JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

Pengembangan Sistem Intrusion Detection and Prevention System (IDPS) Berbasis Random Forest dan Windows Defender Firewall Pada Jaringan Lokal Testing

M. Salman Nuzul Ramdhani [1*], Muhlis Tahir[2], Mohammad Muhyidin Alhaq[3]

[1, 2, 3]Fakultas Keguruan dan Ilmu Pendidikan, Pendidikan Informatika, Universitas Trunodjoyo Madura, Bangkalan, Indonesia
Email:[1*] salman.ramdhani122@gmail.com, [2] muhlis.tahir@trunojoyo.ac.id, [3] muhyidinalhaq16@gmail.com
(*Email Corresponding Author : salman.ramdhani122@gmail.com)
Received: June 2, 2026 | Revision: June 3, 2026 | Accepted: June 5, 2026

Abstrak

Perkembangan teknologi jaringan komputer yang pesat telah meningkatkan penggunaan jaringan lokal (Local Area Network/LAN) dalam berbagai aktivitas digital. Namun, hal tersebut juga diiringi dengan meningkatnya ancaman keamanan seperti akses tidak sah, malware, dan intrusi jaringan. Oleh karena itu, diperlukan sistem keamanan yang mampu mendeteksi dan mencegah serangan secara efektif. Penelitian ini bertujuan untuk mengembangkan sistem Intrusion Detection and Prevention System (IDPS) berbasis algoritma Random Forest yang diintegrasikan dengan Windows Defender Firewall pada jaringan lokal. Sistem ini memanfaatkan machine learning untuk mengklasifikasikan trafik jaringan menjadi normal dan berbahaya, serta firewall sebagai mekanisme pencegahan untuk memblokir aktivitas mencurigakan. Metode penelitian meliputi pengembangan sistem, implementasi pada jaringan lokal, serta pengujian melalui simulasi serangan. Algoritma Random Forest digunakan untuk meningkatkan akurasi deteksi, sedangkan konfigurasi firewall digunakan untuk mengontrol lalu lintas jaringan. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi aktivitas mencurigakan secara efektif serta mencegah akses tidak sah melalui mekanisme firewall. Integrasi antara machine learning dan firewall menghasilkan sistem keamanan berlapis yang meningkatkan perlindungan jaringan. Kesimpulannya, sistem IDPS yang dikembangkan efektif dalam meningkatkan keamanan jaringan lokal dengan menggabungkan mekanisme deteksi dan pencegahan.

Kata kunci: *Intrusion Detection and Prevention System, Random Forest, Keamanan Jaringan, Firewall, Machine Learning, Jaringan Lokal*

Abstract

The rapid development of computer network technology has increased the use of Local Area Networks (LAN) as a primary infrastructure in various digital activities. However, this growth is accompanied by increasing security threats such as unauthorized access, malware, and network intrusions. Therefore, an effective security system is required to detect and prevent potential attacks. This study aims to develop an Intrusion Detection and Prevention System (IDPS) based on the Random Forest algorithm integrated with Windows Defender Firewall in a local network environment. The system utilizes machine learning to classify network traffic into normal and malicious categories, while the firewall functions as a preventive mechanism to block suspicious activities. The research method involves system development, implementation in a local network, and testing through simulated attack scenarios. The Random Forest algorithm is applied to improve detection accuracy, while firewall configuration is used to control network traffic based on predefined rules. The results show that the proposed system is able to detect suspicious activities effectively and prevent unauthorized access through firewall filtering. The integration of machine learning and firewall mechanisms provides a layered security approach that enhances overall network protection. In conclusion, the developed IDPS system demonstrates effectiveness in improving network security by combining detection and prevention mechanisms, making it a suitable solution for securing local network environments.

Keywords: *Intrusion Detection and Prevention System, Random Forest, Network Security, Firewall, Machine Learning, Local Area Network.*

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer yang semakin pesat telah mendorong penggunaan jaringan lokal (Local Area Network/LAN) sebagai infrastruktur utama dalam berbagai aktivitas digital, seperti pertukaran data, komunikasi, serta pengelolaan sistem informasi. Namun, peningkatan penggunaan jaringan tersebut juga diiringi dengan meningkatnya ancaman keamanan yang semakin kompleks dan dinamis. Serangan seperti unauthorized access, malware, dan intrusi jaringan dapat menyebabkan gangguan terhadap ketersediaan layanan, kebocoran data, serta kerusakan sistem yang signifikan.

