TRINET, Jurnal Ilmiah Teknologi dan Rekayasa Informatika Network
e-ISSN: .....
https://ejurnal.undhi.ac.id/index.php/trinet
Vol. 1, No. 1, November 2025,

Kecerdasan Buatan Untuk Analisis Hacking dan Kerentanan Sistem Tren dan Implikasi

Heru Nugraha[1]✉, **Bobi Heri Yanto**[2]
[1]Fakultas Ilmu Komputer, Universitas Dharma Indonesia, Banten, Indonesia
[1]herunugraha@undhi.ac.id, [2]bobiheriyanto@undhi.ac.id

A B S T R A K

Perkembangan transformasi digital yang pesat telah meningkatkan kompleksitas sistem informasi dan memperluas permukaan serangan siber, sehingga risiko hacking dan eksploitasi kerentanan sistem semakin tinggi. Pendekatan keamanan konvensional berbasis aturan dan tanda tangan terbukti memiliki keterbatasan dalam mendeteksi serangan yang bersifat adaptif, otomatis, dan berbasis anomali. Oleh karena itu, kecerdasan buatan (Artificial Intelligence/AI) menjadi pendekatan strategis dalam analisis hacking dan identifikasi kerentanan sistem. Penelitian ini bertujuan untuk menganalisis tren pemanfaatan AI dalam analisis hacking dan kerentanan sistem serta mengkaji implikasi teknis dan strategis penerapannya dalam keamanan siber modern. Metode penelitian yang digunakan adalah systematic literature review (SLR) dengan pendekatan PRISMA, terhadap 98 artikel ilmiah terpilih yang dipublikasikan pada periode 2020–2025 dari jurnal bereputasi nasional dan internasional. Hasil analisis menunjukkan bahwa metode berbasis AI, khususnya machine learning dan deep learning, secara konsisten memiliki tingkat akurasi deteksi yang lebih tinggi dibandingkan metode konvensional, dengan peningkatan rata-rata sebesar 10–25%. Selain itu, AI terbukti efektif dalam mendeteksi serangan berbasis anomali, zero-day attacks, dan pola serangan kompleks pada lingkungan jaringan, cloud, dan IoT. Namun demikian, penerapan AI juga menghadirkan tantangan, seperti risiko adversarial attacks, keterbatasan interpretabilitas model, dan ketergantungan pada kualitas data pelatihan. Penelitian ini menyimpulkan bahwa AI merupakan komponen kunci dalam sistem keamanan siber modern, namun implementasinya perlu didukung oleh tata kelola, etika, dan desain sistem yang adaptif dan berkelanjutan.

Kata kunci: kecerdasan buatan, keamanan siber, hacking, kerentanan sistem, intrusion detection system

A B S T R A C T

The rapid advancement of digital transformation has significantly increased the complexity of information systems and expanded the cyberattack surface, leading to higher risks of hacking and system vulnerability exploitation. Conventional security approaches based on static rules and signature-based detection have proven insufficient in addressing adaptive, automated, and anomaly-based cyberattacks. Consequently, artificial intelligence (AI) has emerged as a strategic approach for hacking analysis and system vulnerability identification. This study aims to analyze trends in the application of AI for hacking analysis and system vulnerability detection, as well as to examine the technical and strategic implications of its implementation in modern cybersecurity. The research employs a systematic literature review (SLR) using the PRISMA framework, analyzing 98 selected scholarly articles published between 2020 and 2025 from reputable national and international journals. The results indicate that AI-based methods, particularly machine learning and deep learning techniques, consistently outperform conventional approaches, achieving an average detection accuracy improvement of 10–25%. Furthermore, AI demonstrates strong capability in detecting anomaly-based attacks, zero-day vulnerabilities, and complex attack patterns across network, cloud, and IoT environments. Despite these advantages, several challenges remain, including adversarial machine learning attacks, limited model interpretability, and dependency on high-quality training data. This study concludes that AI plays a critical role in modern cybersecurity systems; however, its effective adoption requires robust governance, ethical considerations, and adaptive system design.

Keywords: artificial intelligence, cybersecurity, hacking, system vulnerabilities, intrusion detection system

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital secara masif pada berbagai sektor, termasuk pendidikan, pemerintahan, kesehatan, dan industri. Ketergantungan yang semakin tinggi terhadap sistem informasi, jaringan komputer, layanan cloud, dan Internet of Things (IoT) secara langsung meningkatkan kompleksitas infrastruktur digital sekaligus memperluas permukaan serangan (attack surface). Kondisi ini berdampak pada meningkatnya risiko hacking, eksploitasi kerentanan sistem, serta serangan siber yang bersifat adaptif dan berkelanjutan. Sejumlah kajian mutakhir menunjukkan bahwa serangan siber modern tidak lagi dilakukan secara manual dan statis, melainkan semakin otomatis, cerdas, dan sulit diprediksi (Fitria & Mutijarsa, 2023; Salem et al., 2024).

