Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14356 p-ISSN : 2089-9424

Terbit : 21 Desember 2024

Peran Artificial Intelligence dalam Deteksi Dini Ancaman Keamanan Jaringan

[1]Andi Purnomo, [2]Aliyah Kurniasih, [3]Ahlijati Nuraminah, [4]Sri Hartati
[1, 2,3,4] Universitas Ary Ginanjar

[1]andi.purnomo@uag.ac.id, [2]aliyah.kurniasih@uag.ac.id, [3]ahlijati.nuarminah@uag.ac.id, srihartati@uag.ac.id,

ABSTRAK

Keamanan jaringan komputer menghadapi tantangan yang semakin kompleks seiring dengan meningkatnya volume dan variasi ancaman, seperti serangan *Distributed Denial of Service (DDoS)*, malware, dan eksploitasi kerentanan. Pendekatan tradisional dalam deteksi dan mitigasi ancaman sering kali tidak cukup responsif terhadap pola serangan yang dinamis dan canggih. Teknologi kecerdasan buatan *(Artificial Intelligence/AI)*, khususnya *Machine Learning* (ML), menawarkan pendekatan baru yang lebih adaptif dan proaktif.Penelitian ini bertujuan untuk menganalisis peran AI dalam meningkatkan keamanan jaringan melalui penerapan berbagai algoritma ML, seperti *Naïve Bayes Classifier*, *Support Vector Machine* (SVM), *Decision Tree*, dan *Random Forest*. Pendekatan ini memungkinkan analisis data dalam jumlah besar secara real-time, identifikasi pola anomali, dan deteksi dini terhadap serangan yang belum teridentifikasi sebelumnya. Hasil tinjauan literatur menunjukkan bahwa algoritma *Machne Learning* mampu meningkatkan akurasi deteksi ancaman hingga 95% dalam berbagai studi kasus. Meskipun demikian, beberapa tantangan masih dihadapi, seperti tingkat false positives yang tinggi, keterbatasan data pelatihan, dan kebutuhan infrastruktur yang signifikan. Untuk mengatasi tantangan ini, diperlukan pengembangan algoritma yang lebih efisien serta integrasi AI dengan teknologi lain, seperti *blockchain* dan *Software-Defined Networking* (SDN).Penelitian ini menyimpulkan bahwa AI memiliki potensi besar untuk menjadi komponen kunci dalam strategi keamanan jaringan *modern*, dengan memberikan solusi yang lebih cepat, akurat, dan skalabel dalam mendeteksi dan merespons ancaman keamanan siber.

Kata Kunci: Keamanan jaringan, kecerdasan buatan, *Machine Learning*, deteksi intrusi, mitigasi ancaman.

PENDAHULUAN

Di era digital saat ini, jaringan komputer memainkan peran vital dalam hampir setiap aspek kehidupan, mulai dari bisnis, pendidikan, hingga pemerintahan. Namun, seiring dengan semakin kompleks dan terintegrasinya infrastruktur jaringan, ancaman terhadap keamanan siber juga meningkat secara signifikan. Serangan siber, seperti Distributed Denial of Service (DDoS), malware, dan intrusi jaringan, dapat menyebabkan kerugian yang sangat besar, baik dari segi finansial maupun reputasi.(Polgan et al., 2024). Menurut laporan terbaru dari *Cybersecurity* Ventures, kerugian global akibat serangan Infrastruktur jaringan diperkirakan akan mencapai $6 triliun pada tahun 2021, meningkat dari $3 triliun pada tahun 2015, Angka-angka ini mencerminkan dampak devastatif yang dapat ditimbulkan oleh serangan Infrastruktur jaringan, mulai dari gangguan operasional, kehilangan data penting, hingga biaya pemulihan yang tinggi (Bazrafshan (Akbar & Sutabri, 2024). Oleh karena itu, diperlukan pendekatan yang lebih canggih dan adaptif dalam menghadapi tantangan keamanan ini.