Keamanan jaringan menjadi aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Penerapan mekanisme keamanan seperti access control list (ACL) terbukti mampu meningkatkan perlindungan jaringan dengan membatasi akses yang tidak sah serta mengontrol lalu lintas data secara efektif [1]. Namun demikian, pendekatan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

keamanan tradisional yang bersifat statis masih memiliki keterbatasan dalam menghadapi pola serangan modern yang semakin adaptif dan kompleks.

Salah satu pendekatan yang digunakan dalam menjaga keamanan jaringan adalah Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). IDS berfungsi untuk mendeteksi aktivitas mencurigakan dalam jaringan, sedangkan IPS memiliki kemampuan untuk mencegah serangan secara langsung. Kombinasi keduanya dikenal sebagai Intrusion Detection and Prevention System (IDPS), yang menjadi solusi penting dalam sistem keamanan jaringan modern [2].

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan IDPS mampu meningkatkan efektivitas deteksi serangan jaringan. Namun, sebagian besar sistem IDPS konvensional masih bergantung pada metode berbasis signature yang kurang efektif dalam mendeteksi serangan baru (zero-day attack). Selain serangan pada tingkat jaringan, ancaman terhadap aplikasi web juga terus meningkat. Salah satu serangan yang paling umum adalah SQL Injection, yaitu teknik eksploitasi yang memanfaatkan kelemahan validasi input untuk memperoleh akses tidak sah ke basis data. Penelitian menunjukkan bahwa kerentanan SQL Injection masih banyak ditemukan pada aplikasi web dan dapat menyebabkan kebocoran data yang signifikan [3]. Oleh karena itu, pendekatan berbasis machine learning mulai dikembangkan untuk meningkatkan kemampuan deteksi.

Algoritma Random Forest merupakan salah satu metode machine learning yang banyak digunakan dalam sistem deteksi intrusi karena memiliki tingkat akurasi yang tinggi serta mampu menangani data dalam jumlah besar. Penelitian menunjukkan bahwa penggunaan Random Forest dalam sistem deteksi intrusi mampu meningkatkan performa klasifikasi trafik jaringan secara signifikan dibandingkan metode konvensional [4], [5].

Perkembangan penelitian terbaru menunjukkan bahwa performa sistem deteksi intrusi dapat ditingkatkan melalui penggabungan algoritma Random Forest dengan berbagai teknik optimasi dan penyeimbangan data. Lu et al. mengembangkan Enhanced Random Forest yang mampu meningkatkan akurasi klasifikasi serta mengurangi kompleksitas komputasi pada proses deteksi intrusi dengan memanfaatkan optimasi reduksi dimensi dan pendekatan cost-sensitive learning [6]. Selain itu, Wu et al. menunjukkan bahwa permasalahan ketidakseimbangan data pada sistem deteksi intrusi dapat diatasi melalui kombinasi algoritma SMOTE dan Enhanced Random Forest, sehingga mampu meningkatkan kemampuan deteksi terhadap jenis serangan yang memiliki jumlah data lebih sedikit [7].

Penelitian lain juga menunjukkan bahwa Random Forest memiliki performa yang sangat baik dalam mendeteksi ancaman jaringan modern. Abdelaziz et al. berhasil memperoleh nilai weighted F1-score sebesar 99,8% dengan memanfaatkan teknik feature selection dan permutation importance pada dataset CICIDS-2017, yang menunjukkan bahwa Random Forest mampu menjadi solusi efektif untuk meningkatkan kinerja Network Intrusion Detection System (NIDS) [8]. Selain itu, integrasi Random Forest dengan metode deteksi lainnya juga terbukti mampu meningkatkan kemampuan sistem dalam mendeteksi serangan yang belum pernah dikenali sebelumnya (zero-day attack) sekaligus mengurangi tingkat false positive yang sering menjadi kendala pada sistem deteksi tradisional [9].

Hasil-hasil penelitian tersebut menunjukkan bahwa algoritma Random Forest memiliki potensi besar untuk diterapkan sebagai komponen utama dalam sistem Intrusion Detection and Prevention System (IDPS). Namun demikian, sebagian besar penelitian masih berfokus pada aspek deteksi intrusi, sedangkan mekanisme pencegahan otomatis terhadap serangan yang terdeteksi belum banyak diintegrasikan secara langsung dengan sistem keamanan bawaan sistem operasi seperti Windows Defender Firewall [10].