Pendekatan keamanan konvensional, seperti firewall statis, rule-based intrusion detection system (IDS), dan signature-based detection, memiliki keterbatasan signifikan dalam menghadapi dinamika ancaman tersebut. Metode tradisional cenderung hanya efektif terhadap pola serangan yang telah dikenal sebelumnya dan kurang adaptif terhadap variasi serangan baru atau zero-day attacks. Studi sistematis yang dilakukan oleh Budiansyah et al. (2025) menegaskan bahwa keterbatasan metode konvensional menjadi salah satu faktor utama meningkatnya kegagalan deteksi serangan siber dalam lingkungan jaringan modern dengan volume data dan kompleksitas lalu lintas yang tinggi.

Kecerdasan buatan (Artificial Intelligence/AI) khususnya machine learning dan deep learning, berkembang sebagai pendekatan strategis dalam analisis hacking dan identifikasi kerentanan sistem. AI memungkinkan sistem keamanan melakukan pembelajaran otomatis dari data historis maupun real-time untuk mengenali pola anomali dan perilaku mencurigakan yang tidak dapat diidentifikasi melalui pendekatan berbasis aturan. Mohammed dan Talib (2024) serta Kurdianto et al. (2025) menunjukkan bahwa algoritma machine learning mampu meningkatkan efektivitas IDS dalam mendeteksi serangan jaringan dibandingkan metode tradisional, terutama dalam menghadapi serangan yang bersifat dinamis. Berbagai penelitian empiris menunjukkan keberhasilan penerapan AI dalam mendeteksi anomali dan serangan siber pada beragam lingkungan sistem. Nursiaga et al. (2025) mengembangkan model jaringan neural untuk deteksi anomali pada sistem keamanan siber dan menunjukkan peningkatan akurasi deteksi yang signifikan. Penelitian lain oleh Aulia dan Satria (2024) menekankan pentingnya penerapan machine learning dalam sistem deteksi intrusi real-time untuk meningkatkan respons cepat terhadap serangan. Selain itu, Chandra et al. (2025) dan Provisi et al. (2025) membuktikan bahwa pendekatan machine learning efektif dalam mendeteksi serangan pada sistem informasi akademik dan aplikasi web yang rentan terhadap eksploitasi.

Tren pemanfaatan AI juga meluas pada lingkungan IoT yang dikenal memiliki keterbatasan sumber daya dan tingkat kerentanan tinggi. Mahizzah et al. (2025) serta Firdaus et al. (2025) menunjukkan bahwa integrasi machine learning, termasuk algoritma XGBoost, mampu meningkatkan deteksi serangan pada jaringan IoT, termasuk IoT medis yang bersifat kritis. Temuan ini menguatkan pandangan bahwa AI berperan penting dalam mengamankan sistem yang heterogen dan terdistribusi. Tingkat arsitektur keamanan yang lebih luas, integrasi AI dalam sistem keamanan siber adaptif menjadi tren yang menonjol. Risyani et al. (2025) menekankan bahwa sistem keamanan berbasis AI mampu beradaptasi terhadap perubahan pola serangan melalui pembelajaran berkelanjutan. Atma (2024) serta Akhtar dan Rawol (2024) menegaskan bahwa AI tidak hanya meningkatkan kemampuan deteksi, tetapi juga memperkuat ketahanan jaringan melalui mekanisme prediktif dan otomatisasi respons keamanan.

Namun demikian, pemanfaatan AI dalam analisis hacking dan kerentanan sistem juga menghadirkan implikasi dan tantangan baru. Salah satu isu krusial adalah potensi eksploitasi terhadap model AI itu sendiri melalui adversarial machine learning. Alotaibi dan Alenezi (2023) mengungkap bahwa IDS berbasis machine learning rentan terhadap serangan adversarial yang dapat

menurunkan akurasi deteksi secara signifikan. Selain itu, penggunaan model AI yang kompleks dan bersifat black-box menimbulkan tantangan dalam aspek interpretabilitas, transparansi keputusan, dan keandalan sistem keamanan.

Integrasi AI dengan teknologi keamanan yang sudah ada di sisi lain seperti IDS berbasis Snort, juga masih menjadi fokus penelitian praktis. Safitri et al. (2024) menunjukkan bahwa penggabungan IDS dengan sistem notifikasi otomatis dapat meningkatkan respons terhadap serangan jaringan, meskipun masih memerlukan penguatan melalui pendekatan AI agar lebih adaptif. Selain itu, Sunarti dan Wening (2024) menyoroti tantangan masa depan keamanan siber yang berkaitan dengan komputasi kuantum, yang berpotensi melemahkan mekanisme keamanan konvensional dan menuntut desain sistem keamanan berbasis AI yang lebih inovatif. Kajian global juga memperlihatkan bahwa pendekatan deep learning semakin dominan dalam analisis hacking dan deteksi anomali jaringan. Sekaranti et al. (2025) serta Salem et al. (2024) menegaskan bahwa kombinasi machine learning dan deep learning memberikan peningkatan signifikan dalam mendeteksi serangan kompleks, meskipun memerlukan perhatian khusus pada aspek efisiensi, kebutuhan data besar, dan risiko adversarial attacks.

