JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu
E-Mail: jiifkom@sttrcepu.ac.id

Pendekatan *Machine Learning* untuk Deteksi Serangan *Man-in-the-Middle* Menggunakan *K-Nearest Neighbor*

Ahmad Rifqi Nugraha[a], Aryanti Aryanti[b*], Nurhajar Anugraha[c]
aryanti@polsri.ac.id
Politeknik Negeri Sriwijaya[abc]

Kata kunci:
Machine Learning, K-Nearest Neighbor, Man-in-the-Middle

Intisari

Teknologi jaringan nirkabel (Wi-Fi) telah meningkatkan kemampuan transmisi data, tetapi juga meningkatkan kerentanan terhadap ancaman keamanan siber, terutama serangan *Man-in-the-Middle* (MitM). Kerentanan yang dihasilkan oleh serangan ini memungkinkan individu yang tidak berwenang untuk mencegat dan mengubah komunikasi secara diam-diam. Metode *K-Nearest Neighbor* (KNN) disarankan untuk digunakan dalam sistem deteksi intrusi berbasis pembelajaran mesin. Dengan dataset sebanyak 800.000 entri yang dibagi dengan rasio 80:20 untuk pelatihan dan pengujian, model ini mencapai tingkat akurasi 89,22%. Hasil pengujian menunjukkan kinerja yang seragam dengan keseimbangan metrik *precision, recall*, dan *F1-Score* di kedua kelas, serta efisiensi waktu komputasi maksimum. Hasil ini memvalidasi kemampuan algoritma KNN untuk mengkategorikan lalu lintas jaringan dan kemampuan untuk berfungsi sebagai sistem deteksi otomatis serangan MitM.

Tentang naskah:
-diterima, 24 Juni 2026
-diterbitkan, 1 Juli 2026

Abstract

Wireless networking (Wi-Fi) technology has improved data transmission capabilities, but it has also increased vulnerability to cybersecurity threats, particularly Man-in-the-Middle (MitM) attacks. The vulnerabilities created by these attacks allow unauthorized individuals to intercept and alter communications surreptitiously. The K-Nearest Neighbor (KNN) method is proposed for use in a machine learning-based intrusion detection system. With a dataset of 800,000 entries divided in an 80:20 ratio for training and testing, the model achieved an accuracy rate of 89.22%. The test results showed uniform performance with a balance of precision, recall, and F1 score metrics across both classes, as well as maximum computational time efficiency. These results validate the KNN algorithm's ability to categorize network traffic and its ability to function as an automated MitM attack detection system.

Keywords:
Machine Learning, K-Nearest Neighbor, Man-in-the-Middle

1. Pendahuluan

Perkembangan Wi-Fi saat ini mengalami peningkatan yang pesat(Tan & Akbar, 2021). Meskipun jaringan nirkabel secara signifikan memfasilitasi interaksi dan pertukaran informasi, kemajuan teknologi ini juga memicu peningkatan kompleksitas tantangan keamanan siber, khususnya pada jaringan Wi-Fi. Salah satu dampak krusial dari pemanfaatan teknologi tersebut adalah tingginya kerentanan integritas data terhadap ancaman peretasan. (Abdallah et al., 2022). Kerentanan ini dapat digunakan oleh pihak yang tidak berwenang untuk melakukan berbagai bentuk serangan, seperti penyadapan dan manipulasi data, guna memperoleh keuntungan secara tidak sah.

Salah satu ancaman siber yang lazim ditemui pada jaringan Wi-Fi adalah serangan *Man-in-the-Middle* (MitM) (Gurav, 2026). Dalam skema ini, penyerang melakukan intersepsi terhadap kanal komunikasi antara dua pihak. Pelaku kemudian dapat melakukan pengawasan maupun penyamaran sebagai salah satu partisipan, sehingga komunikasi tetap terlihat autentik bagi korban.

Untuk mengatasi ancaman seperti serangan MitM, diperlukan suatu mekanisme keamanan yang mampu mendeteksi aktivitas mencurigakan pada jaringan. Salah satu solusi yang digunakan adalah Sistem deteksi intrusi (IDS) adalah sistem yang dimaksudkan untuk mengawasi lalu lintas jaringan.serta mengidentifikasi apakah suatu aktivitas atau paket data merupakan serangan atau bukan (Rahman et al., 2025).

