BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

ANALISIS KOMPARASI ALGORITMA MACHINE LEARNING DALAM MITIGASI SERANGAN SIBER PADA WEB SERVER UNIVERSITAS MUHAMMADIYAH ACEH

[1]Zahrul Maizi
([1]Universitas Muhammadiyah Aceh)
Korespondensi: zahrulmaizi@unmuha.ac.id

Abstrak

Infrastruktur digital Universitas Muhammadiyah Aceh (UNMUHA) yang dikelola melalui mekanisme *centralized hosting* menghadapi tantangan serius berupa ancaman serangan siber yang berulang, dampak dari serangan ini tidak hanya menyebabkan kegagalan layanan (*downtime*), tetapi juga berakibat pada pemblokiran (*banned*) domain institusi oleh sistem keamanan vendor dan mesin pencari global. Penelitian ini bertujuan untuk menganalisis komparasi performa algoritma *Random Forest* (RF), *K-Nearest Neighbor* (KNN), dan *Support Vector Machine* (SVM) dalam memitigasi serangan siber menggunakan data *log* akses riil dari peladen unmuha.ac.id. Metode penelitian menggunakan kerangka kerja CRISP-DM dengan evaluasi berbasis *confusion matrix*. Hasil eksperimen menunjukkan bahwa Random Forest memiliki tingkat akurasi dan presisi tertinggi sebesar 99,46%, menjadikannya algoritma paling andal untuk klasifikasi serangan. Namun, dari aspek efisiensi, KNN menunjukkan performa luar biasa dengan waktu eksekusi hanya 0,2124 detik, yang mana hampir 4.000 kali lebih cepat dibandingkan SVM (842,99 detik). Penelitian ini menyimpulkan bahwa meskipun RF memiliki tingkat akurasi yang lebih unggul, KNN lebih direkomendasikan sebagai instrumen mitigasi respons cepat guna mencegah dampak pemblokiran domain institusi secara *real-time*.

***Keyword*:** *Access Log*; Keamanan Siber; *Machine Learning*; Mitigasi Serangan; Universitas Muhammadiyah Aceh.

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

1. PENDAHULUAN

1.1 Latar Belakang

Di era transformasi digital, infrastruktur teknologi informasi menjadi aset vital bagi perguruan tinggi dalam menjalankan fungsi pendidikan dan administratif. Universitas Muhammadiyah Aceh (UNMUHA) telah mengimplementasikan manajemen peladen terpusat (*Centralized Hosting Server*) untuk mengelola *domain* utama *unmuha.ac.id* beserta seluruh *sub-domain* unit kerja di bawahnya. Integrasi ini bertujuan untuk meningkatkan efisiensi pengelolaan ekosistem bisnis digital kampus, namun di sisi lain, sentralisasi ini juga meningkatkan risiko keamanan siber yang signifikan.

Masalah utama yang dihadapi UNMUHA saat ini adalah tingginya intensitas serangan siber yang menargetkan kerentanan pada berbagai sub-domain. Dampak dari serangan ini telah menyebabkan domain institusi masuk ke dalam daftar blokir (*banned*) pada sistem *firewall* vendor penyedia *Data Center* serta mesin pencari global. Pemulihan domain yang telah diblokir memerlukan proses teknis yang panjang, yang secara langsung mengganggu kontinuitas layanan digital universitas.

Infrastruktur web server UNMUHA yang dikelola pada *Data Center* pihak ketiga sering kali menjadi target pemindaian kerentanan otomatis (*automated scanning*) oleh *bot* siber. Kurangnya sumber daya manusia dan alat pantau yang mampu melakukan mitigasi secara *real-time* menyebabkan aktivitas anomali sering terlambat dideteksi. Akibatnya, server sering mengalami kegagalan akses mendadak (*downtime*) atau dimatikan secara paksa oleh sistem keamanan vendor untuk mencegah penyebaran infeksi siber yang lebih luas. Ketiadaan sistem deteksi otomatis yang cerdas membuat proses mitigasi di UNMUHA saat ini masih bersifat reaktif dan manual.

Penelitian ini menawarkan kebaruan melalui penggunaan data *log* akses riil dari peladen utama Universitas Muhammadiyah Aceh yang beroperasi pada infrastruktur *Data Center* vendor. Berbeda dengan penelitian sebelumnya yang menggunakan dataset standar seperti CICIDS2017 (Irawan dkk., 2025) atau data simulasi IoT (Mansis dkk., 2025), penelitian ini menggunakan data autentik dari server yang sedang menghadapi ancaman pemblokiran infrastruktur secara riil. Dengan membandingkan performa algoritma *Machine Learning*, penelitian ini memberikan solusi praktis dalam mendeteksi berbagai jenis ancaman siber pada ekosistem *cloud hosting* institusi pendidikan.

1.2 Pokok Permasalahan

Berdasarkan kondisi tersebut, pokok permasalahan dalam penelitian ini adalah bagaimana menerapkan analisis komparasi algoritma *Machine Learning* yang mampu mengklasifikasikan trafik normal dan serangan siber secara umum pada *log* akses web server UNMUHA. Fokus utamanya adalah menemukan algoritma yang memiliki keseimbangan antara presisi deteksi dan kecepatan eksekusi guna memitigasi serangan siber sedini mungkin, sehingga risiko pemblokiran domain oleh pihak vendor dapat diminimalisir.

