Metode Hybrid Deep Learning untuk Deteksi Serangan Siber pada Jaringan Komputer

Ahmad Haidar[1)], Agus Suprianto[2)], Indra Oktavian[3)], Bayu Aji Saputra [4)],Norma Puspitasari[5)]

[1,2,3,4,5] Politeknik Indonusa Surakarta
[1]23.ahmad.haidar @poltekindonusa.ac.id, [2]23.agus.supriyanto@poltekindonusa.ac.id,
[3]23.indra.okktavian @poltekindonusa.ac.id, [4]23.bayu.aji@poltekindonusa.ac.id,
[5]normasari@poltekindonusa.ac.id

Abstrak

Ancaman siber yang berevolusi dengan teknik yang semakin kompleks menghadirkan tantangan signifikan bagi sistem deteksi intrusi (IDS) tradisional, terutama dalam mengidentifikasi serangan baru dan polanya yang berubah-ubah. Penelitian ini bertujuan untuk melakukan tinjauan komprehensif terhadap metode deteksi serangan siber menggunakan kecerdasan buatan (AI), termasuk machine learning dan deep learning. Analisis berfokus pada efektivitasnya dalam meningkatkan akurasi deteksi dan kecepatan respons terhadap serangan. Studi ini menyajikan metode dan implementasi sistem keamanan berbasis AI terbaru, serta menganalisis efektivitasnya pada berbagai skenario serangan. Hasil penelitian menunjukkan bahwa adopsi AI secara signifikan meningkatkan kemampuan deteksi serangan. Berdasarkan temuan ini, penelitian ini merumuskan rekomendasi teknis untuk pengembangan sistem deteksi serangan siber yang adaptif dan tangguh demi menghadapi ancaman di masa mendatang.
Kata kunci: Keamanan Siber,Kecerdasan Buatan,Deep Learning

Abstract

Evolving cyber threats with increasingly complex techniques present significant challenges for traditional intrusion detection systems (IDS), particularly in identifying new attacks and their changing patterns. This study aims to conduct a comprehensive review of cyberattack detection methods using artificial intelligence (AI), including machine learning and deep learning. The analysis focuses on their effectiveness in improving detection accuracy and response speed. The study presents the latest AI-based security system methods and implementations, and analyzes their effectiveness across various attack scenarios. The results show that the adoption of AI significantly improves attack detection capabilities. Based on these findings, this study formulates technical recommendations for the development of adaptive and resilient cyberattack detection systems to address future threats.
Keywords: Cybersecurity, Artificial Intelligence, Deep Learning

1. PENDAHULUAN

Dalam era transformasi digital yang pesat, ketergantungan pada sistem informasi dan jaringan komputer telah meningkat secara eksponensif. Bersamaan dengan itu, ancaman serangan siber juga terus berkembang, menargetkan individu, organisasi, dan infrastruktur kritis. Kerugian yang ditimbulkan tidak hanya terbatas pada finansial, tetapi juga mencakup kerusakan reputasi, kebocoran data sensitif, dan gangguan operasional yang meluas.(Ryandra, n.d.)

Sistem deteksi intrusi (IDS) tradisional yang mengandalkan metode berbasis tanda tangan (signature-based) memiliki keterbatasan signifikan. Metode ini tidak efektif dalam mendeteksi serangan baru (zero-day attacks) atau serangan yang menggunakan pola anomali yang belum pernah teridentifikasi sebelumnya. Keterbatasan ini mengharuskan adanya pendekatan yang lebih adaptif dan proaktif untuk melawan lanskap ancaman yang terus berubah.

Kecerdasan buatan (AI) menawarkan solusi potensial untuk mengatasi tantangan tersebut melalui kemampuannya dalam menganalisis data besar secara otomatis dan adaptif. Algoritma machine learning dan deep learning dapat dilatih untuk mengenali pola-pola anomali yang mengindikasikan aktivitas mencurigakan, bahkan tanpa adanya tanda tangan serangan yang spesifik.