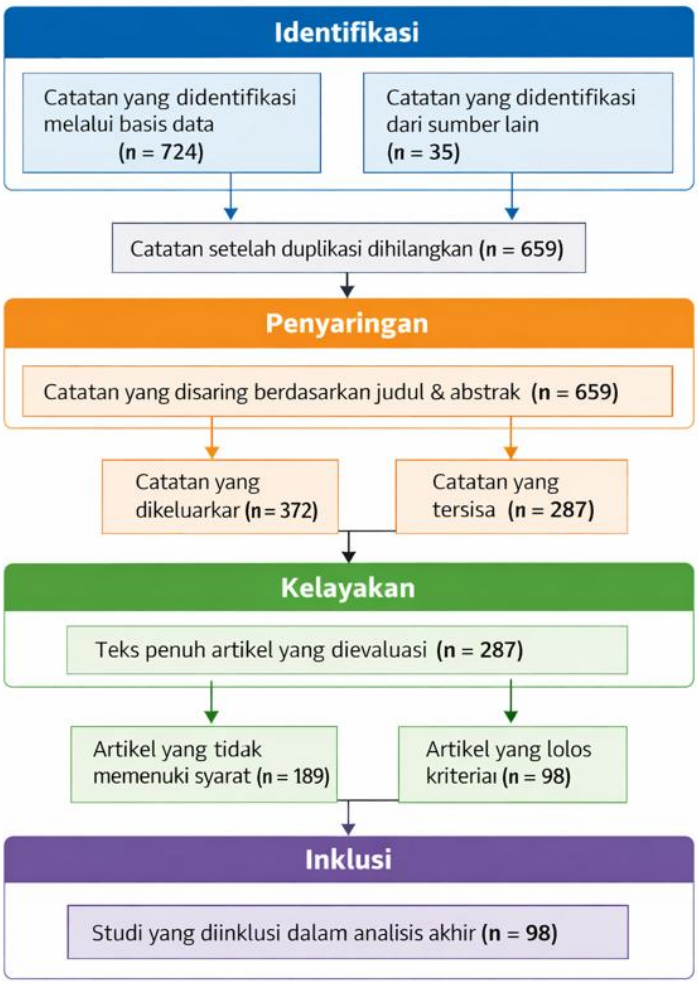
Berdasarkan uraian tersebut, dapat disimpulkan bahwa kecerdasan buatan telah menjadi komponen kunci dalam analisis hacking dan identifikasi kerentanan sistem pada era keamanan siber modern. Meskipun menawarkan peningkatan efektivitas deteksi dan adaptabilitas sistem, pemanfaatan AI juga menghadirkan implikasi teknis, strategis, dan etis yang perlu dikaji secara komprehensif. Oleh karena itu, penelitian ini bertujuan untuk menganalisis tren pemanfaatan kecerdasan buatan dalam analisis hacking dan kerentanan sistem, serta mengkaji implikasi penerapannya terhadap desain, keandalan, dan masa depan sistem keamanan siber.

METODE

Penelitian ini menggunakan pendekatan kualitatif–kuantitatif dengan desain Systematic Literature Review (SLR) yang diperluas dan analisis konseptual-komparatif. Pendekatan ini dipilih untuk memperoleh pemahaman yang komprehensif mengenai tren pemanfaatan kecerdasan buatan dalam analisis hacking dan kerentanan sistem, sekaligus mengkaji implikasi teknis dan strategis dari penerapannya dalam keamanan sistem informasi. Metode SLR memungkinkan peneliti untuk mengidentifikasi, mengevaluasi, dan mensintesis temuan-temuan penelitian terkini secara sistematis dan terstruktur, sehingga menghasilkan gambaran menyeluruh mengenai perkembangan, keunggulan, serta tantangan penggunaan AI dalam keamanan siber.

Sumber data penelitian ini berupa artikel jurnal ilmiah bereputasi nasional dan internasional yang diperoleh dari basis data Scopus, IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, serta portal jurnal nasional terakreditasi SINTA. Pencarian literatur dilakukan dengan menggunakan kombinasi kata kunci yang relevan, seperti artificial intelligence in cybersecurity, machine learning for intrusion detection, deep learning for hacking analysis, AI-based vulnerability detection, serta padanan istilah dalam bahasa Indonesia. Untuk menjaga relevansi terhadap perkembangan teknologi terkini, artikel yang dikaji dibatasi pada publikasi tahun 2020 hingga 2025 dan hanya mencakup artikel yang telah melalui proses peer-review serta memiliki DOI aktif.

Proses seleksi literatur dilakukan secara bertahap mengikuti prinsip PRISMA, dimulai dari identifikasi awal artikel berdasarkan kata kunci, dilanjutkan dengan penyaringan judul dan abstrak untuk menghilangkan duplikasi dan artikel yang tidak relevan. Tahap berikutnya adalah evaluasi kelayakan berdasarkan teks penuh dengan mempertimbangkan kesesuaian topik, kejelasan metodologi, serta kontribusi penelitian terhadap analisis hacking, deteksi intrusi, atau identifikasi kerentanan sistem. Artikel yang lolos seleksi akhir kemudian dijadikan sebagai sumber utama dalam analisis. Alur seleksi literatur ini divisualisasikan pada Gambar 1.