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

1.3 Tujuan Penelitian

Berdasarkan pokok permasalahan yang telah diuraikan, penelitian ini memiliki tujuan utama sebagai berikut:

1. Melakukan ekstraksi dan transformasi data *log* akses mentah dari *web server* UNMUHA menjadi dataset terstruktur yang siap diolah oleh algoritma *Machine Learning*.
2. Menganalisis perbandingan performa algoritma *Random Forest*, *K-Nearest Neighbor* (KNN), dan *Support Vector Machine* (SVM) dalam mengklasifikasikan aktivitas trafik normal dan serangan siber.
3. Menentukan algoritma yang paling optimal berdasarkan keseimbangan tingkat akurasi dan kecepatan waktu eksekusi sebagai dasar rekomendasi sistem mitigasi serangan siber pada infrastruktur *hosting* Universitas Muhammadiyah Aceh.

2. TEORI

2.1 Keamanan Siber dan Deteksi Anomali pada Web Server

Keamanan siber merupakan fondasi utama dalam menjaga keberlangsungan layanan digital, terutama pada institusi pendidikan yang mengelola data sensitif. Menurut Irawan dkk. (2025), ancaman siber seperti *Distributed Denial of Service* (DDoS) semakin sulit dibedakan dengan trafik normal, sehingga memerlukan sistem deteksi yang cerdas. Salah satu sumber data utama dalam mengidentifikasi ancaman adalah *log* sistem. Santoso dan Wahyuni (2024) menjelaskan bahwa analisis *log* akses web server Apache sangat krusial untuk menemukan jejak aktivitas yang tidak biasa melalui fitur seperti ukuran respon (*size*) dan pola permintaan HTTP. Deteksi anomali ini menjadi garda terdepan dalam memitigasi risiko sebelum serangan berdampak luas pada infrastruktur vendor *hosting*.

access log pada web server Apache menyimpan rekaman transaksional yang mendetail mengenai setiap permintaan yang diterima oleh peladen. Menurut Ma'ali dkk. (2022), data *log* ini merupakan sumber informasi primer dalam kegiatan forensik digital karena menyimpan atribut krusial seperti alamat IP asal, stempel waktu, metode HTTP, hingga *user agent* yang digunakan oleh pengakses. Analisis terhadap atribut-atribut ini memungkinkan pengelola infrastruktur untuk memetakan perilaku pengguna dan mengidentifikasi pola akses yang tidak wajar.

Selain itu, Santoso dan Wahyuni (2024) menekankan juga bahwa setiap entri dalam *log* akses memberikan gambaran mengenai status keberhasilan atau kegagalan sebuah permintaan melalui kode status HTTP (seperti 200 untuk sukses atau 404 untuk tidak ditemukan). Dalam ekosistem bisnis digital yang kompleks seperti di UNMUHA, pemantauan terhadap anomali pada ukuran respon (*byte size*) dan frekuensi akses yang tidak wajar ke direktori sensitif menjadi indikator awal adanya aktivitas pemindaian kerentanan (*vulnerability scanning*) atau upaya eksploitasi oleh bot otomatis. Oleh karena

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

itu, pengolahan *log* akses menjadi data terstruktur merupakan langkah krusial agar algoritma *machine learning* dapat melakukan klasifikasi ancaman dengan lebih presisi.

2.2 Konsep Machine Learning dalam Keamanan Jaringan

Machine Learning (ML) didefinisikan sebagai pengembangan sistem yang mampu mengekstraksi pengetahuan dari data masa lalu untuk melakukan prediksi atau pengambilan keputusan secara mandiri (Wijoyo dkk., 2024). Dalam bidang keamanan jaringan, teknologi ML digunakan untuk mengotomatisasi pengenalan pola serangan yang kompleks seperti *malware, ransomware,* dan *spyware* (Zy dkk., 2023). Pendekatan ini jauh lebih efektif dibandingkan metode konvensional karena sifatnya yang adaptif terhadap variasi serangan baru yang terus berkembang (Mansis dkk., 2025).

2.3 Algoritma Random Forest (RF)

Random Forest adalah metode *ensemble learning* yang menggabungkan banyak pohon keputusan untuk meningkatkan akurasi klasifikasi dan mengontrol *overfitting*. Algoritma ini bekerja dengan menentukan hasil akhir berdasarkan suara terbanyak dari setiap pohon yang dibentuk (Mansis dkk., 2025). Menurut Ningrum dkk. (2025), keunggulan utama RF terletak pada kemampuannya menangani dataset dalam jumlah besar dengan banyak atribut, yang sangat relevan dengan karakteristik data *log* serangan siber yang kompleks.