Penelitian ini bertujuan untuk mengeksplorasi secara komprehensif perkembangan dan aplikasi teknologi AI dalam deteksi serangan siber. Fokus utama mencakup tinjauan terhadap berbagai algoritma machine learning dan deep learning yang relevan, serta analisis tantangan operasional dalam implementasinya. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan ketahanan sistem keamanan siber di berbagai sektor.(Studi et al., 2025)

2. TINJAUAN PUSTAKA

Perbaikan dan Penyempurnaan Tinjauan Pustaka

Tinjauan pustaka yang diberikan sudah memuat poin-poin penting, namun perlu disempurnakan agar lebih terstruktur, komprehensif, dan memenuhi standar penulisan jurnal ilmiah nasional. Poin-poin di bawah ini disusun ulang dan diperluas untuk membentuk kerangka tinjauan pustaka yang ideal.(Mahdi et al., 2025)

Konsep Dasar dan Klasifikasi Sistem Deteksi Intrusi (IDS)

Sistem Deteksi Intrusi (IDS) merupakan komponen krusial dalam arsitektur keamanan siber, berfungsi untuk memantau lalu lintas jaringan atau aktivitas sistem guna mengidentifikasi potensi ancaman dan aktivitas mencurigakan. Secara umum, IDS modern diklasifikasikan menjadi tiga kategori utama:

IDS Berbasis Tanda Tangan (Signature-Based IDS): Metode ini bekerja dengan membandingkan lalu lintas jaringan dengan database tanda tangan serangan yang telah diketahui. Keunggulannya adalah akurasi tinggi dalam mendeteksi serangan yang sudah teridentifikasi, namun memiliki kelemahan signifikan dalam mengenali serangan baru (zero-day attacks) atau varian serangan yang belum terdaftar.

IDS Berbasis Anomali (Anomaly-Based IDS): Pendekatan ini membangun profil perilaku jaringan atau sistem yang normal, lalu menandai setiap deviasi dari profil tersebut sebagai potensi serangan. Keunggulannya adalah kemampuannya yang adaptif untuk mendeteksi serangan baru, namun sering kali menghasilkan tingkat positif palsu (false positive) yang tinggi.

IDS Hibrida (Hybrid IDS): Model ini menggabungkan kekuatan dari kedua pendekatan sebelumnya, menggunakan basis tanda tangan untuk serangan yang diketahui dan basis anomali untuk mendeteksi pola yang tidak biasa. Pendekatan hibrida secara luas dianggap sebagai solusi optimal karena mampu meningkatkan akurasi deteksi sambil meminimalkan tingkat positif palsu.

Peran dan Penerapan Kecerdasan Buatan (AI) dalam Deteksi Intrusi

Seiring dengan kompleksitas serangan siber, penerapan teknologi kecerdasan buatan (AI) telah menjadi fondasi dalam pengembangan IDS generasi terbaru. AI, khususnya machine learning dan deep learning, memungkinkan sistem untuk secara otomatis menganalisis volume data besar dan mengidentifikasi pola-pola serangan yang kompleks.

Machine Learning (ML): Algoritma ML seperti Random Forest, Support Vector Machine (SVM), dan K-Nearest Neighbors (KNN) sering digunakan untuk mengklasifikasikan lalu lintas jaringan sebagai normal atau anomali. Metode ini membutuhkan ekstraksi fitur secara manual dari data mentah sebelum proses pelatihan model.

Deep Learning (DL): Model DL seperti Convolutional Neural Networks (CNN) dan Long Short-Term Memory (LSTM) menawarkan keunggulan dalam ekstraksi fitur otomatis. Jaringan DL dapat memproses data jaringan mentah secara langsung, sehingga menyederhanakan pra-pemrosesan data yang rumit dan meningkatkan akurasi deteksi. Pendekatan ini sangat efektif dalam mendeteksi serangan yang tersembunyi dalam pola lalu lintas data yang kompleks.(Studi et al., 2025)

Dataset Standar dan Evaluasi Kinerja

Untuk mengevaluasi efektivitas algoritma deteksi serangan siber, komunitas riset menggunakan beberapa dataset standar sebagai tolok ukur (benchmark). Dataset ini merepresentasikan kondisi jaringan yang disimulasikan atau data nyata dengan beragam jenis serangan:

NSL-KDD: Merupakan versi perbaikan dari dataset KDD Cup 1999 yang telah disesuaikan untuk mengurangi data duplikat dan bias.