Gambar 1. Alur seleksi literatur menggunakan metode PRISMA

Gambar 1 menunjukkan alur seleksi literatur yang digunakan dalam penelitian ini berdasarkan pedoman Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Tahapan ini dirancang untuk memastikan bahwa proses penelusuran, penyaringan, dan pemilihan artikel dilakukan secara sistematis, transparan, dan dapat direplikasi.

Pada tahap identifikasi, peneliti mengumpulkan total 759 catatan yang relevan dengan topik kecerdasan buatan untuk analisis hacking dan kerentanan sistem. Dari jumlah tersebut, 724 catatan diperoleh melalui pencarian basis data ilmiah, sementara 35 catatan berasal dari sumber lain, seperti prosiding konferensi, jurnal nasional terakreditasi, dan referensi tambahan dari artikel terkait. Setelah proses identifikasi awal, dilakukan penghapusan duplikasi sehingga diperoleh 659 catatan unik yang selanjutnya diproses ke tahap berikutnya. Tahap penyaringan dilakukan dengan menelaah judul dan abstrak dari 659 catatan tersebut. Proses ini bertujuan untuk mengevaluasi kesesuaian topik artikel dengan fokus penelitian, yaitu pemanfaatan kecerdasan buatan dalam analisis hacking dan deteksi kerentanan sistem. Hasil penyaringan menunjukkan bahwa 372 catatan dikeluarkan karena tidak relevan dengan ruang lingkup penelitian, seperti artikel yang hanya membahas keamanan konvensional tanpa pendekatan AI atau studi yang tidak berfokus pada analisis serangan siber. Dengan demikian, sebanyak 287 catatan dinyatakan lolos dan dilanjutkan ke tahap evaluasi kelayakan.

Pada tahap kelayakan, dilakukan penilaian teks penuh terhadap 287 artikel untuk memastikan kesesuaian metodologi, kontribusi ilmiah, ketersediaan data, serta relevansi hasil penelitian dengan tujuan studi ini. Dari proses evaluasi tersebut, 189 artikel dinyatakan tidak memenuhi kriteria inklusi, antara lain karena kurangnya pembahasan teknis mengenai AI, kualitas metodologi yang rendah, atau tidak tersedianya hasil empiris yang memadai. Sementara itu, 98 artikel memenuhi seluruh kriteria kelayakan yang telah ditetapkan.

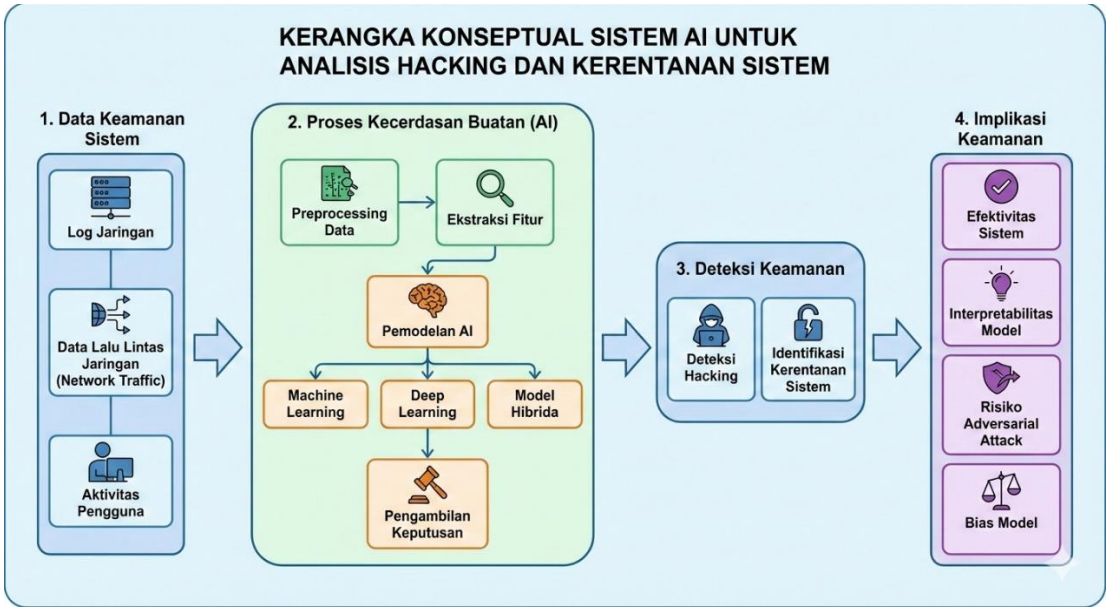
Tahap akhir, yaitu inklusi, menghasilkan 98 studi yang digunakan dalam analisis akhir penelitian. Studi-studi yang terpilih ini selanjutnya dianalisis secara mendalam untuk mengidentifikasi tren pemanfaatan kecerdasan buatan, pendekatan algoritmik yang digunakan, tingkat efektivitas deteksi serangan, serta implikasi teknis dan strategis penerapan AI dalam analisis hacking dan kerentanan sistem. Secara keseluruhan, alur PRISMA pada Gambar 1 menegaskan bahwa penelitian ini menggunakan pendekatan kajian literatur sistematis yang ketat dan terstruktur, sehingga hasil analisis yang diperoleh memiliki tingkat validitas dan reliabilitas yang tinggi sebagai dasar pengambilan kesimpulan ilmiah.