2.4 Algoritma K-Nearest Neighbor (KNN)

K-Nearest Neighbor merupakan algoritma klasifikasi yang bersifat non-parametrik dan berbasis instansi, di mana penentuan kelas suatu data ditentukan oleh kedekatan jarak (seperti *Euclidean distance*) dengan tetangga terdekatnya (Himawan dkk., 2024). Prasetyo dkk. (2023) menyatakan bahwa KNN sangat efisien dalam mengklasifikasikan data riwayat jaringan karena kesederhanaan logikanya. Selain akurasi yang kompetitif, KNN sering dipilih karena responsivitasnya yang tinggi dalam proses deteksi, menjadikannya kandidat kuat untuk mitigasi serangan secara *real-time* (Wicaksono dkk., 2025).

2.5 Algoritma Support Vector Machine (SVM)

Support Vector Machine adalah model pembelajaran mesin yang fokus pada pencarian *hyperplane* atau bidang pemisah paling optimal untuk membagi dua kelas berbeda dengan margin maksimal. Eldo dkk. (2024) menekankan bahwa SVM memiliki performa yang sangat baik dalam menangani data dengan dimensi tinggi dan kasus klasifikasi yang rumit. Dalam penelitian keamanan siber, SVM sering digunakan untuk mengidentifikasi ancaman spesifik pada trafik jaringan dengan tingkat presisi yang tinggi, meskipun memerlukan waktu komputasi yang lebih intensif dibandingkan algoritma lainnya (Irawan dkk., 2025).

2.6 Keamanan Data dan Privasi pada Layanan Daring

Keamanan data informasi dan privasi telah menjadi isu krusial di Indonesia, terutama setelah disahkannya regulasi perlindungan data pribadi. Taufan dan Wibowo (2024) menjelaskan bahwa peningkatan penetrasi internet harus dibarengi dengan

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

mekanisme pertahanan data yang tangguh untuk meminimalisir kerugian pengguna akibat kebocoran informasi. Dalam konteks perguruan tinggi seperti UNMUHA, perlindungan terhadap *log* akses bukan hanya sekadar kebutuhan teknis, melainkan bentuk kepatuhan terhadap standar perlindungan data privasi civitas akademika dari ancaman pihak ketiga yang tidak bertanggung jawab.

2.7 Mitigasi Risiko pada Infrastruktur Bisnis Digital

Keberlangsungan operasional dalam ekosistem bisnis digital sangat bergantung pada kemampuan sistem dalam mendeteksi dan merespons ancaman secara dini. Menurut Eldo dkk. (2024), penggunaan algoritma cerdas seperti SVM sangat efektif dalam mengklasifikasikan aktivitas sah dan upaya penipuan (*fraud*) pada transaksi daring yang memiliki dimensi fitur yang kompleks. Implementasi model pembelajaran mesin pada infrastruktur peladen bertujuan untuk menciptakan lingkungan digital yang stabil, sehingga risiko kegagalan layanan (*downtime*) yang dapat merugikan reputasi dan ekonomi institusi dapat ditekan serendah mungkin.

2.8 Penelitian Terkait

Berbagai studi sebelumnya telah mengeksplorasi efektivitas penggunaan algoritma *machine learning* dalam menghadapi ancaman siber pada infrastruktur digital. Referensi-referensi berikut memberikan landasan mengenai performa algoritma yang relevan dengan penelitian ini.

Penelitian mengenai deteksi ancaman pada infrastruktur digital telah banyak dilakukan dengan berbagai pendekatan algoritma. Mansis dkk. (2025) dalam studinya menunjukkan bahwa algoritma *Random Forest* dan *K-Nearest Neighbor* memiliki efektivitas tinggi dalam mengidentifikasi pola serangan pada jaringan. Hal ini diperkuat oleh penelitian Ningrum dkk. (2025) yang secara spesifik mengevaluasi penggunaan KNN dan RF untuk klasifikasi log serangan siber di lingkungan universitas, di mana kedua algoritma tersebut terbukti mampu memberikan hasil deteksi yang akurat pada data log.

Selain itu, penggunaan *Support Vector Machine* (SVM) juga menjadi perhatian luas dalam literatur keamanan siber. Irawan dkk. (2025) dan Zy dkk. (2023) menekankan bahwa SVM memiliki keunggulan dalam menangani data dengan dimensi tinggi untuk mendeteksi serangan seperti DDoS dan ancaman jaringan lainnya. Sejalan dengan hal tersebut, Eldo dkk. (2024) juga memanfaatkan SVM untuk klasifikasi dalam upaya memitigasi risiko keamanan di platform digital.

Dalam konteks pengolahan data log, Ma'ali dkk. (2022) menekankan pentingnya proses *parsing* dan *feature importance* dalam mentransformasi log *web server* yang tidak terstruktur menjadi dataset yang siap diolah. Pendekatan lain dalam mendeteksi anomali pada log sistem juga dikembangkan oleh Santoso dan Wahyuni (2024) yang menggunakan model *Isolation Forest* untuk mengidentifikasi aktivitas tidak biasa pada trafik *web server*. Integrasi berbagai algoritma *machine learning* ini, sebagaimana dijelaskan dalam buku Permana dkk. (2023), memberikan landasan teoritis bahwa