Selain sistem deteksi, firewall juga memiliki peran penting dalam sistem keamanan jaringan sebagai mekanisme kontrol akses. Firewall bekerja dengan menyaring lalu lintas jaringan berdasarkan aturan tertentu untuk mencegah akses yang tidak sah. Implementasi firewall filtering terbukti mampu meningkatkan keamanan jaringan dengan membatasi akses ilegal serta mengontrol trafik jaringan secara efektif [11]. Integrasi antara sistem deteksi berbasis machine learning dengan firewall memungkinkan terbentuknya sistem keamanan berlapis (layered security) yang lebih efektif dalam menghadapi ancaman siber [12], [13].

Berdasarkan penelitian terkait tersebut, terdapat kesenjangan (gap analysis) yaitu belum optimalnya integrasi antara metode deteksi berbasis machine learning dengan sistem pencegahan seperti firewall dalam satu sistem yang terintegrasi secara langsung. Sebagian penelitian hanya berfokus pada deteksi tanpa mekanisme pencegahan yang optimal, atau sebaliknya hanya mengandalkan firewall tanpa sistem deteksi yang cerdas.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem Intrusion Detection and Prevention System (IDPS) berbasis algoritma Random Forest yang diintegrasikan dengan Windows Defender Firewall pada jaringan lokal. Sistem ini diharapkan mampu meningkatkan efektivitas dalam mendeteksi dan mencegah serangan jaringan secara lebih optimal, serta memberikan kontribusi dalam pengembangan sistem keamanan jaringan yang adaptif dan modern.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode eksperimen dengan pendekatan pengembangan sistem keamanan jaringan berbasis *Intrusion Detection and Prevention System* (IDPS). Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem yang mampu mendeteksi serta mencegah serangan jaringan secara efektif dengan memanfaatkan algoritma *machine learning* dan mekanisme firewall.

Pendekatan pengembangan sistem keamanan jaringan berbasis machine learning banyak digunakan pada penelitian terkini karena mampu meningkatkan kemampuan deteksi terhadap serangan yang terus berkembang.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

Random Forest dipilih karena memiliki kemampuan klasifikasi yang baik pada data trafik jaringan, tahan terhadap overfitting, serta mampu menangani data berdimensi besar dengan tingkat akurasi yang tinggi. Beberapa penelitian menunjukkan bahwa Random Forest dapat digunakan secara efektif dalam sistem Intrusion Detection System (IDS) maupun Network Intrusion Detection System (NIDS) untuk mendeteksi berbagai jenis serangan jaringan secara akurat [14], [15]. Selain itu, penggunaan metode berbasis machine learning memungkinkan sistem untuk mengenali pola anomali yang tidak dapat dideteksi secara optimal oleh metode berbasis signature saja [16]. Oleh karena itu, pendekatan ini dinilai sesuai untuk diterapkan pada pengembangan Intrusion Detection and Prevention System (IDPS) yang membutuhkan kemampuan deteksi dan respons secara otomatis.

Tahapan penelitian dilakukan secara sistematis untuk memastikan proses pengembangan sistem berjalan dengan baik dan menghasilkan output yang sesuai dengan tujuan penelitian. Tahapan tersebut meliputi:

1. Planning (Perencanaan)
   Pada tahap ini dilakukan identifikasi permasalahan yang terjadi pada keamanan jaringan, serta analisis kebutuhan sistem yang akan dikembangkan. Tahap ini juga mencakup penentuan metode yang digunakan, yaitu algoritma *Random Forest* untuk deteksi dan *Windows Defender Firewall* untuk pencegahan.
2. Information Gathering (Pengumpulan Data)
   Tahap ini dilakukan untuk mengumpulkan data yang berkaitan dengan trafik jaringan. Data yang digunakan meliputi aktivitas normal dan aktivitas yang mengandung indikasi serangan, yang nantinya digunakan sebagai bahan pelatihan dan pengujian sistem.
3. Scanning (Pemindaian)
   Pada tahap ini dilakukan proses pemindaian terhadap jaringan untuk mengidentifikasi potensi celah keamanan serta pola trafik jaringan. Proses ini bertujuan untuk memahami karakteristik data yang akan digunakan dalam proses klasifikasi.
4. Exploitation (Eksploitasi)
   Tahap eksploitasi dilakukan dengan mensimulasikan serangan terhadap sistem untuk menguji kemampuan deteksi dari algoritma *Random Forest* serta efektivitas firewall dalam mencegah serangan yang terjadi.
5. Reporting (Pelaporan)
   Tahap akhir berupa analisis hasil pengujian sistem serta dokumentasi hasil penelitian. Pada tahap ini dilakukan evaluasi terhadap kinerja sistem dalam mendeteksi dan mencegah serangan jaringan.