Untuk mengatasi keterbatasan pada metode deteksi tradisional, diperlukan

pendekatan yang lebih adaptif dalam mengidentifikasi serangan jaringan. Salah satu pendekatan yang banyak digunakan adalah *machine learning* (ML), yaitu teknik yang memungkinkan sistem untuk mengambil informasi dan mengenali pola secara otomatis. Dalam konteks *Intrusion Detection System* (IDS), ML berperan dalam menganalisis lalu lintas jaringan serta mengklasifikasikan aktivitas normal dan aktivitas yang tergolong sebagai serangan. Penerapan ML dalam IDS terbukti mampu meningkatkan akurasi deteksi serta mendeteksi pola serangan baru yang tidak dapat diidentifikasi oleh metode berbasis *signature* (Berhili et al., 2024).

Banyak metode pembelajaran mesin telah dirancang untuk meningkatkan efektivitas Sistem Deteksi Intrusi (IDS), terutama *K-Nearest Neighbour* (KNN). Pada penelitian (*E-Issn : 2988-1986*, 2026) Pendekatan KNN menghasilkan data analitis dengan tingkat akurasi 50,5 %. KNN memiliki kelemahan pada proses komputasi yang relative

Tujuan penelitian ini adalah untuk menilai seberapa baik *algoritma K-Nearest Neighbor* (KNN) dapat mengidentifikasi serangan MitM pada jaringan nirkabel, menggunakan informasi yang diberikan di atas sebagai tolak ukur. Untuk menemukan algoritma terbaik dalam mendeteksi aktivitas serangan, para peneliti menjalankan algoritma tersebut melalui serangkaian tes Studi ini menilai berbagai metrik kinerja, termasuk akurasi, presisi, recall, dan skor F1. Dengan memberikan informasi untuk pengembangan Sistem Deteksi Intrusi (IDS) berbasis pembelajaran mesin, penelitian ini bertujuan untuk meningkatkan pertahanan jaringan nirkabel terhadap serangan.

2. Kerangka Teori

2.1. Machnine Learning

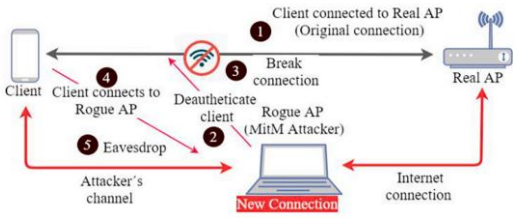
machine learning sebagai kapasitas sistem untuk belajar dari data pelatihan yang spesifik terhadap masalah tertentu guna mengotomatiskan proses pembangunan model analitik dan menyelesaikan tugas terkait. ML bekerja dengan menerapkan algoritma yang secara berulang belajar dari data pelatihan, sehingga komputer dapat menemukan wawasan tersembunyi dan pola kompleks tanpa diprogram secara eksplisi (Muchlinski, 2022).

2.2. K-Nearest Neighbor (KNN)

Algoritma KNN menentukanklasifikasi mengenaidata baru dengan cara menghitung kedekatan atau kemiripan terhadap sejumlah K data terdekat dalam dataset pelatihan (Aryanti et al., 2025). Kelebihan KNN antara lain kemudahan implementasi, kemampuan bekerja dengan banyak kelas, dan tidak memerlukan proses pelatihan rumit. Namun, KNN juga memiliki kelemahan, seperti sensitif terhadap dataset yang noisy dan biaya komputasi tinggi apabila dataset sangat besar. Dengan karakteristiknya yang berbasis pengukuran jarak dan pola tetangga terdekat, KNN sering digunakan dalam berbagai aplikasi klasifikasi, termasuk deteksi intrusi jaringan, prediksi klinis, dan pengenalan pola. Karakteristik ini membuat KNN relevan dipertimbangkan untuk sistem deteksi serangan seperti *Man-in-the-Middle*, di mana pola trafik abnormal perlu dikenali secara efektif (Hendriyanto & Sari, 2022)

2.3. Man-in-the-Middle

Sebuah jenis intrusi siber yang dikenal sebagai serangan *Man-in-the-Middle* melibatkan intersepsi komunikasi antara dua pihak secara terselubung, tanpa diketahui oleh pihak yang terlibat. (Auliafitri et al., 2024), kemudian mencegat informasi pribadi (Ali & Al-Sharafi, 2025). Termasuk kredensial login MitM umumnya mencakup berbagai jenis serangan di mana pelaku mengendalikan saluran komunikasi dan mengalihkan koneksi asli guna mengintersep atau mengubah data yang ditukarkan (Fereidouni et al., 2025).