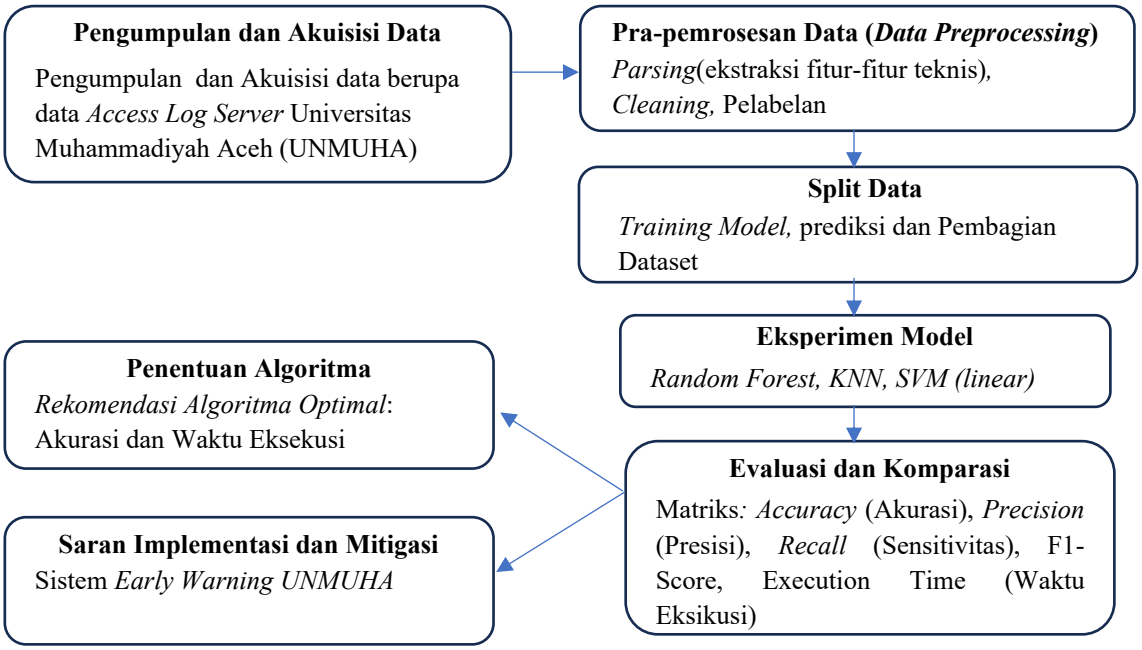
BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

pendekatan berbasis data merupakan solusi efektif dalam menghadapi dinamika ancaman siber saat ini.

3. METODOLOGI

3.1. Kerangka Kerja Penelitian

Penelitian ini dilaksanakan dengan mengadopsi kerangka kerja *Cross-Industry Standard Process for Data Mining* (CRISP-DM) yang sistematis dengan evaluasi berbasis *confusion matrix*. Tahapan dimulai dari pemahaman terhadap masalah keamanan pada server UNMUHA, pengumpulan data *log*, pemb ersihan data, pemodelan menggunakan tiga algoritma *machine learning*, hingga evaluasi performa model (Wijoyo dkk., 2024). Alur ini memastikan bahwa setiap proses transformasi data dari bentuk mentah menjadi informasi mitigasi dilakukan secara terukur.



Gambar 1
Diagram Alur Penelitian

Tahapan penelitian yang dilakukan dalam studi ini digambarkan secara sistematis pada Gambar 1. Proses dimulai dengan Pengumpulan dan Akuisisi Data yang bersumber dari aktivitas trafik riil pada *web server* unmuha.ac.id. Data mentah tersebut kemudian masuk ke tahap Pra-pemrosesan Data yang meliputi tiga langkah krusial: *Parsing* untuk mengekstraksi fitur-fitur teknis menjadi dataset terstruktur, *Cleaning* untuk membersihkan entri yang tidak lengkap, serta *Labeling* untuk mengklasifikasikan trafik normal dan serangan.

Selanjutnya, dilakukan tahap Split Data dengan membagi dataset ke dalam proporsi 80% untuk Pelatihan (*Training*) dan 20% untuk Pengujian (*Testing*). Tahap ini dilanjutkan dengan Eksperimen Model menggunakan algoritma *Random Forest*, KNN,

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

dan SVM (Linear). Hasil dari eksperimen tersebut kemudian masuk ke tahap Evaluasi dan Komparasi menggunakan *Confusion Matrix* dan waktu eksekusi. Rangkaian proses ini diakhiri dengan Penentuan Algoritma optimal yang menjadi dasar bagi Saran Implementasi dan Mitigasi berupa sistem *Early Warning* untuk memperkuat keamanan infrastruktur digital di Universitas Muhammadiyah Aceh.

3.2. Prosedur Pengumpulan dan Akuisisi Data

Objek penelitian ini adalah data *log* akses riil yang berasal dari peladen utama Universitas Muhammadiyah Aceh (unmuha.ac.id) yang dikelola pada infrastruktur *cloud hosting* vendor. Data diambil dalam format teks mentah (*raw text*) yang mencatat setiap aktivitas permintaan HTTP ke domain utama maupun sub-domain. Sejalan dengan metode yang dipaparkan oleh Ma'ali dkk. (2022), proses akuisisi data ini bertujuan untuk mendapatkan bukti digital berupa stempel waktu, alamat IP pengakses, metode permintaan, serta URL yang menjadi target aktivitas siber.