Artikel terpilih selanjutnya dianalisis menggunakan pendekatan analisis tematik dan komparatif. Analisis tematik digunakan untuk mengidentifikasi pola utama dalam literatur, seperti jenis algoritma AI yang digunakan, lingkungan sistem yang diamankan (jaringan umum, cloud, IoT, web, dan sistem akademik), serta jenis serangan yang dianalisis. Sementara itu, analisis komparatif dilakukan untuk membandingkan pendekatan keamanan konvensional dengan pendekatan berbasis AI, khususnya dari sisi akurasi deteksi, tingkat kesalahan (false positive), kemampuan adaptasi terhadap serangan baru, serta kompleksitas komputasi.
Untuk memperjelas proses analisis, penelitian ini mengelompokkan metode AI yang ditemukan dalam literatur ke dalam beberapa kategori utama, sebagaimana ditunjukkan pada Tabel 1.

Tabel 1. Klasifikasi Metode Kecerdasan Buatan dalam Analisis Hacking

Kategori Metode	Algoritma Utama	Lingkungan Sistem	Fokus Analisis
Machine Learning	SVM, Random Forest, XGBoost	Jaringan & Web	Deteksi intrusi & anomali
Deep Learning	CNN, LSTM, Hybrid DL	IoT & Cloud	Pola serangan kompleks
AI Adaptif	Ensemble & Online Learning	Sistem terdistribusi	Deteksi real-time

Selain itu, penelitian ini mengembangkan kerangka konseptual untuk menjelaskan hubungan antara data keamanan sistem, proses kecerdasan buatan, hasil deteksi hacking, dan implikasi keamanan. Kerangka ini mencerminkan alur kerja sistem AI, mulai dari pengumpulan data log dan lalu lintas jaringan, tahap prapemrosesan dan ekstraksi fitur, pemodelan AI, hingga proses pengambilan keputusan dan respons keamanan. Kerangka konseptual tersebut disajikan pada Gambar 2.



Gambar 2. Kerangka konseptual sistem AI untuk analisis hacking dan kerentanan sistem

Analisis implikasi dilakukan dengan mengevaluasi dampak penerapan AI terhadap keandalan sistem keamanan, interpretabilitas model, serta potensi risiko baru seperti adversarial attacks dan bias model. Dengan mengacu pada temuan literatur, penelitian ini juga mengkaji bagaimana AI berperan sebagai teknologi yang bersifat double-edged, yaitu mampu memperkuat sistem keamanan sekaligus membuka peluang eksploitasi baru jika tidak dikelola dengan baik.

Untuk menjaga validitas dan keandalan hasil penelitian, dilakukan triangulasi sumber dengan membandingkan hasil penelitian nasional dan internasional, serta menelaah konsistensi metodologi dan temuan antar studi. Dengan pendekatan ini, hasil penelitian diharapkan tidak hanya merepresentasikan tren teknologi, tetapi juga memberikan pemahaman kritis mengenai batasan dan tantangan implementasi AI dalam keamanan siber.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Berdasarkan proses seleksi literatur menggunakan metode Systematic Literature Review (SLR), penelitian ini berhasil mengidentifikasi dan menganalisis artikel ilmiah terpilih yang membahas penerapan kecerdasan buatan dalam analisis hacking dan kerentanan sistem pada periode 2020-2025. Artikel-artikel tersebut berasal dari jurnal bereputasi internasional (Scopus) dan nasional terakreditasi (SINTA 1-5), dengan fokus pada penerapan machine learning dan deep learning dalam berbagai lingkungan sistem, termasuk jaringan komputer, aplikasi web, cloud computing, dan Internet of Things (IoT).