Gambar 2. 1 Rekayasa MitM

2.4. Wiresahrk

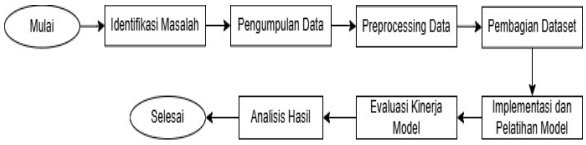
Wireshark adalah program untuk mengambil paket data yang berbasis open-source. (Rakhmadi Rahman; Ghina R.S Odja, 2024). Wireshark merupakan salah satu *tools* analisis paket paling terkenal yang digunakan untuk memantau lalu

lintas jaringan (B et al., 2023). Wireshark memungkinkan analis untuk memantau dan meneliti lalu lintas data, mengidentifikasi masalah seperti penyalahgunaan jaringan, koneksi berbahaya, dan penurunan kinerja (Soepeno, 2023). Wireshark mampu menangkap semua paket data yang melewati jaringan tempat paket tersebut diarahkan (Syaiful Haq, 2025). Wireshark kompatibel dengan berbagai sistem, termasuk Windows, Linux, dan MacOS, menjadikannya alat yang serbaguna untuk berbagai skenario dan jenis jaringan. (Mustofa et al., 2025)

3. Metodologi

3.1 Metodologi Penelitian

Alur penelitian disusun sebagai pedoman untuk menggambarkan proses penelitian secara sistematis dan terstruktur. Alur ini menunjukkan keterkaitan antarproses yang dilakukan dalam penelitian serta memberikan gambaran menyeluruh mengenai mekanisme pelaksanaannya. Dengan adanya alur yang jelas, setiap proses dapat dilaksanakan secara terarah dan sesuai dengan tujuan penelitian, sehingga mendukung diperolehnya hasil yang valid dan dapat dipertanggungjawabkan.



Gambar 3. 1 Tahapan Penelitian

Untuk memberikan pemahaman yang lebih baik tentang proses penelitian, setiap langkah yang ditunjukkan pada Gambar 3.1 dijelaskan sebagai berikut.

1. Mulai
2. Identifikasi Masalah
   Tujuan dari langkah ini adalah untuk menemukan masalah penelitian, yaitu serangan MitM, yang memungkinkan individu yang tidak berwenang mengubah komunikasi data. Akibatnya, penelitian ini dilakukan untuk mengevaluasi kinerja algoritma pembelajaran mesin dalam mendeteksi serangan dengan data trafik jaringan.
3. Pengumpulan Data
   Pada tahap ini dilakukan proses akuisisi data trafik jaringan menggunakan perangkat lunak Wireshark. Data yang diperoleh mencakup trafik jaringan dalam kondisi normal serta trafik ketika terjadi serangan. Kedua jenis data tersebut digunakan sebagai sumber data utama untuk proses analisis dan pengujian model pada penelitian ini. terjadi serangan.
4. Pembagian Dataset
   Data yang telah dihimpun kemudian dipartisi menjadi data latih dan data uji. Prosedur ini bertujuan untuk melatih model pada sebagian data serta menguji kapabilitas klasifikasinya menggunakan data yang berbeda, sehingga evaluasi performa model dapat dilakukan secara objektif.
5. Implementasi dan Pelatihan Model
   Algoritma *machine learning* yang dipilih diimplementasikan dan dilatih menggunakan data latih (*training data*) yang telah disiapkan sebelumnya. Proses pelatihan bertujuan untuk membentuk model yang mampu membedakan antara trafik normal dan trafik yang mengandung serangan MitM berdasarkan pola yang dipelajari dari data. Model yang dihasilkan kemudian digunakan pada tahap evaluasi untuk mengukur performanya dalam mendeteksi serangan tersebut.
6. Evaluasi Kinerja Model
   Kinerja model dievaluasi melalui data uji untuk menilai kapabilitas klasifikasi trafik jaringan. Efektivitas model dalam mendeteksi serangan MitM diukur menggunakan sejumlah metrik penting seperti akurasi, precision, recall, dan skor F1.
7. Analisis Hasil
   Hasil evaluasi model dianalisis berdasarkan nilai metrik kinerja yang diperoleh untuk menilai kemampuan model dalam mengklasifikasikan trafik normal dan trafik serangan MitM. Analisis tersebut menjadi dasar dalam penyusunan kesimpulan terkait performa algoritma machine learning yang diterapkan pada penelitian ini.
8. Selesai