3.3. Pra-pemrosesan Data (*Data Preprocessing*)

Mengingat data *log* bersifat tidak terstruktur, dilakukan tahap pra-pemrosesan untuk meningkatkan kualitas data sebelum tahap pelatihan model. Tahapan ini meliputi:

1. Pembersihan Data (*Cleaning*): Menghilangkan entri log yang tidak lengkap atau memiliki nilai *null*.
2. Ekstraksi Fitur dengan Regex: Menggunakan ekspresi reguler untuk memisahkan komponen log (IP, *Method, Path, Status, Size*) menjadi kolom-kolom terstruktur (Santoso & Wahyuni, 2024).
3. Transformasi Data: Fitur kategorikal seperti metode HTTP dikonversi menjadi nilai numerik menggunakan teknik *Label Encoding* agar dapat diproses oleh algoritma klasifikasi (Mansis dkk., 2025).
4. Pelabelan Otomatis (*Labeling*): Data diklasifikasikan menjadi dua kategori, yaitu "Normal" dan "Serangan", berdasarkan pola tanda tangan (*signature*) yang merujuk pada aktivitas mencurigakan seperti pemindaian direktori sensitif dan pola injeksi (Wicaksono dkk., 2025).

3.4. Implementasi Algoritma Komparasi

Penelitian ini membandingkan tiga algoritma dengan karakteristik yang berbeda untuk menemukan solusi mitigasi terbaik:

- Random Forest (RF): Dipilih karena kemampuannya dalam menangani data dengan fitur yang kompleks dan meminimalisir kesalahan prediksi melalui mekanisme *ensemble* (Ningrum dkk., 2025).
- K-Nearest Neighbor (KNN): Diimplementasikan untuk menguji kecepatan deteksi berdasarkan kemiripan jarak fitur, yang sangat krusial untuk respon mitigasi cepat (Prasetyo dkk., 2023).
- Support Vector Machine (SVM): Digunakan untuk mengevaluasi pemisahan kelas antara trafik legal dan ilegal dengan menggunakan *hyperplane* optimal (Irawan dkk., 2025).

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

3.5. Instrumen Evaluasi Performa

Untuk mengukur efektivitas dan memvalidasi keandalan algoritma *Machine Learning* yang diuji, penelitian ini menggunakan instrumen evaluasi berupa *Confusion Matrix*. Metrik ini digunakan untuk membandingkan nilai prediksi sistem dengan nilai aktual pada dataset *testing*. Berdasarkan kriteria evaluasi standar dalam keamanan siber (Zy dkk., 2023; Prasetyo dkk., 2023), performa model diukur menggunakan empat metrik utama sebagai berikut:

a. ***Accuracy*** **(Akurasi)**

Akurasi menggambarkan tingkat ketepatan model dalam mengklasifikasikan seluruh trafik (baik trafik normal maupun serangan) secara benar dari total keseluruhan data.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

b. ***Precision*** **(Presisi)**

Presisi digunakan untuk mengukur tingkat keakuratan model dalam menetapkan label serangan. Metrik ini sangat penting untuk meminimalkan tingkat kesalahan deteksi (*false alarm*).

$$Precision = \frac{TP}{TP + FP}$$

c. ***Recall*** **(Sensitivitas)**

Recall mengukur kemampuan model dalam mendeteksi dan menangkap seluruh upaya serangan yang terdapat di dalam log akses. Dalam mitigasi serangan siber di UNMUHA, nilai *recall* yang tinggi sangat krusial agar tidak ada serangan yang lolos dari deteksi.

$$Recall = \frac{TP}{TP + FN}$$

d. ***F1-Score***

F1-Score merupakan rata-rata harmonik antara presisi dan *recall*. Metrik ini memberikan gambaran keseimbangan performa model, terutama pada karakteristik data log yang tidak seimbang (*imbalanced data*).

$$F1 - Score = \frac{Precision\ x\ Recall}{Precesion + Recall}$$

Keterangan variabel dalam rumus tersebut didefinisikan berdasarkan konteks akses pada server UNMUHA:

- **TP (*True Positive*):** Aktivitas serangan yang berhasil dideteksi dengan benar sebagai serangan.
- **TN (*True Negative*):** Aktivitas akses normal yang berhasil dideteksi dengan benar sebagai akses normal.
- **FP (*False Positive*):** Akses normal yang salah teridentifikasi sebagai serangan (*false alarm*).

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

- **FN (*False Negative*):** Aktivitas serangan yang gagal terdeteksi dan dianggap sebagai akses normal oleh sistem.

Selain metrik matematis di atas, penelitian ini juga mengukur *Execution Time* (Waktu Eksikusi) untuk mengevaluasi kecepatan respons setiap algoritma dalam melakukan mitigasi serangan pada infrastruktur web server secara *real-time*.