Dalam beberapa tahun terakhir, kecerdasan buatan (AI) telah muncul sebagai solusi yang menjanjikan untuk mengatasi tantangan ini. AI menawarkan kemampuan untuk memproses dan menganalisis data dengan cepat serta mengidentifikasi pola dan anomali yang mungkin sulit dideteksi oleh manusia atau sistem tradisional(Sinaga et al., 2024). Dengan kemampuannya dalam

Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14356 p-ISSN : 2089-9424

memproses data secara *rea-ltime* dan memberikan analisis yang mendalam, AI dapat membantu organisasi dalam berbagai aspek operasional dan strategis(Zulkarnain et al., 2024).Selain itu, AI dapat memproses data dalam skala besar dengan kecepatan yang jauh lebih tinggi daripada manusia, memungkinkan deteksi dan respons yang lebih cepat terhadap ancaman.(Simanjuntak et al., 2024). Teknologi kecerdasan buatan (AI) memberikan kontribusi besar dalam keamanan siber, memungkinkan sistem untuk mendeteksi anomali dan pola serangan secara *real-time*, sehingga potensi serangan dapat dicegah sebelum menyebabkan kerusakan.(Hafsah et al., 2024).

Salah satu pendekatan teknologi AI yang dapat digunakan untuk deteksi intrusi pada jaringan komputer adalah penggunaan teknik *Machine Learning*. Algoritma *Machine Learning* menganalisis data besar, mengklasifikasikan, mencocokkan, mendeteksi, dan melaporkan jejak penyusupan.(Tan et al., 2023). Terdapat tiga algoritma *Machine Learning* yang secara luas digunakan untuk meningkatkan deteksi ancaman keamanan jaringan, yaitu *Naïve Bayes Classifier, Support Vector Machine (SVM), dan Decision Tree*(Zy et al., 2023).

Namun, meskipun teknologi ini memiliki potensi besar dalam meningkatkan keamanan Jaringan , penerapannya tidak lepas dari tantangan. Salah satu tantangan utama adalah masalah *false positive*, di mana sistem dapat salah mengklasifikasikan aktivitas normal sebagai mencurigakan, yang dapat mengganggu operasi normal organisasi(Wardhani, 2024).

Oleh karena itu, melalui Literature Review ini, penelitian diharapkan dapat menjadi acuan bagi penerapan teknologi kecerdasan buatan (AI) yang memanfaatkan *algoritma Machine Learning*, agar dapat meningkatkan efektivitas deteksi dan mitigasi ancaman keamanan jaringan komputer secara real-time, dengan tingkat akurasi yang tinggi dalam mengidentifikasi anomali dan pola serangan. Penelitian ini bertujuan utnuk mengetahui sejauh mana teknologi kecerdasan buatan (AI), khususnya *algoritma Machine Learning*, dapat meningkatkan efektivitas deteksi dan mitigasi ancaman keamanan pada jaringan komputer, serta dapat menjadi rekomendasi berbasis hasil penelitian untuk mendukung implementasi AI dalam meningkatkan keamanan jaringan.

TINJAUAN PUSTAKA

Keamanan Jaringan

Keamanan jaringan merupakan praktik yang dilakukan untuk melindungi sistem komputer, perangkat, dan data dari ancaman baik yang berasal dari dalam maupun luar jaringan(Khairunnisa et al., 2024). Konsep dan Tantangan Keamanan jaringan komputer adalah bidang yang berfokus pada perlindungan integritas, kerahasiaan, dan ketersediaan data yang dikirimkan melalui jaringan. Ancaman terhadap jaringan komputer mencakup berbagai jenis serangan, seperti serangan *Distributed Denial of Service (DDoS), malware, sniffing*, dan berbagai bentuk intrusi lainnya(Polgan et al., 2024)