Alur tahapan penelitian ini dapat digambarkan dalam bentuk diagram alur yang menunjukkan urutan proses dari tahap awal hingga tahap akhir penelitian. Metode ini umum digunakan dalam pengujian keamanan sistem karena mampu memberikan gambaran nyata terhadap celah keamanan yang ada [17].

2.2 Desain Pengujian

Metode yang digunakan dalam penelitian ini adalah algoritma *Random Forest* sebagai sistem deteksi dan *Windows Defender Firewall* sebagai sistem pencegahan. Kedua metode ini diintegrasikan untuk membentuk sistem keamanan jaringan yang bersifat deteksi sekaligus preventif.

Algoritma *Random Forest* digunakan untuk mengklasifikasikan trafik jaringan berdasarkan pola yang terbentuk dari data pelatihan. Proses klasifikasi dilakukan dengan membangun sejumlah *decision tree* yang bekerja secara paralel, kemudian hasil dari masing-masing *tree* digabungkan untuk menghasilkan keputusan akhir. Output dari proses ini berupa klasifikasi trafik jaringan menjadi dua kategori, yaitu trafik normal dan trafik berbahaya.

Sebelum proses klasifikasi dilakukan, data trafik jaringan terlebih dahulu melalui tahap preprocessing yang meliputi pembersihan data, transformasi fitur, serta normalisasi data untuk meningkatkan kualitas data masukan. Tahapan preprocessing merupakan langkah penting dalam pengembangan sistem deteksi intrusi karena dapat meningkatkan performa model klasifikasi dan mengurangi kesalahan prediksi. Beberapa penelitian menunjukkan bahwa proses normalisasi dan pemilihan fitur yang relevan dapat meningkatkan akurasi model Random Forest dalam mendeteksi serangan jaringan [15], [16].

Pada tahap pengujian, sistem akan melakukan pemantauan trafik jaringan secara real-time menggunakan packet sniffing. Data yang diperoleh kemudian diekstraksi menjadi sejumlah fitur yang digunakan sebagai input model Random Forest. Hasil klasifikasi berupa trafik normal atau trafik berbahaya akan menjadi dasar pengambilan keputusan oleh modul pencegahan. Apabila suatu alamat IP teridentifikasi melakukan aktivitas yang mencurigakan, sistem secara otomatis akan mengirimkan perintah ke Windows Defender Firewall untuk melakukan pemblokiran akses terhadap alamat IP tersebut. Mekanisme ini memungkinkan proses deteksi dan pencegahan berjalan secara otomatis tanpa memerlukan intervensi administrator jaringan.

Pendekatan integrasi antara machine learning dan firewall juga telah banyak digunakan dalam penelitian keamanan jaringan modern karena mampu membentuk sistem keamanan berlapis (layered security). Kombinasi tersebut tidak hanya meningkatkan kemampuan deteksi ancaman, tetapi juga mempercepat proses respons terhadap serangan yang teridentifikasi sehingga risiko kerusakan sistem dapat diminimalkan [16].

Setelah proses deteksi dilakukan, hasil klasifikasi digunakan sebagai dasar dalam menentukan tindakan pencegahan. Jika terdeteksi adanya aktivitas mencurigakan, maka sistem akan menerapkan aturan pada *Windows Defender Firewall* untuk memblokir akses atau trafik yang dianggap berbahaya.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

Integrasi antara *Random Forest* dan firewall memungkinkan sistem untuk bekerja secara otomatis dalam mendeteksi dan merespon ancaman keamanan jaringan. Pendekatan ini menciptakan sistem keamanan berlapis (*layered security*), di mana proses deteksi dan pencegahan dilakukan secara berkelanjutan.

Untuk mendukung implementasi sistem, digunakan beberapa komponen utama seperti perangkat komputer sebagai server, jaringan lokal sebagai lingkungan pengujian, serta perangkat lunak yang mendukung proses analisis data dan konfigurasi firewall. Penggunaan firewall sebagai mekanisme kontrol akses juga terbukti efektif dalam meningkatkan keamanan jaringan [11].