4. HASIL DAN PEMBAHASAN

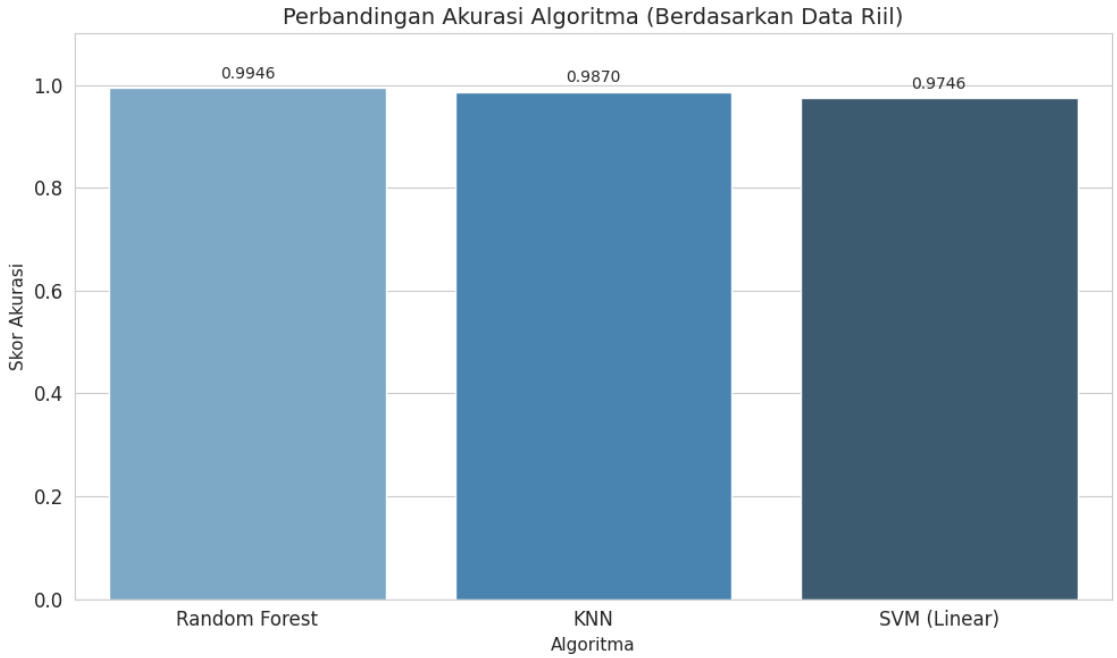
4.1 Hasil Analisis Data

Eksperimen dilakukan terhadap data *log* akses *web server* Universitas Muhammadiyah Aceh telah melalui tahap pra-pemrosesan dan pelabelan. Pengujian dilakukan menggunakan pembagian dataset 80% untuk pelatihan (*training*) dan 20% untuk pengujian (*testing*). Berdasarkan skenario tersebut, dilakukan pengujian terhadap tiga algoritma *Machine Learning* untuk mengukur performa masing-masing dalam mengklasifikasikan trafik. Hasil lengkap pengujian disajikan pada Tabel 1, untuk perbandingan algoritma berdasarkan nilai akurasi telah disajikan dalam bentuk visual berupa grafik batang pada gambar 2 dan perbandingan algoritma berdasarkan nilai waktu eksikusi disajikan pada gambar 3.

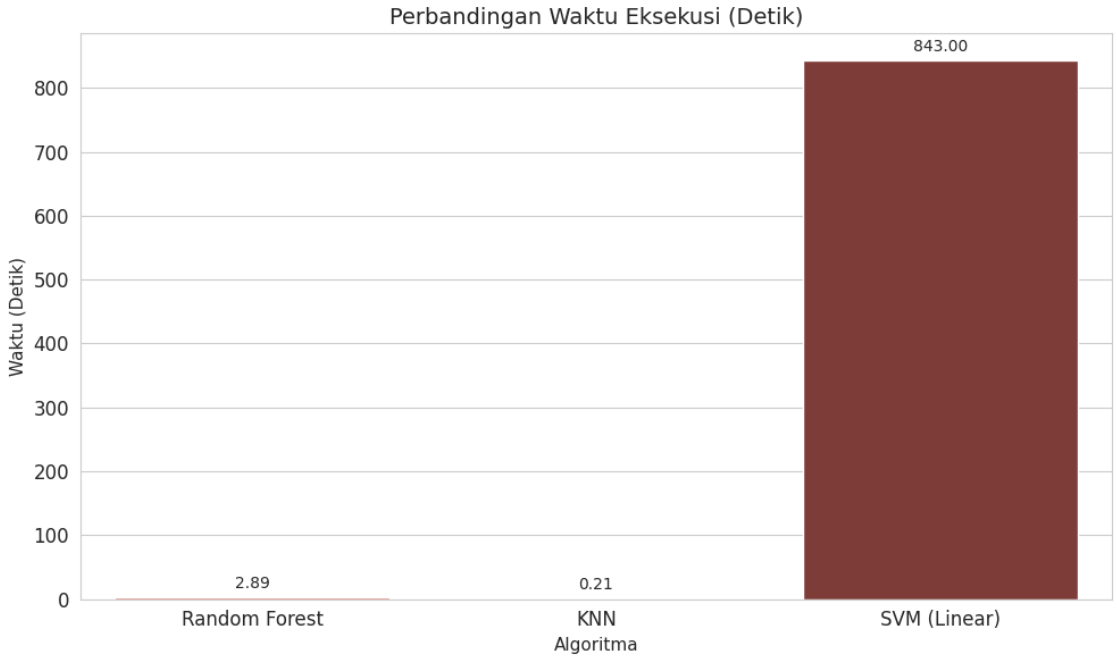
Tabel 1
Perbandingan Performa Algoritma Klasifikasi