Machine Learning

Machine learning telah menjadi salah satu pendekatan AI yang paling populer dan banyak dieksplorasi dalam mendeteksi malware(Akbar & Sutabri, 2024). *Machine Learning*, juga dikenal sebagai pembelajaran mesin, merupakan ilmu komputer yang bekerja tanpa diprogram secara eksplisit, Pembelajaran mesin merupakan kecerdasan buatan yang mempelajari cara membuat data(Tjahjadi & Santoso, 2023). Dalam konteks deteksi intrusi, *supervised learning* lebih umum digunakan, terutama dengan algoritma seperti *Naïve Bayes Classifier, Support Vector Machine (SVM), dan Decision Tree, Random Forest* yang telah terbukti efektif dalam berbagai studi(Polgan et al., 2024) :

a. ***Decision Tree*** umumnya menunjukkan akurasi yang baik dalam mendeteksi serangan intrusi, terutama untukdataset yang tidak terlalu besar.Algoritma *Decision Tree* merupakan salah satu algoritma *Supervised Learning* yang sering digunakan dalam klasifikasi dan regresi(Yuliani, 2024).

Jurnal Minfo Polgan
Volume 13, Nomor 2, Desember 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i2.14356 p-ISSN : 2089-9424

b. ***Support Vector Machine*** merupakan algoritma pembelajaran mesin yang kuat dan serbaguna yang dapat digunakan untuk klasifikasi dan regresi.(Arum Sari & Pramono, 2024) SVM digunakan untuk membangun model yang dapat memisahkan data normal dari data yang mencurigakan atau berpotensi berbahaya. Dengan demikian, SVM dapat membantu dalam mendeteksi serangan dan mengklasifikasikan data dengan akurasi tinggi(Zy et al., 2023)
c. ***Naïve bayes Classifier*** merupakan teknik klasifikasi yang diusulkan oleh ilmuwan Inggris Thomas Bayes menggunakan Metode Probabilitas dan Statistik, yang memprediksi peluang masa depan berdasarkan pengalaman sebelumnya untuk apa yang disebut Teorema Bayes adalah dengan gabungan Naive, dengan asumsi bahwa kondisi antar atribut adalah independen. Klasifikasi Naive Bayes mengasumsikan bahwa ada tidaknya karakteristik tertentu dari satu kelas tidak ada hubungannya dengan karakteristik kelas lainnya(Silmina et al., 2022)
d. ***Random Forest*** merupakan metode bagging yang, ketika membangun pohon selama pelatihan, menghasilkan pohon dalam jumlah besar dari data sampel secara independen dari pohon sebelumnya dan membuat keputusan berdasarkan suara terbanyak(Tjahjadi & Santoso, 2023)

Deteksi Anomali

Deteksi anomali adalah proses mengidentifikasi perilaku yang tidak biasa atau mencurigakan dalam suatu sistem, Tujuannya adalah untuk mengidentifikasi kejadian yang tidak sesuai dengan pola normal atau yang mungkin menandakan adanya serangan atau pelanggaran keamanan(Kurniawan Informatika, 2023).

METODE PENELITIAN

Metode penelitian dalam artikel ini didasarkan pada tinjauan pustaka atau bisa disebutjuga dengan literature review yang komprehensif tentang peran *Artificial Intelligence* (AI) dalam peningkatan IT Governance. Metode tersebut akan diawali dengan pengumpulan literatur mengenai Peran *Artificial Intelligence* (AI) dalam deteksi dini ancaman keamanan jaringan yang relevan dari berbagai sumber, termasuk basis data jurnal dan sumber lainnya yang terkait. Literatur tersebut kemudian dipilih dengan hati-hati berdasarkan kriteria kualitas, kebaruan dan relevansi terhadap topik penelitian. Proses analisis literatur ini dilakukan secara cermat untuk mengidentifikasi temuan utama, metode penelitian yang digunakan serta kesimpulan yang dihasilkan oleh peneliti terdahulu. Pendapat-pendapat yang didapatkan dari temuan-temuan tersebut kemudian akan dijadikan kesimpulan yang relevan dengan topik penelitian, serta untuk memberikan saran terkait arah penelitian masa depan dalam bidang ini.