3.2. Pengujian dan Evaluasi Model

Pengujian sistem dilakukan untuk mengevaluasi performa algoritma KNN dalam mendeteksi serangan MitM *Attack*

berdasarkan data trafik jaringan. Pengujian dilakukan dengan mengukur kemampuan algoritma dalam mengklasifikasikan trafik jaringan ke dalam kategori normal dan serangan. Hasil yang diperoleh selanjutnya dianalisis menggunakan metrik evaluasi yang telah ditentukan.

1. Pengujian Menggunakan Data Uji
   Pengujian model dilakukan dengan data pengujian untuk menilai kemampuan generalisasi algoritma KNN pada data yang belum diproses sebelumnya. Hasil pengujian kemudian dianalisis menggunakan ukuran penilaian yang relevan untuk menilai efektivitas model dalam mengidentifikasi serangan MitM secara akurat.
2. Proses Klasifikasi Data
   Proses klasifikasi data dilakukan menggunakan algoritma KNN untuk mengelompokkan data trafik jaringan ke dalam dua kategori, yaitu trafik normal dan trafik serangan MitM *Attack*. Pada proses ini, model memanfaatkan pola yang telah dipelajari selama tahap pelatihan untuk menentukan kelas dari setiap data uji yang diberikan. Hasil klasifikasi kemudian digunakan sebagai landasan untuk menilai kinerja model.
3. Evaluasi Kinerja Model
   Evaluasi model dilakukan untuk mengukur kapabilitas klasifikasi data trafik jaringan ke dalam kategori normal maupun serangan. Kinerja model dinilai melalui serangkaian metrik evaluasi yang ditetapkan guna menentukan tingkat akurasi serta efektivitas dalam mendeteksi serangan MitM.
   1) *Accuracy*
      Metrik ini digunakan untuk mengukur proporsi data yang berhasil diklasifikasikan dengan benar oleh model terhadap total data yang diuji. Hasil pengukuran tersebut menjadi salah satu indikator dalam mengevaluasi tingkat kinerja dan efektivitas model klasifikasi (Syafrizal et al., 2024).

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

   2) *Precision*
      Metrik ini digunakan untuk mengukur tingkat ketepatan model dalam mengidentifikasi data yang benar-benar termasuk serangan dari seluruh data yang diprediksi sebagai serangan, sehingga memberikan gambaran mengenai kemampuan model dalam menghasilkan prediksi positif yang akurat dan mengurangi jumlah kesalahan positif (*false positive*) (Syafrizal et al., 2024)

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

   3) *Recall*
      Metrik ini digunakan untuk mengukur kemampuan model dalam mengidentifikasi seluruh data kategori serangan secara tepat dibandingkan dengan total data serangan yang sebenarnya. Hal ini memberikan gambaran komprehensif mengenai tingkat sensitivitas dan efektivitas model dalam mendeteksi ancaman yang ada pada dataset (Syafrizal et al., 2024).

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

   4) *F1-Score*
      F1-score merupakan nilai rata-rata harmonis antara precision dan recall yang berfungsi untuk mengevaluasi keseimbangan performa model. Metrik ini menjadi indikator krusial saat diperlukan titik temu antara ketepatan prediksi dan kemampuan deteksi, terutama pada dataset dengan distribusi kelas yang tidak seimbang. (Syafrizal et al., 2024).

$$F1 = \frac{2TP}{2TP + FP + FN}$$

   5) *Confusion matrix*
      Metode ini memungkinkan analisis menyeluruh terhadap hasil klasifikasi dengan menyajikan rincian jumlah

prediksi tepat dan keliru untuk setiap kelas. Dengan demikian, evaluasi performa model dapat dilakukan secara lebih mendalam, termasuk dalam mengidentifikasi kesalahan klasifikasi seperti *false positive* maupun *false negative*.