Algoritma	Accuracy	Precision	Recall	F1-Score	Execution Time (s)
Random Forest	0,9946	0,9344	0.8584	0,8948	2,8892
KNN	0,9870	0,8226	0,6566	0,7303	0,2124
SVM (Linear)	0,9746	0,6957	0,0964	0,1693	842,9966

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2



Gambar 2
Grafik Perbandingan Akurasi Algoritma



Gambar 3
Grafik Perbandingan Waktu Eksikusi

BIDIG: Jurnal Bisnis Digital
Volume 5 No. 2: Edisi Juli - Desember 2025
E-ISSN: 2807-1042
DOI: 10.37598/jbidig.v5i2

4.2 Pembahasan

Analisis Ketepatan Klasifikasi (Akurasi dan Presisi) Algoritma *Random Forest* menunjukkan performa yang paling unggul dalam mendeteksi ancaman siber pada peladen UNMUHA dengan akurasi mencapai 99,46%. Nilai presisi sebesar 0,9344 menunjukkan bahwa model ini sangat handal dalam meminimalisir kesalahan deteksi (*false alarm*). Keunggulan ini dimungkinkan karena mekanisme *ensemble learning* pada *Random Forest* yang mampu menangani fitur-fitur kompleks pada log akses melalui kombinasi beberapa *decision trees*.

Analisis Efisiensi dan Responsivitas Poin krusial dalam penelitian ini adalah waktu respons sistem mitigasi. Hasil pengujian menunjukkan perbedaan waktu eksekusi yang sangat kontras. SVM (Linear) memerlukan waktu hingga 842,99 detik, yang menjadikannya sangat tidak efektif untuk lingkungan produksi. Rendahnya nilai *Recall* pada SVM (0,0964) juga menunjukkan bahwa algoritma ini kesulitan dalam mengidentifikasi pola serangan pada dataset yang tidak seimbang (*imbalanced data*), di mana jumlah akses normal jauh lebih dominan daripada trafik serangan.

Sebaliknya, KNN mampu menyelesaikan klasifikasi dalam waktu 0,2124 detik, atau hampir 4.000 kali lebih cepat dibandingkan SVM. Kecepatan ini sangat vital bagi UNMUHA untuk memicu sistem *early warning* secara otomatis sebelum mekanisme keamanan pihak vendor melakukan pemblokiran domain institusi secara permanen akibat akumulasi trafik anomali yang tidak tertangani.

Implikasi terhadap Mitigasi Serangan Siber UNMUHA Meskipun *Random Forest* unggul dalam akurasi absolut, KNN menawarkan keseimbangan yang lebih baik antara performa deteksi dan kecepatan eksekusi. Dalam konteks mitigasi operasional, waktu eksekusi yang rendah memungkinkan sistem untuk melakukan pemblokiran alamat IP penyerang secara *real-time*. Implementasi KNN sebagai dasar algoritma sistem pendeteksi serangan akan secara signifikan mengurangi risiko terjadinya *downtime* layanan serta melindungi reputasi domain unmuha.ac.id pada mesin pencari global.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan eksperimen yang telah dilakukan terhadap mitigasi serangan siber pada *web server* Universitas Muhammadiyah Aceh menggunakan data *log* akses riil, maka dapat ditarik beberapa kesimpulan utama sebagai berikut:

1. Penelitian ini berhasil mentransformasi data *log* mentah dari peladen unmuha.ac.id menjadi dataset terstruktur yang dapat diolah oleh algoritma *Machine Learning* untuk mendeteksi anomali trafik secara akurat.
2. Dari hasil komparasi tiga algoritma, Random Forest menunjukkan performa yang paling unggul dalam aspek ketepatan klasifikasi dengan nilai akurasi mencapai 99,46% dan presisi 0,9344. Hal ini menjadikannya algoritma yang sangat andal

untuk membedakan antara trafik normal dan serangan siber dengan risiko kesalahan deteksi yang minimal.

3. Dalam aspek efisiensi waktu, KNN terbukti sebagai algoritma yang paling responsif dengan waktu eksekusi hanya 0,2124 detik, atau hampir 4.000 kali lebih cepat dibandingkan SVM (842,99 detik). Kecepatan ini sangat krusial dalam konteks mitigasi *real-time* untuk mencegah pemblokiran domain institusi oleh pihak vendor dan mesin pencari global.
4. Implementasi algoritma *Machine Learning* (khususnya KNN) sebagai instrumen mitigasi dapat memberikan solusi bagi UNMUHA dalam mengatasi ancaman serangan siber yang berulang, meminimalkan *downtime* layanan, serta melindungi reputasi digital institusi.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilaksanakan, terdapat beberapa saran yang dapat diajukan untuk kepentingan praktis maupun pengembangan ilmu pengetahuan:

1. Bagi Pengelola Web Server Universitas Muhammadiyah Aceh, disarankan agar pihak universitas mengintegrasikan sistem *early warning* berbasis algoritma *Machine Learning* (khususnya KNN) ke dalam infrastruktur peladen. Hal ini bertujuan untuk mengotomatisasi proses deteksi dan pemblokiran alamat IP penyerang secara *real-time*, sehingga risiko kegagalan layanan (*downtime*) dan pemblokiran domain institusi oleh vendor keamanan dapat diminimalisir.
2. Bagi Pengembangan Penelitian, penelitian selanjutnya disarankan untuk melakukan eksplorasi metode penanganan ketidakseimbangan data (*imbalanced data*) seperti teknik *oversampling* (SMOTE) untuk meningkatkan sensitivitas deteksi. Selain itu, pengembangan dapat diarahkan pada penggunaan algoritma *Deep Learning* serta penggabungan dataset dari berbagai sumber log server yang lebih luas untuk menghasilkan model mitigasi yang lebih general dan tangguh.

6. DAFTAR PUSTAKA

Eldo, H., Ayuliana., Suryadi, D., Chrisnawati, G., & Judijanto, L. (2024). Penggunaan Algoritma Support Vector Machine (SVM) Untuk Deteksi Penipuan pada Transaksi Online. *Jurnal Minfo Polgan*, 13(2), 728-736. https://doi.org/10.33395/jmp.v13i2.14186

Himawan, A. J., Sari, A. M. K., Parsa, N. A., Hermansyah, K. S. P., & Rizki, E. S. D. (2024). Penerapan Metode K-Nearest Neighbors dalam Mendeteksi Website Phishing. *COREAI: Jurnal Kecerdasan Buatan, Komputasi dan Teknologi Informasi*, 5(2).

Irawan, Y., Pramitasari, R., Ashari, W. M., & Yansyah, A. N. H. (2025). Support Vector Machine Classification Algorithm for Detecting DDoS Attacks on

Network Traffic. *Journal of Applied Informatics and Computing (JAIC)*, 9(4), 1945-1954.

Ma'ali, A. A., Girinoto., Ghiffari, M. N., & Hadiprakoso, R. B. (2022). Analisis Log Web Server dengan Pendekatan Algoritme K-Means Clustering dan Feature Importance. *Jurnal Info Kripto*, 16(3).

Mansis, M. I., Putri, F. S., Siregar, M. R., & Kurniabudi. (2025). Analisis Kinerja Algoritma K-Nearest Neighbor dan Random Forest untuk Deteksi Serangan pada Jaringan Perangkat IoT. *Jurnal Processor*, 20(2).

Ningrum, A. W., Aji, M. P., Wijaya, E. S., & Pambudi, E. A. (2025). Deteksi dan Klasifikasi Ancaman pada Log Serangan Siber Menggunakan Algoritma K-Nearest Neighbor (KNN) dan Random Forest (RF). *Jurnal Pendidikan dan Teknologi Indonesia (JPTI)*, 5(12), 3610-3619. https://doi.org/10.52436/1.jpti.1197

Permana, A. A., Wahyuddin, S., Santoso, L. W., Wibowo, G. W. N., Wardhani, A. K., Rahmaddeni., ... Abdurrasyid. (2023). *Machine Learning*. Global Eksekutif Teknologi.

Prasetyo, D. S., Auliasari, K., & Syalabi, M. R. P. (2023). Klasifikasi Serangan Jaringan Menggunakan Metode K-Nearest Neighbour pada Data Riwayat Jaringan. *Seminar Nasional SENIATI 2023*, 66-70. ISSN 2085-4218.

Santoso, D. B., & Wahyuni, Y. (2024). Sistem Log Web Server sebagai Pendeteksi Anomali Menggunakan Isolation Forest. *JUBIKOM: Jurnal Aplikasi Bisnis dan Komputer*, 4(3).

Taufan, A. Z., & Wibowo, W. (2024). Analisis Sentimen Terkait Persepsi Keamanan Data Informasi dan Privasi di Indonesia Menggunakan Pendekatan Machine Learning. *JINTEKS: Jurnal Informatika Teknologi dan Sains*, 6(3), 728-736.

Wicaksono, B. S., Pramukantoro, E. S., & Kartikasari, D. P. (2025). Perbandingan Kinerja Algoritma Support Vector Machine dan K-Nearest Neighbor dalam Mendeteksi Pesan Berisi Tautan Phishing pada Platform Media Sosial X. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 9(7).

Wijoyo, A., Saputra, A. Y., Ristanti, S., Sya'Ban, S. R., Amalia, M., & Febriansyah, R. (2024). Pembelajaran Machine Learning. *OKTAL: Jurnal Ilmu Komputer dan Science*, 3(2), 375-380.

Zy, A. T., Sasongko, A. T., & Kamalia, A. Z. (2023). Penerapan Naïve Bayes Classifier, Support Vector Machine, dan Decision Tree untuk Meningkatkan Deteksi Ancaman Keamanan Jaringan. *KLIK: Kajian Ilmiah Informatika dan Komputer*, 4(1), 610-617. https://doi.org/10.30865/klik.v4i1.1134