2.3 Alur Penelitian

Alur penelitian menggambarkan tahapan proses yang dilakukan dalam pengembangan sistem *Intrusion Detection and Prevention System* (IDPS) berbasis *Random Forest* yang diintegrasikan dengan *Windows Defender Firewall*. Alur ini disusun secara sistematis untuk memastikan setiap tahap penelitian berjalan sesuai dengan tujuan yang telah ditetapkan.

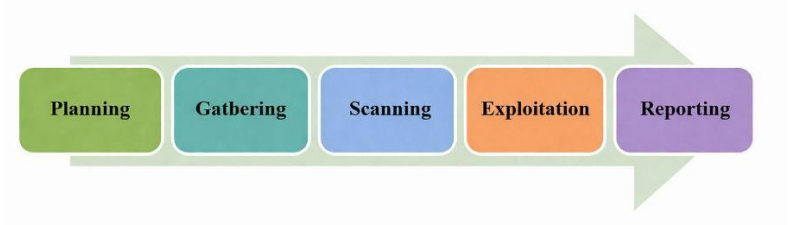
Alur penelitian dimulai dari tahap perencanaan hingga tahap pelaporan hasil penelitian. Pada tahap awal dilakukan identifikasi masalah serta analisis kebutuhan sistem keamanan jaringan. Selanjutnya dilakukan pengumpulan data trafik jaringan yang digunakan sebagai bahan analisis dan pelatihan model.

Setelah data diperoleh, dilakukan proses pemindaian (*scanning*) untuk mengidentifikasi pola trafik jaringan serta potensi celah keamanan yang ada. Data tersebut kemudian diproses menggunakan algoritma *Random Forest* untuk melakukan klasifikasi antara trafik normal dan trafik berbahaya.

Tahap berikutnya adalah proses eksploitasi (*exploitation*), yaitu melakukan simulasi serangan terhadap sistem untuk menguji kemampuan deteksi dan pencegahan yang telah dikembangkan. Pada tahap ini, sistem akan mendeteksi aktivitas mencurigakan dan secara otomatis menerapkan aturan pada *Windows Defender Firewall* untuk memblokir aktivitas tersebut.

Tahap akhir adalah pelaporan (*reporting*), yaitu melakukan analisis terhadap hasil pengujian serta mendokumentasikan kinerja sistem dalam mendeteksi dan mencegah serangan jaringan.

Alur penelitian ini dapat digambarkan dalam bentuk diagram seperti pada Gambar 1.



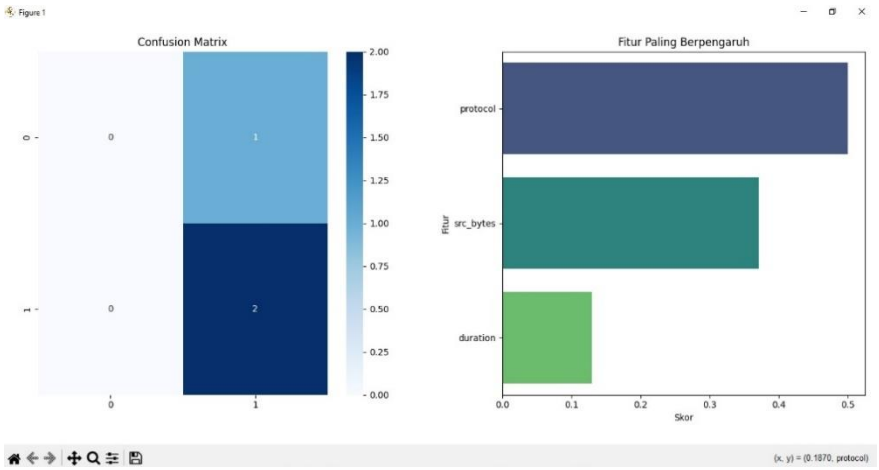
Gambar 1. Alur tahapan penelitian

3. HASIL DAN PEMBAHASAN

3.1 Evaluasi Performa Model AI

Pengembangan sistem ini dimulai dengan pelatihan model *Random Forest* menggunakan dataset trafik jaringan lokal. Analisis terhadap fitur yang paling berpengaruh menunjukkan bahwa **Protocol** memiliki kontribusi tertinggi terhadap keputusan model dengan skor **0.499**. Skor ini menunjukkan bahwa jenis protokol (TCP, UDP, ICMP) merupakan indikator paling valid untuk mendeteksi anomali pada jaringan lokal. Fitur **src_bytes** menyusul dengan skor **0.370**, sementara **duration** memberikan pengaruh sebesar **0.130**. Penggunaan algoritma *Random Forest* dalam klasifikasi trafik siber telah terbukti memberikan akurasi yang lebih stabil dibandingkan model linear tradisional .