4. Analisis Hasil Pengujian
   Nilai metrik evaluasi yang dihasilkan dari proses pengujian digunakan untuk melakukan analisis hasil pengujian. Tujuan analisis adalah untuk mengetahui seberapa efektif dan andal model dalam mengklasifikasikan data. Selanjutnya, temuan ini digunakan sebagai dasar penyusunan hasil penelitian.

4. Hasil dan Pembahasan

Bagian ini menyajikan hasil dari proses klasifikasi dan evaluasi kinerja model yang dilakukan dalam penelitian. Analisis difokuskan pada kemampuan model dalam mengklasifikasikan data trafik jaringan serta menilai tingkat efektivitasnya berdasarkan metrik evaluasi yang digunakan.

4.1. Representasi Fitur Hasil Ekstraksi Data Trafik Jaringan

Data trafik jaringan yang telah melalui proses preprocessing direpresentasikan dalam bentuk sejumlah atribut atau fitur yang digunakan sebagai masukan pada model klasifikasi. Fitur-fitur tersebut digunakan untuk merepresentasikan karakteristik setiap data sehingga dapat diproses lebih lanjut oleh model. Detail fitur yang digunakan ditunjukkan pada Tabel 4.1.

Tabel 4. 1 Dataset

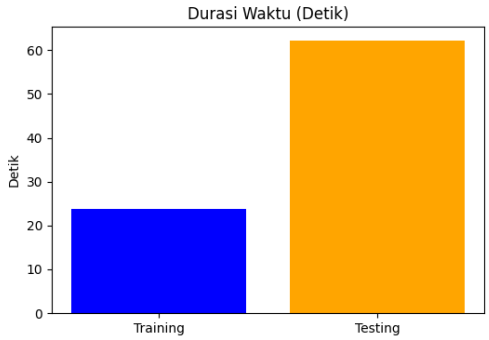
Dataset	Jumlah Data
Training	640.000
Testing	160.000
Total	800.000

Sesuai dengan Tabel 4.1, penelitian ini memanfaatkan dataset trafik jaringan berjumlah 800.000 data. Dataset tersebut dibagi ke dalam dua bagian dengan rasio 80:20, yaitu 640.000 data untuk proses pelatihan dan 160.000 data untuk proses pengujian.Pembagian proporsional ini dirancang untuk memastikan model mendapatkan cakupan pola yang luas guna pembelajaran, sekaligus menyediakan data yang memadai untuk evaluasi yang objektif.

Data uji digunakan untuk menguji generalisasi model, sementara data latih digunakan untuk membuat model klasifikasi, terhadap data yang belum pernah diproses sebelumnya. Pemilihan rasio 80:20 bertujuan untuk menyeimbangkan kebutuhan antara fase pelatihan dan evaluasi, sehingga performa model dapat diukur dengan lebih akurat dan andal. Dengan skema pembagian data yang sistematis ini, efektivitas model dalam mendeteksi serangan dapat dinilai secara optimal.

4.2. Waktu Eksekusi Mode

Gambar 4.1 menunjukkan perbandingan waktu yang dibutuhkan model pada proses pelatihan (*training*) dan pengujian (*testing*). Berdasarkan hasil pengukuran, proses pelatihan memerlukan waktu sekitar 24 detik, sedangkan proses pengujian memerlukan waktu sekitar 62 detik. Perbedaan tersebut menunjukkan bahwa proses pengujian membutuhkan waktu komputasi yang lebih besar dibandingkan proses pelatihan. Hal ini disebabkan karena model harus melakukan proses klasifikasi terhadap seluruh data uji yang tersedia. Meskipun demikian, waktu eksekusi yang diperoleh masih tergolong efisien mengingat jumlah data yang digunakan dalam penelitian mencapai 800.000 data. Hasil ini menunjukkan bahwa model memiliki kemampuan untuk menjalankan prosedur klasifikasi dengan
waktu komputasi yang relatif singkat.