UNSW-NB15: Dataset yang lebih modern, dibuat dengan lingkungan lab yang mensimulasikan aktivitas normal dan serangan siber secara real-time.

CICIDS2017:Dikenal [1]karena merepresentasikan lalu lintas jaringan yang lebih realistis dan mencakup serangan yang beragam.

CICIoT2023: Dataset terbaru yang secara spesifik berfokus pada lalu lintas jaringan dalam lingkungan Internet of Things (IoT), merefleksikan ancaman yang terus berkembang pada perangkat IoT.

Tantangan dan Keterbatasan dalam Implementasi
Meskipun potensi AI dalam deteksi intrusi sangat menjanjikan, terdapat beberapa tantangan dan keterbatasan yang perlu diperhatikan dalam implementasinya:

Tingkat Positif Palsu (False Positive Rate): Salah satu kendala utama adalah tingginya tingkat alarm palsu yang dapat mengganggu operasional sistem dan menyebabkan kelelahan peringatan (alert fatigue) pada analis keamanan.

Kebutuhan Komputasi Tinggi: Model deep learning yang kompleks memerlukan sumber daya komputasi yang besar, baik untuk pelatihan maupun inferensi, yang dapat menjadi hambatan dalam penerapan real-time.

Keamanan AI: Model AI itu sendiri dapat menjadi target serangan, seperti adversarial attacks di mana penyerang memanipulasi data input untuk menipu model agar membuat prediksi yang salah.

Respons Waktu Nyata (Real-Time Response): Mengingat volume data jaringan yang sangat besar, tantangan untuk mencapai deteksi dan respons yang cepat dan real-time masih menjadi fokus penelitian.(Jyothi et al., 2024)

3. METODE PENELITIAN

1. Studi Literatur dan Perumusan Kerangka Konseptual
Tahap awal penelitian melibatkan studi literatur mendalam terkait perkembangan terbaru dalam bidang keamanan siber dan aplikasi AI. Fokus utama adalah pada analisis tren dan tinjauan sistematis terhadap berbagai algoritma machine learning dan deep learning yang digunakan untuk deteksi intrusi. Hasil dari studi ini digunakan untuk merumuskan kerangka kerja konseptual penelitian dan memilih metode eksperimental yang paling relevan.

2. Persiapan Dataset
Penelitian ini menggunakan dua dataset standar yang umum dipakai dalam riset keamanan siber: NSL-KDD dan UNSW-NB15. Tahapan persiapan dataset meliputi:

a. Pengumpulan Data: Mengunduh dataset dari repositori resmi.
b. Preprocessing Data: Melakukan serangkaian proses untuk memastikan kualitas data, termasuk:
c. Pembersihan Data: Menangani nilai yang hilang dan data yang tidak konsisten.
d. Seleksi Fitur: Memilih fitur-fitur yang paling relevan dan signifikan untuk meningkatkan efisiensi dan akurasi model.
e. Normalisasi Data: Menskalakan fitur numerik ke dalam rentang yang seragam untuk menghindari bias pada model.

(Ryandra, n.d.)

3. Implementasi dan Pelatihan Model
Pada tahap ini, dilakukan implementasi algoritma AI untuk membangun model deteksi intrusi. Lingkungan pengembangan yang digunakan adalah Python dengan library utama scikit-learn untuk machine learning dan TensorFlow/Keras untuk deep learning. Model yang diimplementasikan mencakup:

a. Machine Learning: Random Forest dan Support Vector Machine (SVM).
b. Deep Learning: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), dan model hibrida CNN-LSTM untuk mengeksploitasi kemampuan ekstraksi fitur spasial dan temporal secara bersamaan.