HASIL DAN PEMBAHASAN

Penelitian ini menegaskan bahwa teknologi AI, khususnya *Machine Learning*, memiliki potensi besar dalam meningkatkan keamanan jaringan dengan memanfaatkan kemampuan analitik canggih untuk mendeteksi dan merespons ancaman secara cepat. AI juga dapat membantu organisasi untuk mengelola risiko keamanan dengan lebih proaktif, mengurangi ketergantungan pada metode deteksi konvensional yang seringkali tidak efektif terhadap ancaman *modern* (Sinaga et al., 2024; Zulkarnain et al., 2024). Algoritma *Machine Learning* seperti *Naïve Bayes Classifier*, *Support Vector Machine (SVM), Decision Tree, dan Random Forest* efektif dalam menganalisis pola serangan dan mendeteksi anomali pada data jaringan besar (Zy et al., 2023; Silmina et al., 2022). AI membantu mengurangi waktu respons terhadap ancaman melalui proses analisis cepat dan otomatisasi tindakan mitigasi (Simanjuntak et al., 2024).

Algoritma yang berbeda memiliki keunggulan dan kelemahan spesifik tergantung pada jenis dataset dan skenario penggunaan. Misalnya, *Decision Tree* menunjukkan keakuratan tinggi dalam mendeteksi ancaman dengan dataset kecil hingga menengah (Yuliani, 2024), *Support Vector Machine (SVM)* menawarkan keandalan dalam memisahkan data normal dari aktivitas mencurigakan, memberikan akurasi tinggi untuk klasifikasi serangan (Arum Sari & Pramono, 2024), *Naïve Bayes Classifier* sangat cocok untuk memproses data yang memiliki hubungan antar atribut independen, meskipun akurasinya dipengaruhi oleh asumsi independensi tersebut (Silmina

et al., 2022), *Random Forest* menghasilkan prediksi yang lebih stabil melalui metode ensemble learning dengan membangun banyak pohon keputusan dari data sampel (Tjahjadi & Santoso, 2023). Dalam aplikasi praktis, kombinasi beberapa algoritma sering digunakan untuk meningkatkan akurasi dan keandalan deteksi.

Tantangan utama dalam penerapan AI untuk keamanan jaringan adalah tingginya tingkat *false positives*, yang dapat menyebabkan gangguan operasional (Wardhani, 2024). Deteksi anomali menjadi salah satu pendekatan utama dalam mengidentifikasi perilaku mencurigakan pada jaringan. Teknik ini terbukti efektif dalam mendeteksi pola yang tidak sesuai dengan aktivitas normal sistem (Kurniawan Informatika, 2023). Selain itu, kompleksitas implementasi teknologi AI membutuhkan infrastruktur jaringan dan sumber daya yang memadai (Bazrafshan (Akbar & Sutabri, 2024).

Untuk mengurangi tingkat *false positives*, penelitian lebih lanjut diperlukan untuk mengoptimalkan algoritma *Machine Learning* yang lebih sensitif terhadap anomali dan pola serangan. Penggunaan dataset yang representatif dan pelatihan model berbasis data *real-time* dapat membantu meningkatkan akurasi deteksi dan memperbaiki kelemahan model saat ini. Kolaborasi antara akademisi dan industri juga penting untuk memastikan bahwa solusi berbasis AI dapat diimplementasikan dalam lingkungan jaringan yang kompleks.

Penelitian lebih lanjut harus fokus pada pengembangan sistem AI yang tidak hanya mendeteksi ancaman tetapi juga memberikan rekomendasi tindakan mitigasi secara otomatis. Selain itu, diperlukan kajian tentang integrasi AI dengan teknologi keamanan lainnya, seperti *blockchain* dan *SDN (Software-Defined Networking),* untuk membangun ekosistem keamanan yang lebih adaptif.