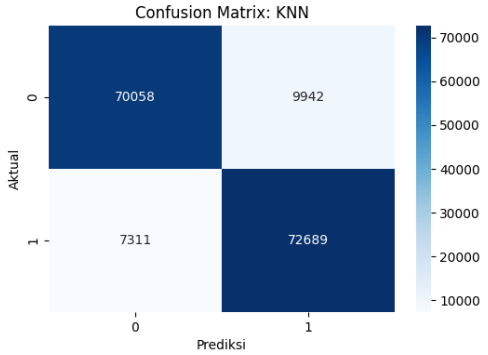


Gabar 4. 1 Perbandingan waktu eksekusi pada proses training dan testing

4.3. Evaluasi Hasil Klasifikasi

Visualisasi *Confusion Matrix* pada Gambar 4.2 memperlihatkan kinerja klasifikasi model secara lebih mendalam. Model berhasil mengidentifikasi dengan tepat 70.058 data pada kelas 0 dan 72.689

data pada kelas 1. Di sisi lain, terdapat 9.942 data kelas 0 yang terklasifikasi secara keliru ke dalam kelas 1, serta 7.311 data kelas 1 yang salah diprediksi sebagai kelas 0. Secara keseluruhan, dominasi prediksi yang benar dibandingkan dengan kesalahan prediksi menunjukkan kapabilitas model yang baik dalam membedakan kedua kelas. Selain itu, distribusi kesalahan klasifikasi yang relatif seimbang di kedua kelas menunjukkan bahwa model bersifat netral dan tidak bias terhadap kelas tertentu; ini menunjukkan bahwa model itu netral.



Gabar 4. 2 Confusion Matrix

4.4 Evaluasi Kinerja Model Berdasarkan Metrik Evaluasi

Tabel 4.2 merangkum evaluasi kinerja model menggunakan metrik klasifikasi utama seperti ketepatan, recall, dan skor F1, untuk memberikan gambaran komprehensif mengenai efektivitas klasifikasi.

Tabel 4. 2 Metrik Evaluasi

Kelas	Presidion	Recall	F1-Score	Support
0	0.91	0.88	0.89	80000
1	0.88	0.91	0.89	80000
Accuracy			0.89	

Berdasarkan evaluasi performa model yang disajikan pada Tabel 4.2, nilai *precision* sebesar 0,91, *recall* 0,88, dan *F1-score* 0,89 menunjukkan bahwa model memiliki kemampuan klasifikasi yang baik dengan tingkat sensitivitas yang tinggi pada kedua kelas. Dengan akurasi total mencapai 89,22%, model ini terbukti mampu mengklasifikasikan data uji secara akurat serta menunjukkan konsistensi yang stabil dalam mendeteksi serangan. Hasil penelitian ini memberikan kontribusi yang signifikan jika dibandingkan dengan studi terdahulu (*E-Issn : 2988-1986*, 2026) yang menerapkan pendekatan KNN dengan tingkat akurasi sebesar 50,5%. Peningkatan performa yang dicapai dalam penelitian ini mengonfirmasi bahwa model yang diusulkan memiliki keunggulan yang lebih kompetitif dalam mengidentifikasi trafik berbahaya pada jaringan nirkabel dibandingkan dengan pendekatan pada studi tersebut.

5. Simpulan

Penelitian ini menunjukkan bahwa algoritma *K-Nearest Neighbor* (KNN) mampu mendeteksi serangan *Man-in-the-Middle* (MitM) pada jaringan nirkabel dengan tingkat akurasi yang baik. Melalui perolehan nilai *precision* 0,91, *recall* 0,88, dan *F1-score* 0,89, model yang diusulkan membuktikan kemampuan klasifikasi yang akurat serta sensitivitas yang tinggi dalam mengenali trafik berbahaya secara otomatis. Keunggulan model ini terletak pada keseimbangan metrik evaluasi yang optimal dan efisiensi waktu komputasi yang memadai. Meskipun demikian, penelitian ini memiliki keterbatasan karena cakupan jenis serangan yang diuji masih terbatas pada deteksi MitM. Oleh karena itu, pengembangan riset selanjutnya diharapkan dapat mengeksplorasi penggunaan dataset yang lebih beragam untuk mencakup berbagai ancaman siber lainnya, serta melakukan optimasi parameter algoritma agar performa deteksi dapat ditingkatkan pada lingkungan jaringan yang lebih kompleks dan dinamis.