Pelatihan model dilakukan menggunakan teknik k-fold cross-validation untuk

memastikan validitas dan generalisasi model yang optimal.
(Fitria & Mutijarsa, 2023)
4. Evaluasi Kinerja Model
Kinerja setiap model dievaluasi secara ketat menggunakan metrik-metrik standar dalam klasifikasi:

a. Akurasi (Accuracy): Mengukur proporsi total prediksi yang benar.
b. Presisi (Precision): Mengukur proporsi prediksi positif yang benar.
c. Recall: Mengukur proporsi kasus positif aktual yang berhasil dideteksi.
d. F1-Score: Nilai harmonik rata-rata dari presisi dan recall.
e. Tingkat Positif Palsu (False Positive Rate): Mengukur proporsi kasus negatif yang salah diklasifikasikan sebagai positif.

5. Simulasi dan Analisis Komparatif
Sebagai bagian dari pengujian praktis, model-model yang telah dilatih disimulasikan pada skenario serangan yang beragam, termasuk multiple attack vectors, untuk mengevaluasi kemampuan deteksinya dalam konteks yang mendekati kondisi nyata. Hasil dari simulasi ini kemudian dianalisis secara komparatif dengan metode deteksi tradisional untuk menyoroti keunggulan pendekatan berbasis AI dalam hal akurasi, kecepatan, dan kemampuan adaptasi terhadap ancaman baru.(Fitria & Mutijarsa, 2023)

4. HASIL DAN PEMBAHASAN

Performa Model Deteksi Berbasis AI
Evaluasi model deteksi intrusi menunjukkan variasi performa yang signifikan di antara algoritma yang diuji. Secara umum, model deep learning menunjukkan kinerja superior dibandingkan model machine learning tradisional. Secara spesifik, model hybrid CNN-LSTM mencapai akurasi tertinggi, berkisar antara 97% hingga 99%. Keunggulan ini disebabkan oleh kemampuan model hibrida untuk mengekstraksi fitur spasial dan temporal dari data lalu lintas jaringan secara simultan, sehingga memungkinkan deteksi pola serangan yang sangat kompleks dan sulit dikenali oleh metode lain. Selain itu, model ini juga berhasil mempertahankan tingkat positif palsu (false positive rate) yang jauh lebih rendah, sebuah metrik kritis yang menunjukkan efisiensi dan keandalan model dalam lingkungan operasional.
Model machine learning seperti Random Forest dan Support Vector Machine (SVM) juga menunjukkan performa yang solid, terutama pada dataset dengan volume data yang lebih kecil dan tingkat kebisingan (noise) yang rendah. Kedua model ini memberikan akurasi yang memuaskan dan dapat menjadi pilihan efektif untuk implementasi dengan keterbatasan sumber daya komputasi.

Studi Kasus: Deteksi Phishing Menggunakan AI
Studi kasus implementasi AI pada deteksi phishing menggarisbawahi efektivitas pendekatan ini dalam skenario spesifik. Sistem yang menggunakan kombinasi algoritma SVM dan Neural Networks berhasil mencapai akurasi deteksi hingga 97% dalam mengidentifikasi email dan URL phishing. Keberhasilan ini tidak hanya bergantung pada kekuatan algoritma, tetapi juga pada pra-pemrosesan data yang komprehensif, yang mencakup pembersihan dan ekstraksi fitur relevan dari konten email dan URL. Hal ini menunjukkan bahwa kualitas data pelatihan memegang peranan krusial dalam keberhasilan implementasi AI, tidak hanya pada model itu sendiri.