KESIMPULAN

Hasil dari penelitian ini menunjukkan bahwa AI, khususnya melalui algoritma *Machine Learning*, dapat secara signifikan meningkatkan efektivitas deteksi dan mitigasi ancaman keamanan jaringan. Namun, penerapan teknologi ini memerlukan pendekatan yang hati-hati untuk mengatasi tantangan seperti *false positives* dan kebutuhan akan infrastruktur yang kuat. Kombinasi teknologi dan penelitian berkelanjutan akan menjadi kunci untuk menciptakan solusi keamanan yang lebih efektif di masa depan.

REFERENSI

Akbar, M. R., & Sutabri, T. (2024). IJM: Indonesian Journal of Multidisciplinary Implementasi Teknologi AI Dalam Deteksi dan Pencegahan Serangan Malware pada Jaringan Komputer Perusahaan. *Indonesian Journal of Multidisciplinary*, *2*(3), 20–30. https://journal.csspublishing/index.php/ijm

Arum Sari, A., & Pramono, P. (2024). *Prediksi Serangan Sql Injection Pada Jaringan Komputer Menggunakan Metode Support Vector Machine (SVM)*. 317–326. https://www.kaggle.com/datasets/syedsaqlainhussain/sql-injection-dataset

Hafsah, A., Irwan, M., Nasution, P., Ekonomi, F., Bisnis, D., Manajemen, P., Islam, U., & Sumatera, N. (2024). *Issn : 3025-9495*. *10*(9).

Khairunnisa, P. A., Annisa, N., & Parhusip, Y. J. (2024). *Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI : Studi Kasus di Indonesia*. *4*, 9–16.

Kurniawan Informatika, J. (2023). Implementasi Deep Learning Dalam Deteksi Anomali: Meningkatkan Keamanan Sistem Informasi. *Teknologipintar.Org*, *3*(12), 1–20.

Polgan, J. M., Sari, D. P., Halim, Z., Waseso, B., Gunadarma, U., Utomo, T. B., Buana, U. M., Forest, R., Forest, R., Intrusi, D., & Komputer, J. (2024). *Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer*. *13*(September), 1389–1394.

Silmina, E. P., Firdonsyah, A., & Amanda, R. A. A. (2022). Analisis Keamanan Jaringan Sistem

Informasi Sekolah Menggunakan Penetration Test Dan Issaf. *Transmisi*, *24*(3), 83–91. https://doi.org/10.14710/transmisi.24.3.83-91

Simanjuntak, E. N., Irmayani, D., & Nasution, F. A. (2024). Tinjauan Penerapan Kecerdasan Buatan Dalam Keamanan Jaringan Tantangan Dan Prospek Masa Depan. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *7*(2), 370–375.

Sinaga, N. H., Irmayani, D., & Hasibuan, M. N. S. (2024). Mengoptimalkan Keamanan Jaringan: Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI*, *7 Nomor 2*(September), 364–369. https://ejournal.sisfokomtek.org/index.php/jikom

Tan, T., Sama, H., Wijaya, G., & Aboagye, O. E. (2023). Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN). *Jurnal Teknologi Dan Informasi*, *13*(2), 152–164. https://doi.org/10.34010/jati.v13i2.10484

Tjahjadi, E. V., & Santoso, B. (2023). Klasifikasi Malware Menggunakan Teknik Machine Learning. *Jurnal Ilmiah Ilmu Komputer*, *2*(1), 60–70.

Wardhani, N. F. (2024). Penggunaan Machine Learning Dalam Deteksi Intrusi Pada Jaringan Komputer. *Duniadata.Org*, *1*(4), 1–16.

Yuliani, Y. (2024). *Perbandingan Algoritma Klasifikasi untuk Deteksi Intrusi pada Jaringan Komputer*.

Zulkarnain, Z., Jesselyn, J., Hansvirgo, H., Gunawan, F., & Dion, S. A. (2024). *Peran Artificial Intelligence (AI) dalam Peningkatan IT Governance : Kajian Literatur*. *2*(3).

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. *Media Online)*, *4*(1), 610–617. https://doi.org/10.30865/klik.v4i1.1134