Daftar Pustaka

Abdallah, E. E., Eleisah, W., & Otoom, A. F. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. *Procedia Computer Science*, *201*(C), 205–212. https://doi.org/10.1016/j.procs.2022.03.029

Ali, M. A., & Al-Sharafi, S. A. H. (2025). Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation. *Discover Internet of Things*, *5*(1). https://doi.org/10.1007/s43926-025-00104-w

Aryanti, A., Putri Daviana, F., Dhia Ulhaq, N., Riswanto, M., Dio Alfajri, M., & Trisya Novita, N. (2025). Perbandingan Metode K-Nearest Neighbor dan Logistic Regression dalam Klasifikasi Dini Anemia Berdasarkan Parameter Hematologi Dasar. *Jurnal Riset Rekayasa Elektro*, *7*(2), 251–258.

Auliafitri, D., RizkiSuro, E., Malik, M. R. M., & Setiawan, A. (2024). Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit. *Journal of Internet and Software Engineering*, *1*(3), 12. https://doi.org/10.47134/pjise.v1i3.2620

B, N. A. L. M., Jassim, H., & Mani, J. (2023). Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022). In *Proceedings of the 1st International Conference on Innovation in*

Information Technology and Business (ICIITB 2022). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-110-4

Berhili, M., Chaieb, O., & Benabdellah, M. (2024). Intrusion Detection Systems in IoT Based on Machine Learning: A state of the art. *Procedia Computer Science*, *251*, 99–107. https://doi.org/10.1016/j.procs.2024.11.089

E-issn : 2988-1986. (2026). *10*(12), 1–11.

Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and Man-in-the-Middle Attacks. *Security and Privacy*, *8*(2). https://doi.org/10.1002/spy2.70016

Gurav, R. (2026). *Detect Man-In-The-Middle Attack using ARP Analysis*. 1–10. https://doi.org/10.55041/ISJEM05445

Hendriyanto, M. D., & Sari, B. N. (2022). Penerapan Algoritma K-Nearest Neighbor Dalam Klasifikasi Judul Berita Hoax. *Jurnal Ilmiah Informatika*, *10*(02), 80–84. https://doi.org/10.33884/jif.v10i02.5477

Muchlinski, D. (2022). Machine learning and deep learning. *Elgar Encyclopedia of Technology and Politics*, 114–118. https://doi.org/10.4337/9781800374263.machine.learning.deep

Mustofa, D., Saputra, D. I. S., & Apitiadi, S. D. (2025). Analisis Kinerja Kualitas Layanan Jaringan Internet dengan HTB dan OLT Menggunakan Wireshark di Media Computindo. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(11), 3051–3060. https://doi.org/10.52436/1.jpti.911

Rahman, R., Leksona, A. Y. N., & Afiqah. (2025). Serangan Man-In-The-Middle (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra). *Jejak Digital Jurnal Ilmiah Multidisplin*, *1*(4b), 2145–2156. https://doi.org/10.63822/np7skj98

Rakhmadi Rahman; Ghina R.S Odja. (2024). *Technology Sciences Insights Journal*. *d*, 0–3.

Soepeno, R. A. A. P. (2023). Wireshark: An Effective Tool for Network Analysis. *CYBV - Introductory Methods of Network Analysis*, (September), 1–15. https://www.researchgate.net/publication/374675769_Wireshark_An_Effective_Tool_for_Network_Analysis

Syafrizal, Afdal, M., & Novita, R. (2024). Sentiment Analysis of PLN Mobile Application Review Using Naïve Bayes Classifier and K-Nearest Neighbor Algorithm. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(January), 10–19.