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

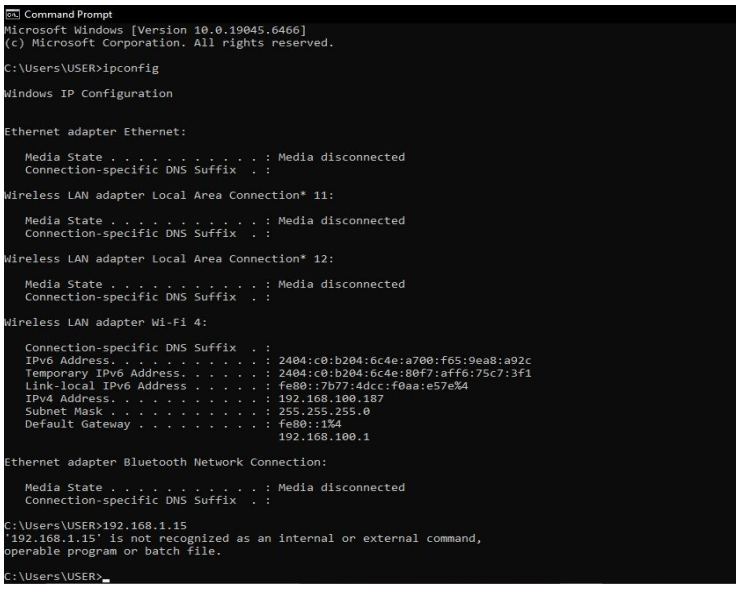


Gambar 2. Hasil Confusion Matrix dan Feature Importance Algoritma Random Forest

Berdasarkan *Confusion Matrix*, model mencapai akurasi sebesar **67%** pada data uji. Sistem berhasil memprediksi secara tepat 2 sampel serangan (*True Positive*), meskipun terdapat 1 kesalahan klasifikasi trafik normal yang dianggap sebagai anomali (*False Positive*). Nilai *F1-score* untuk kelas serangan yang mencapai **0.80** menunjukkan efektivitas model dalam mengenali ancaman siber meskipun dengan dataset yang terbatas.

3.2 Implementasi Deteksi dan Pencegahan Real-Time

Sistem IDPS dijalankan pada antarmuka jaringan aktif melalui modul main.py. Alamat IP target yang dipantau dalam pengujian ini adalah **192.168.100.187** menggunakan adapter *Wireless LAN Wi-Fi 4*. Implementasi *sniffing* paket dilakukan secara *real-time* menggunakan pustaka Scapy untuk menangkap paket IP yang melewati kartu jaringan tersebut. Integrasi sistem keamanan siber berbasis *Machine Learning* dengan alat keamanan sistem operasi merupakan strategi krusial untuk mempercepat waktu respons pertahanan [2].



Gambar 3. Hasil Konfigurasi Alamat IP pada Perangkat Pengujian Menggunakan Perintah ipconfig

Mekanisme pencegahan (IPS) diintegrasikan langsung dengan **Windows Defender Firewall**. Ketika model AI mendeteksi paket dengan label anomali, sistem secara otomatis mengeksekusi perintah PowerShell New-NetFirewallRule untuk memblokir IP sumber serangan tersebut. Pendekatan ini memungkinkan pemblokiran paket berbahaya secara dinamis tanpa memerlukan intervensi manual dari administrator jaringan [4].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

3.3 Pengujian Simulasi Serangan

Pengujian efektivitas sistem dilakukan menggunakan aplikasi *Nmap Wrapper* pada perangkat Android yang bertindak sebagai penyerang. Skenario pengujian meliputi pemindaian port (*fast port scan*) dengan perintah nmap -F dan deteksi OS dengan perintah -Pn. Pengujian dengan parameter -Pn sangat penting untuk memastikan paket tetap dikirimkan meskipun target mengabaikan protokol ICMP (ping) [5].