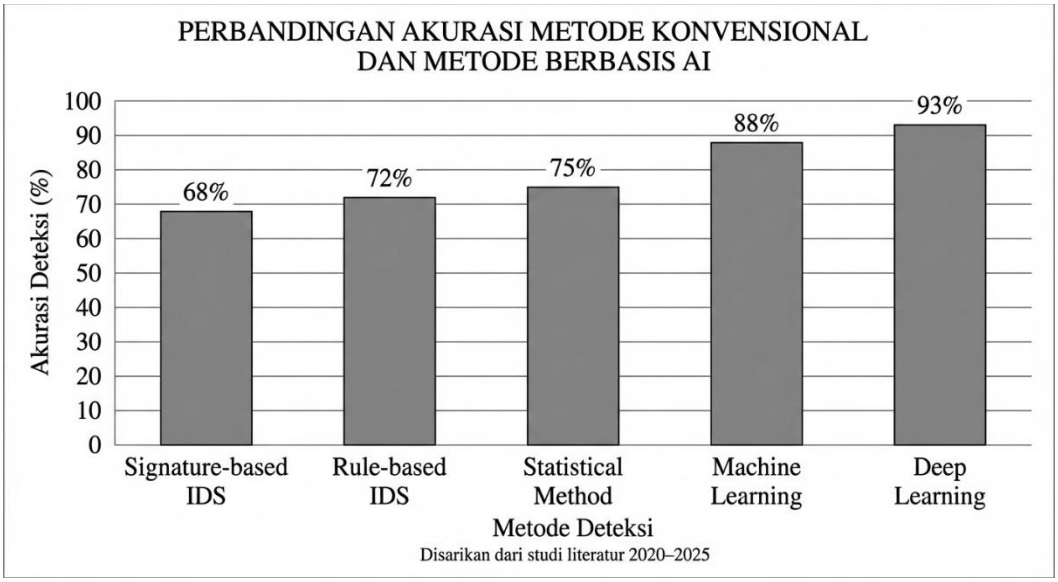
Hasil analisis menunjukkan bahwa pendekatan berbasis AI secara konsisten dilaporkan mampu meningkatkan efektivitas deteksi serangan siber dibandingkan metode konvensional. Sebagian besar penelitian yang dikaji melaporkan peningkatan akurasi deteksi intrusi serta penurunan tingkat false positive, terutama pada sistem dengan lalu lintas data yang besar dan dinamis. Temuan ini mengonfirmasi bahwa AI berperan signifikan dalam mengatasi keterbatasan sistem keamanan berbasis aturan statis.

Distribusi metode kecerdasan buatan yang digunakan dalam penelitian-penelitian terpilih menunjukkan dominasi algoritma machine learning dan deep learning. Algoritma machine learning seperti Random Forest, Support Vector Machine (SVM), dan XGBoost banyak digunakan karena stabilitas dan efisiensi komputasi, sedangkan model deep learning seperti Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM) lebih unggul dalam mendeteksi pola serangan kompleks dan bersifat temporal.
Ringkasan hasil klasifikasi metode dan fokus penelitian disajikan pada Tabel 2.

Tabel 2. Ringkasan Hasil Penelitian Terkait AI dalam Analisis Hacking

Fokus Penelitian	Metode AI Dominan	Lingkungan Sistem	Temuan Utama
Deteksi intrusi jaringan	Random Forest, SVM	Jaringan komputer	Akurasi meningkat, false positive menurun
Deteksi anomali	CNN, LSTM	Cloud & IoT	Efektif mendeteksi pola serangan kompleks
Deteksi serangan web	Machine Learning	Aplikasi web	Adaptif terhadap variasi serangan
Keamanan IoT	XGBoost, DL	IoT & IoT medis	Meningkatkan ketahanan sistem kritis
Sistem adaptif	Ensemble & AI adaptif	Sistem terdistribusi	Deteksi real-time dan pembelajaran berkelanjutan

Selain itu, hasil sintesis literatur menunjukkan bahwa integrasi AI dalam arsitektur keamanan modern, seperti Intrusion Detection Systems (IDS) dan Security Information and Event Management (SIEM), memungkinkan sistem keamanan beroperasi secara lebih proaktif. Sistem berbasis AI tidak hanya mendeteksi serangan yang sedang berlangsung, tetapi juga mampu memprediksi potensi eksploitasi kerentanan berdasarkan pola historis dan anomali perilaku.
Untuk menggambarkan perbandingan kinerja antara metode konvensional dan metode berbasis AI, penelitian ini menyusun visualisasi konseptual berupa grafik perbandingan akurasi yang dijelaskan pada Gambar 3.



Gambar 3. Grafik Perbandingan Akurasi Metode Konvensional dan Metode Berbasis AI

Gambar 3 menyajikan perbandingan tingkat akurasi deteksi serangan siber antara metode konvensional dan metode berbasis kecerdasan buatan (AI) yang disarikan dari hasil analisis literatur periode 2020–2025. Grafik batang menunjukkan bahwa metode konvensional, seperti signature-based intrusion detection system (IDS), rule-based IDS, dan pendekatan statistik, memiliki tingkat akurasi yang relatif lebih rendah dibandingkan metode berbasis AI. Akurasi metode konvensional berada pada kisaran 68–75%, yang menunjukkan keterbatasannya dalam mendeteksi serangan siber modern yang bersifat dinamis, kompleks, dan belum terdokumentasi sebelumnya.
Sebaliknya, metode berbasis AI, khususnya machine learning dan deep learning, menunjukkan peningkatan akurasi yang signifikan. Algoritma machine learning mencapai tingkat akurasi rata-rata sekitar 88%, sedangkan pendekatan deep learning mencatat akurasi tertinggi, yakni sekitar 93%. Perbedaan ini mencerminkan keunggulan AI dalam melakukan pembelajaran pola secara otomatis, mengenali hubungan nonlinier dalam data, serta mendeteksi anomali dan perilaku serangan yang sulit diidentifikasi oleh pendekatan berbasis aturan statis.

