Tree and Random Forest as Tree-Based Machine Learning Techniques for Analyzing the Ultimate Strain of Spliced and Non-Spliced Reinforcement Bars," *Appl. Sci.*, vol. 12, no. 10, pp. 1–13, 2022, doi: 10.3390/app12104851.

[34] H. A. Salman, A. Kalakech, and A. Steiti, "Random Forest Algorithm Overview," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 69–79, 2024, doi: 10.58496/bjml/2024/007.

[35] M. M. Abualhaj, M. Al-Zyoud, A. Alsaaidah, A. Abu-Shareha, and S. Al-Khatib, "Enhancing Malware Detection through Self-Union Feature Selection Using Firefly Algorithm with Random Forest Classification," *Int. J. Intell. Eng. Syst.*, vol. 17, no. 4, pp. 376–389, 2024, doi: 10.22266/IJIES2024.0831.29.

[36] J. L. Solorio-Ramírez, R. Jiménez-Cruz, Y. Villuendas-Rey, and C. Yáñez-Márquez, "Random forest Algorithm for the Classification of Spectral Data of Astronomical Objects," *Algorithms*, vol. 16, no. 6, 2023, doi: 10.3390/a16060293.

[37] H. Fei *et al.*, "Cotton Classification Method at the County Scale Based on Multi-Features and Random Forest Feature Selection Algorithm and Classifier," *Remote Sens.*, vol. 14, no. 4, 2022, doi: 10.3390/rs14040829.