Hasil pengujian menunjukkan bahwa:

- Sistem berhasil mendeteksi pola pemindaian yang dilakukan oleh perangkat penyerang secara *real-time*.
- Setelah deteksi, sistem secara otomatis menambahkan aturan blokir pada *firewall*, yang mengakibatkan status penyerang berubah menjadi **"Host seems down"**.
- Pemindaian lanjutan oleh penyerang menghasilkan status **"0 hosts up"**, yang membuktikan bahwa akses IP penyerang telah diputus sepenuhnya oleh Windows Defender Firewall.

Tabel 1. Hasil Pengujian Sistem IDPS Berbasis Random Forest dan Windows Defender Firewall

Parameter	Sebelum Deteksi (Normal)	Sesudah Deteksi (Blocked)
Status Host	*Host is up*	*Host seems down*
Port Status	*Open/Unfiltered*	*100 filtered tcp ports*
Akses Jaringan	Terhubung penuh	Terputus total (*No-response*)

4. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, sistem Intrusion Detection and Prevention System (IDPS) berbasis Random Forest dan Windows Defender Firewall berhasil dikembangkan dan diimplementasikan dengan baik. Sistem mampu mengintegrasikan algoritma Random Forest sebagai metode deteksi dengan Windows Defender Firewall sebagai mekanisme pencegahan. Melalui pemanfaatan Python dan library Scapy, sistem dapat melakukan pemantauan serta analisis trafik jaringan secara real-time sehingga mampu mendeteksi aktivitas mencurigakan dan memberikan respons secara otomatis. Hasil pengujian menunjukkan bahwa model Random Forest mampu mengklasifikasikan trafik jaringan berdasarkan fitur-fitur penting seperti *protocol*, *src_bytes*, dan *duration*, dengan fitur *protocol* sebagai faktor yang paling dominan dalam proses deteksi. Selain itu, sistem juga berhasil menerapkan konsep *layered security* melalui kombinasi deteksi berbasis machine learning dan pencegahan berbasis firewall, sehingga tidak hanya mampu mendeteksi ancaman tetapi juga langsung melakukan tindakan pemblokiran terhadap sumber serangan. Meskipun demikian, penelitian ini masih memiliki beberapa keterbatasan, seperti penggunaan dataset yang terbatas, akurasi model yang masih dapat ditingkatkan, serta pengujian yang hanya difokuskan pada jenis serangan tertentu seperti *port scanning*. Untuk pengembangan penelitian selanjutnya, disarankan menggunakan dataset yang lebih besar dan seimbang guna meningkatkan performa model serta mengurangi tingkat *false positive*. Pengujian juga dapat diperluas dengan berbagai jenis serangan lain, seperti SQL Injection dan Brute Force, agar kemampuan sistem dapat dievaluasi secara lebih menyeluruh. Pengujian SQL Injection menggunakan metode OWASP dan platform DVWA telah banyak digunakan untuk mengidentifikasi kerentanan aplikasi web serta mengevaluasi efektivitas mekanisme pertahanan yang diterapkan. Selain itu, pengembangan antarmuka berbasis web atau desktop dapat dilakukan untuk memudahkan proses monitoring, disertai penambahan fitur notifikasi otomatis seperti Telegram Bot agar administrator dapat menerima informasi serangan secara cepat. Penggunaan framework keamanan yang lebih kuat serta pelaksanaan *penetration testing* secara berkala juga direkomendasikan untuk meningkatkan efektivitas dan keandalan sistem keamanan yang dikembangkan.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 613-619
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1054

REFERENCES

[1] M. Tahir, Hariyanto, M. I. Firdausi, Saim, Nuriyah, and Maimunah, "Peningkatan Keamanan Jaringan LAN dan WLAN Melalui Standard Acces Control List," *Digital Transformation Technology*, vol. 4, no. 1, pp. 607–614, 2024, doi: 10.47709/digitech.v4i1.4261.

[2] M. Tahir and A. B. Rifai, "Implementasi Firewall Filtering Pada Situs Web Dan Game Online Menggunakan Layer 7 Protocols Dan Manajemen Bandwidth Dengan Metode Hierarchical," *Jurnal Teknologi Informasi dan Komputer*, vol. 12, no. 1, pp. 130–141, 2026.