Secara keseluruhan, grafik tersebut mengindikasikan adanya selisih peningkatan akurasi antara 10–25% ketika sistem keamanan beralih dari metode konvensional ke metode berbasis AI. Peningkatan ini menjadi bukti empiris bahwa AI mampu meningkatkan efektivitas deteksi serangan siber, khususnya dalam lingkungan jaringan modern yang memiliki volume data besar dan pola lalu lintas yang sangat dinamis. Namun demikian, meskipun metode deep learning menawarkan akurasi tertinggi, penerapannya tetap memerlukan perhatian terhadap kebutuhan data pelatihan yang besar, kompleksitas komputasi, serta potensi kerentanan terhadap adversarial attacks. Oleh karena itu, hasil ini menegaskan bahwa pemilihan metode deteksi harus mempertimbangkan keseimbangan antara tingkat akurasi, efisiensi sistem, dan risiko implementasi.

Pembahasan

Hasil penelitian ini menunjukkan bahwa kecerdasan buatan telah menjadi komponen kunci dalam transformasi paradigma keamanan siber dari pendekatan reaktif menuju pendekatan proaktif dan prediktif. Temuan ini sejalan dengan berbagai penelitian sebelumnya yang menegaskan keunggulan AI dalam mendeteksi serangan siber yang bersifat adaptif dan kompleks. Machine learning terbukti efektif dalam menangani data keamanan yang terstruktur, sedangkan deep learning unggul dalam mengenali pola serangan yang bersifat non-linear dan berurutan.
Namun demikian, hasil analisis juga mengungkap bahwa peningkatan kinerja deteksi tidak terlepas dari konsekuensi teknis tertentu. Model deep learning, meskipun memiliki akurasi tinggi, umumnya membutuhkan sumber daya komputasi yang besar dan data pelatihan dalam jumlah signifikan. Kondisi ini menjadi tantangan tersendiri dalam implementasi pada lingkungan sistem dengan keterbatasan sumber daya, seperti IoT dan sistem edge computing.
Dari sisi implikasi keamanan, penelitian ini menemukan bahwa penggunaan AI juga memperkenalkan risiko baru, terutama terkait adversarial attacks dan isu interpretabilitas model. Sistem keamanan berbasis AI yang bersifat black-box berpotensi menyulitkan proses audit dan pengambilan keputusan, khususnya pada sistem kritis yang memerlukan transparansi tinggi. Temuan ini memperkuat pandangan bahwa AI dalam keamanan siber bersifat double-edged sword, yaitu mampu meningkatkan perlindungan sistem sekaligus membuka peluang eksploitasi baru apabila tidak dirancang dan dikelola dengan baik.
Implikasi strategis lainnya adalah perlunya integrasi antara pendekatan AI dan kebijakan keamanan organisasi. Hasil penelitian menunjukkan bahwa efektivitas sistem keamanan berbasis AI akan optimal apabila didukung oleh tata kelola keamanan yang kuat, pembaruan data pelatihan secara berkala, serta mekanisme evaluasi dan mitigasi risiko yang berkelanjutan. Dengan demikian, AI tidak diposisikan sebagai pengganti penuh sistem keamanan konvensional, melainkan sebagai komponen strategis yang melengkapi dan memperkuat arsitektur keamanan secara keseluruhan.

SIMPULAN

Penelitian ini menyimpulkan bahwa kecerdasan buatan telah menjadi elemen fundamental dalam pengembangan sistem keamanan siber modern, khususnya dalam analisis hacking dan identifikasi kerentanan sistem. Berdasarkan sintesis sistematis terhadap literatur ilmiah periode 2020-2025, ditemukan bahwa pendekatan berbasis machine learning dan deep learning secara konsisten menunjukkan kinerja yang lebih unggul dibandingkan metode keamanan konvensional dalam mendeteksi serangan siber yang bersifat dinamis, kompleks, dan adaptif. AI memungkinkan sistem keamanan untuk mengenali pola anomali yang tidak terdefinisi secara eksplisit, sehingga meningkatkan kemampuan deteksi terhadap serangan baru dan zero-day attacks.

Hasil kajian juga menunjukkan bahwa penerapan AI tidak terbatas pada satu jenis lingkungan sistem, melainkan mencakup jaringan komputer, aplikasi web, cloud computing, serta Internet of Things (IoT), termasuk sistem IoT medis yang bersifat kritis. Integrasi AI dalam Intrusion Detection System (IDS) dan arsitektur keamanan adaptif terbukti mampu meningkatkan akurasi deteksi, menurunkan tingkat false positive, serta mempercepat respons terhadap insiden keamanan. Dengan demikian, AI berkontribusi signifikan dalam pergeseran paradigma keamanan siber dari pendekatan reaktif menuju pendekatan proaktif dan prediktif.

Meskipun demikian, penelitian ini juga menegaskan bahwa pemanfaatan kecerdasan buatan dalam keamanan siber tidak terlepas dari berbagai tantangan. Kompleksitas model, kebutuhan data pelatihan yang besar, keterbatasan interpretabilitas, serta kerentanan terhadap adversarial attacks merupakan isu krusial yang perlu mendapatkan perhatian serius. Oleh karena itu, AI tidak dapat dipandang sebagai solusi tunggal, melainkan harus diintegrasikan secara strategis dengan mekanisme keamanan konvensional, kebijakan organisasi, dan kerangka tata kelola keamanan yang komprehensif.