Implikasi Terhadap Kecepatan dan Efisiensi Respons
Temuan dari penelitian ini memperkuat argumen bahwa integrasi AI secara signifikan dapat meningkatkan kecepatan dan efisiensi respons terhadap insiden siber. Ketika model deteksi AI digabungkan dengan sistem respons otomatis, waktu antara deteksi dan mitigasi serangan dapat dipercepat secara drastis, sehingga meminimalkan downtime dan kerugian data. Konsep reinforcement learning menjadi kunci dalam adaptasi berkelanjutan, memungkinkan sistem untuk terus belajar dari serangan baru dan menyesuaikan strategi pertahanan tanpa intervensi manusia secara manual.(Barlyan Kurdianto et al., 2025)

Tantangan dan Batasan Implementasi
Meskipun menunjukkan kemajuan signifikan, implementasi AI dalam keamanan siber masih menghadapi beberapa tantangan. Kebutuhan akan perangkat keras (hardware) dengan spesifikasi tinggi, terutama untuk melatih dan menjalankan model deep learning yang kompleks, menjadi salah satu kendala utama. Selain itu, keamanan model AI itu sendiri dari

serangan adversarial menjadi isu yang mendesak, di mana penyerang dapat memanipulasi input untuk menipu model agar membuat prediksi yang salah. Solusi untuk tantangan-tantangan ini terus menjadi fokus

5. PENUTUP

Penelitian ini menyimpulkan bahwa sistem deteksi serangan siber berbasis kecerdasan buatan (AI) menawarkan solusi yang jauh lebih efektif dan adaptif dibandingkan sistem tradisional. Temuan kunci menunjukkan bahwa pengembangan model hibrida yang menggabungkan pendekatan machine learning dan deep learning, didukung oleh penggunaan dataset yang komprehensif, terbukti signifikan dalam meningkatkan akurasi deteksi dan mereduksi tingkat positif palsu (false positive).

Implementasi sistem ini di lapangan memerlukan pertimbangan matang terhadap aspek komputasi dan keamanan model AI itu sendiri. Oleh karena itu, penelitian mendatang disarankan untuk memfokuskan diri pada pengembangan metode deteksi real-time yang lebih efisien, menciptakan sistem yang mampu beradaptasi secara otomatis terhadap serangan baru, serta mengkaji secara mendalam isu keamanan dan privasi data dalam sistem AI. Dengan kemajuan yang terus berlanjut di bidang ini, diharapkan perusahaan dan institusi dapat memperkuat ketahanan siber mereka dalam menghadapi lanskap ancaman yang terus berevolusi.

6. REFERENSI

Barlyan Kurdianto, Yohanzah Febriyanto, & Yustian Servanda. (2025). Intrusion Detection System Analysis to Improve Computer Network Security. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, *4*(3), 1855–1862. https://doi.org/10.59934/jaiea.v4i3.1036

Fitria, E. Y., & Mutijarsa, K. (2023). Survei Penelitian Metode Kecerdasan Buatan untuk Mendeteksi Ancaman Teknologi Serangan Siber. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(6), 1185–1196. https://doi.org/10.25126/jtiik.2023107341

Jyothi, K. K., Borra, S. R., Srilakshmi, K., Balachandran, P. K., Reddy, G. P., Colak, I., Dhanamjayulu, C., Chinthaginjala, R., & Khan, B. (2024). A novel optimized neural network model for cyber attack detection using enhanced whale optimization algorithm. *Scientific Reports*, *14*(1), 1–11. https://doi.org/10.1038/s41598-024-55098-2

Mahdi, Z. S., Zaki, R. M., & Alzubaidi, L. (2025). Advanced Hybrid Techniques for Cyberattack Detection and Defense in IoT Networks . *Security and Privacy*, *8*(2). https://doi.org/10.1002/spy2.471

Ryandra, M. F. . (n.d.). *Deteksi+Dan+Pencegahan+Serangan+Cyber+Menggunakan+Sistem+Deteksi+Intrusi+Berbasis+Ai*. 1–12.

Studi, P., Informasi, S., Sains, F., Triputra, U. P., Theologi, F., Kristen, U., & Solo, T. (2025). *Komputasi Kuantum*. *3*(2), 74–88.