[3] R. S. Wiandani, M. Tahir, I. A. Dyransyha, and R. Ummah, "Identifikasi Serangan SQL Injection Berbantuan Aplikasi Pengujian Keamanan Web DVWA (Damn Vulnerable Web Application)," *Digital Transformation Technology*, vol. 5, no. 1, pp. 375–382, 2025, doi: 10.47709/digitech.v5i1.5922.

[4] A. M. Putri, M. Tahir, Bustomi, R. N. Fitriani, and N. Halimah, "Penerapan Keamanan Berlapis pada Jaringan WLAN dengan WPA / WPA2-PSK dan Captive Portal menggunakan MikroTik," *Jurnal RESTIKOM*, vol. 7, no. 1, pp. 38–50, 2025.

[5] S. Aljawarneh, M. Aldwairi, and M. O. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient classifiers," *Journal of Computational Science*, vol. 25, pp. 152–160, 2018, doi: 10.1016/j.jocs.2017.03.006.

[6] C. Lu, Y. Cao, and Z. Wang, "Research on Intrusion Detection Based on an Enhanced Random Forest Algorithm," *Applied Sciences*, vol. 14, no. 2, p. 714, 2024, doi: 10.3390/app14020714.

[7] X. Chen, "Intrusion Detection in IoT Networks Using Extra Trees , Random Forests , and Hybrid Optimization Algorithms," *Informatica*, vol. 49, pp. 283–302, 2025, doi: 10.31449/inf.v49i18.7734.

[8] M. T. Abdelaziz, A. Radwan, H. Mamdouh, A. S. Saad, A. S. Abuzaid, A. A. AbdElhakeem, S. Zakzouk, K. Moussa, and M. S. Darweesh, "Enhancing Network Threat Detection with Random Forest-Based NIDS and Permutation Feature Importance," *Journal of Network and Systems Management*, vol. 33, no. 1, 2025, doi: 10.1007/s10922-024-09874-0.

[9] R. C. Wang and R. P. Avrianto, "Improving Detection Accuracy of Network Intrusions Using a Hybrid Network Intrusion Detection System Based on Isolation Forest and Random Forest Algorithms," *Jurnal Teknik Informatika (JUTIF)*, vol. 6, no. 6, pp. 5371–5385, 2025.

[10] R. Hadi, R. Kurniyanto, and H. P. F. C, "Penerapan Firewall dan Intrusion Detection System pada Jaringan Komputer," *Journal of Computer Science and Information Technology*, vol. 2, no. 1, pp. 9–15, 2026, doi: 10.70716/jocsit.v2i1.411.

[11] C. Zhang, N. Wang, Y. T. Hou, and W. Lou, "Machine Learning-Based Intrusion Detection Systems: Capabilities, Methodologies, and Open Research Challenges," *TechRxiv Preprint*, 2025, doi: 10.36227/techrxiv.173627464.48290242.v1.

[12] N. Mishra and S. Mishra, "A Review of Machine Learning-based Intrusion Detection System," *EAI Endorsed Trans. Internet Things*, vol. 10, pp. 1–8, 2024, doi: 10.4108/eetiot.5332.

[13] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. 2013.

[14] Guntoro, Lisnawita, and L. Costaner, "Optimizing Random Forest for IoT Cyberattack Detection Using SMOTE : A Study on CIC-IoT2023 Dataset," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 25, no. 1, pp. 83–96, 2025, doi: 10.30812/matrik.v25i1.5382.

[15] F. H. Saputra and M. R. H, "Enhancing Intrusion Detection Using Random Forest and SMOTE on the NSL - KDD Dataset," *Journal of System and Computer Engineering (JSCE)*, vol. 6, no. 3, pp. 240–247, 2025, doi: 10.61628/jsce.v6i3.2056.

[16] F. Ardiansyah, N. N. Zuhra, L. Zahra, R. Alfarisyi, H. Nisa, and R. A. Astiyanto, "Implementasi Keamanan Jaringan Menggunakan Firewall dan Intrusion Detection System (IDS) pada Infrastruktur Jaringan Skala Kecil – Menengah," *JIKUM J. Ilmu Komput.*, vol. 2, no. 1, pp. 124–126, 2026.

[17] V. K. Pandey, S. Prakash, T. K. Gupta, and P. Sinha, "Enhancing intrusion detection in wireless sensor networks using a Tabu search based optimized random forest," *Scientific Reports*, vol. 15, Art. no. 18634, 2025, doi: 10.1038/s41598-025-03498-3.