DAFTAR PUSTAKA

Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. IT Journal Research and Development, 1(1), Article 16852. https://doi.org/10.25299/itjrd.2024.16852

Alotaibi, A., & Alenezi, M. (2023). Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. Future Internet, 15(2), 62. https://doi.org/10.3390/fi15020062

Atma, G. A. (2024). Toward resilient networks: AI and deep learning strategies for intrusion detection. Digitus: Journal of Computer Science Applications, 3(2), 881. https://doi.org/10.61978/digitus.v3i2.881

Aulia, N., & Satria, R. (2024). Automated detection of network intrusions using machine learning in real-time systems. International Journal of Computer Technology and Science, 1(2), 63. https://doi.org/10.62951/ijcts.v1i2.63

Budiansyah, A., Zulfan, Z., Nizamuddin, N., Candra, R. A., Ilham, D. N., & Nazaruddin, N. (2025). The effectiveness of machine learning techniques in anomaly detection for cyberattack prevention: Systematic literature review 2020–2025. Brilliance: Research of Artificial Intelligence, 5(1), 259–271. https://doi.org/10.47709/brilliance.v5i1.6124

Chandra, C., Mulya, D. P., & Faradika, F. (2025). Deteksi serangan siber menggunakan machine learning: Studi pada sistem informasi akademik. Jurnal Sistem Informasi dan Informatika, 3(2), 2139. https://doi.org/10.47233/jiska.v3i2.2139

Firdaus, D., Afin, A., Sumardi, I., & Chazar, C. (2025). Deteksi serangan pada jaringan Internet of Things medis menggunakan machine learning dengan algoritma XGBoost. Cyber Security dan Forensik Digital, 8(1), 34–42. https://doi.org/10.14421/csecurity.2025.8.1.5036

Fitria, E. Y., & Mutijarsa, K. (2023). Survei penelitian metode kecerdasan buatan untuk mendeteksi ancaman teknologi serangan siber. Jurnal Teknologi Informasi dan Ilmu Komputer. https://doi.org/10.25126/jtiik.2023107341

Kurdianto, B., Febriyanto, Y., & Servanda, Y. (2025). Intrusion detection system analysis to improve computer network security. Journal of Artificial Intelligence and Engineering Applications, 4(3), 1036. https://doi.org/10.59934/jaiea.v4i3.1036

Mahizzah, N. H., Dewi, I. K., Fernandes, A. L., & Saro, D. (2025). Improvement of IoT security with a machine learning-based intrusion detection system approach. Jurnal Responsive Teknik Informatika, 8(2), 1001. https://doi.org/10.36352/jr.v8i02.1001

Mohammed, M. S., & Talib, H. A. (2024). Using machine learning algorithms in intrusion detection systems: A review. Tikrit Journal of Pure Science, 29(3), 63–74. https://doi.org/10.25130/tjps.v29i3.1553

Nursiaga, R., Mulyana, N., & Sanjaya, H. (2025). Model jaringan neural untuk deteksi anomali pada sistem keamanan siber: Rancangan, implementasi, dan analisis. JAREKOM: Jurnal Jaringan dan Rekayasa Komputer, 1(1), 905. https://doi.org/10.9020/jarekom.v1i1.905

Provisi, N. R., Umar Gani, E., & Arfriandi, A. (2025). A machine learning approach to web attack detection. Jurnal Ilmiah Sistem Informasi (JUISI). https://doi.org/10.51903/3w0vwc80

Risyani, Y., Japit, S., Bombongan, C., Selamat, T., & Yuliana, Y. (2025). Sistem keamanan siber adaptif berbasis AI: Analisis kinerja, arsitektur, dan penerapannya pada organisasi modern. Jurnal Minfo Polgan, 14(2), 2999–3006. https://doi.org/10.33395/jmp.v14i2.15630

Safitri, Z. A., Haerani, E., Muzawi, R., Affandes, M., & Pizaini. (2024). Intrusion Detection System (IDS) pada Snort dengan bot Telegram sebagai sistem notifikasi terhadap serangan Syn Flood dan Ping of Death. SATIN – Sains dan Teknologi Informasi, 10(1), 1138. https://doi.org/10.33372/stn.v10i1.1138

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. Journal of Big Data, 11, 105. https://doi.org/10.1186/s40537-024-00957-y

Sekaranti, M., Kanan, M. K. J., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. Frontiers in Artificial Intelligence, 8, 1625891. https://doi.org/10.3389/frai.2025.1625891

Sunarti, M. A. E. H., & Wening, S. (2024). Desain inovatif sistem keamanan siber berbasis kecerdasan buatan menghadapi tantangan komputasi kuantum. Jurnal Ilmiah Sains Teknologi dan Informasi, 3(2), 1180. https://doi.org/10.59024/jiti.v3i2.1180