Syaiful Haq, M. (2025). Analisis Keamanan Jaringan Nirkabel dari Packet Sniffing pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo. *Jurnal Ilmu Komputer*, *1*(2). https://e-journal.my.id/Peripheral/index

Tan, F., & Akbar, A. (2021). Sistem Informasi Pemetaan Wifi Gratis Diskominfo Kabupaten Hulu Sungai Selatan. *Jurnal Pranala*, *16*(1), 19–26.

Abdallah, E. E., Eleisah, W., & Otoom, A. F. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. *Procedia Computer Science*, *201*(C), 205–212. https://doi.org/10.1016/j.procs.2022.03.029

Ali, M. A., & Al-Sharafi, S. A. H. (2025). Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation. *Discover Internet of Things*, *5*(1). https://doi.org/10.1007/s43926-025-00104-w

Aryanti, A., Putri Daviana, F., Dhia Ulhaq, N., Riswanto, M., Dio Alfajri, M., & Trisya Novita, N. (2025). Perbandingan Metode K-Nearest Neighbor dan Logistic Regression dalam Klasifikasi Dini Anemia Berdasarkan Parameter Hematologi Dasar. *Jurnal Riset Rekayasa Elektro*, *7*(2), 251–258.

Auliafitri, D., RizkiSuro, E., Malik, M. R. M., & Setiawan, A. (2024). Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit. *Journal of Internet and Software Engineering*, *1*(3), 12. https://doi.org/10.47134/pjise.v1i3.2620

B, N. A. L. M., Jassim, H., & Mani, J. (2023). Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022). In *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*. Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-110-4
Berhili, M., Chaieb, O., & Benabdellah, M. (2024). Intrusion Detection Systems in IoT Based on Machine Learning: A state of the art. *Procedia Computer Science*, *251*, 99–107. https://doi.org/10.1016/j.procs.2024.11.089

E-issn : 2988-1986. (2026). *10*(12), 1–11.

Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and Man-in-the-Middle Attacks. *Security and Privacy*, *8*(2). https://doi.org/10.1002/spy2.70016

Gurav, R. (2026). *Detect Man-In-The-Middle Attack using ARP Analysis*. 1–10. https://doi.org/10.55041/ISJEM05445

Hendriyanto, M. D., & Sari, B. N. (2022). Penerapan Algoritma K-Nearest Neighbor Dalam Klasifikasi Judul Berita Hoax. *Jurnal Ilmiah Informatika*, *10*(02), 80–84. https://doi.org/10.33884/jif.v10i02.5477

Muchlinski, D. (2022). Machine learning and deep learning. *Elgar Encyclopedia of Technology and Politics*, 114–118. https://doi.org/10.4337/9781800374263.machine.learning.deep

Mustofa, D., Saputra, D. I. S., & Apitiadi, S. D. (2025). Analisis Kinerja Kualitas Layanan Jaringan Internet dengan HTB dan OLT Menggunakan Wireshark di Media Computindo. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(11), 3051–3060. https://doi.org/10.52436/1.jpti.911

Rahman, R., Leksona, A. Y. N., & Afiqah. (2025). Serangan Man-In-The-Middle (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra). *Jejak Digital Jurnal Ilmiah Multidisplin*, *1*(4b), 2145–2156. https://doi.org/10.63822/np7skj98

Rakhmadi Rahman; Ghina R.S Odja. (2024). *Technology Sciences Insights Journal*. *d*, 0–3.

Soepeno, R. A. A. P. (2023). Wireshark: An Effective Tool for Network Analysis. *CYBV - Introductory Methods of Network Analysis*, (September), 1–15. https://www.researchgate.net/publication/374675769_Wireshark_An_Effective_Tool_for_Network_Analysis

Syafrizal, Afdal, M., & Novita, R. (2024). Sentiment Analysis of PLN Mobile Application Review Using Naïve Bayes Classifier and K-Nearest Neighbor Algorithm. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(January), 10–19.

Syaiful Haq, M. (2025). Analisis Keamanan Jaringan

Nirkabel dari Packet Sniffing pada Kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Palopo. *Jurnal Ilmu Komputer*, *1*(2). https://e-journal.my.id/Peripheral/index

Tan, F., & Akbar, A. (2021). Sistem Informasi Pemetaan Wifi Gratis Diskominfo Kabupaten Hulu Sungai Selatan. *Jurnal Pranala*, *16*(1), 19–26.