Peran Teknologi AI Machine Learning dalam Menangani Kompleksitas Ancaman Keamanan Siber di Era Digital

Dimas Rajendra Pandya Jiwanta
Sistem Informasi, Fakultas Teknologi Informasi, Universitas Merdeka Malang, Indonesia
E-mail: dimasrajendra0@gmail.com.

INFO ARTIKEL:

Kata Kunci :
Kecerdasan Buatan, Pembelajaran Mesin, Keamanan Siber, Systematic Literature Review, Sistem Deteksi Intrusi

ABSTRAK

Perkembangan teknologi digital pada era Revolusi Industri 4.0 telah mendorong transformasi berbagai sektor, namun di sisi lain turut meningkatkan kompleksitas ancaman keamanan siber. Serangan digital seperti malware, phishing, ransomware, dan Distributed Denial of Service (DDoS) semakin canggih dan dinamis, sehingga menuntut sistem pertahanan yang lebih adaptif dibandingkan pendekatan keamanan konvensional. Berdasarkan urgensi tersebut, penelitian ini bertujuan untuk meninjau peran teknologi Artificial Intelligence (AI) dan Machine Learning (ML) dalam menghadapi tantangan keamanan siber di era digital. Metode yang digunakan adalah Systematic Literature Review (SLR) dengan menganalisis empat artikel ilmiah yang relevan. Hasil kajian menunjukkan bahwa penerapan algoritma seperti Support Vector Machine (SVM), Random Forest (RF), Deep Neural Network (DNN), dan K-Means mampu meningkatkan akurasi serta kecepatan deteksi serangan, sekaligus mendorong pergeseran sistem keamanan dari pendekatan reaktif menuju proaktif dan prediktif. Selain itu, integrasi AI dan ML dengan teknologi pendukung seperti enkripsi modern dan blockchain terbukti memperkuat perlindungan data, khususnya pada lingkungan cloud computing dan Internet of Things (IoT). Meskipun demikian, implementasi teknologi ini masih menghadapi tantangan berupa kebutuhan dataset berkualitas tinggi, keterbatasan sumber daya komputasi, potensi serangan adversarial, serta isu etika dan privasi data. Secara keseluruhan, hasil kajian menegaskan bahwa AI dan ML memiliki peran strategis dalam membangun sistem keamanan siber yang adaptif, efisien, dan berkelanjutan, dengan catatan perlu didukung oleh kebijakan, infrastruktur, dan kesiapan sumber daya manusia yang memadai.

Keyword:
Artificial Intelligence, Machine Learning, Cybersecurity, Systematic Literature Review, Intrusion Detection Systems

ABSTRACT

The rapid development of digital technology in the era of the Fourth Industrial Revolution has driven significant advancements across various sectors, while simultaneously increasing the complexity of cybersecurity threats. Digital attacks such as malware, phishing, ransomware, and Distributed Denial of Service (DDoS) have become more sophisticated and dynamic, requiring security systems that are more adaptive than traditional approaches. In response to this urgency, this study aims to review the role of Artificial Intelligence (AI) and Machine Learning (ML) in addressing cybersecurity challenges in the digital era. This research employs a Systematic Literature Review (SLR) method by analyzing four relevant scientific articles. The findings indicate that the application of algorithms such as Support Vector Machine (SVM), Random Forest (RF), Deep Neural Network (DNN), and K-Means significantly improves the accuracy and speed of attack detection, while also shifting cybersecurity strategies from reactive to proactive and predictive approaches. Furthermore, the integration of AI and ML with supporting technologies such as advanced encryption and blockchain enhances data protection, particularly in cloud computing and Internet of Things (IoT) environments. Nevertheless, the implementation of these technologies still faces several challenges, including the need for high-quality datasets, substantial computational resources, vulnerability to adversarial attacks, and concerns related to data privacy and ethics. Overall, the results of this review confirm that AI and ML play a strategic role in building adaptive, efficient, and sustainable cybersecurity systems, provided that their adoption is supported by appropriate policies, infrastructure, and human resource readiness.

1. PENDAHULUAN

Pada era Revolusi Industri 4.0 yang sedang dialami saat ini, atau yang juga dikenal dengan istilah cyber-physical system. Dimana era ini merupakan suatu fase perkembangan industri yang ditandai oleh integrasi antara dunia fisik dan digital melalui pemanfaatan teknologi yang canggih (Purba, 2021). Revolusi Industri 4.0 ini membawa dampak besar terhadap cara manusia berinteraksi, bekerja, dan mengelola informasi. Perubahan tersebut dapat dilihat dari semakin meluasnya digitalisasi di berbagai bidang, mulai dari pendidikan, pemerintahan, kesehatan, hingga industri manufaktur. Penerapan sistem berbasis digital memungkinkan proses kerja menjadi lebih cepat, efisien, dan terintegrasi lintas sektor (Hasibuan, 2025). Selain itu, kemajuan konektivitas melalui jaringan internet berkecepatan tinggi menjadikan arus informasi lebih terbuka, transparan, dan mudah diakses oleh masyarakat luas. Transformasi ini juga mendorong pergeseran paradigma ekonomi dari berbasis sumber daya alam menuju ekonomi berbasis pengetahuan dan data. Dengan demikian, Revolusi Industri 4.0 tidak hanya dipahami sebagai fenomena teknologi, tetapi juga sebagai proses sosial dan ekonomi yang mengubah struktur aktivitas manusia di era modern. Perubahan besar ini turut menggeser paradigma ekonomi dunia dari yang berfokus pada sumber daya alam menuju ekonomi berbasis pengetahuan dan data (*knowledge and data-driven economy*). Dalam konteks ini, data menjadi sumber daya strategis yang bernilai tinggi dan digunakan sebagai dasar dalam inovasi, pengambilan keputusan, serta pengembangan strategi bisnis di berbagai sektor. Dengan demikian, Revolusi Industri 4.0 bukan hanya fenomena teknologi semata, tetapi juga merupakan perubahan sosial, ekonomi, dan budaya yang kompleks yang secara mendalam mempengaruhi pola hidup dan aktivitas manusia di era modern(Prasetyo, 2018). Kondisi ini menuntut manusia untuk beradaptasi secara cepat terhadap kemajuan teknologi, meningkatkan kemampuan literasi digital, serta mampu menghadapi tantangan baru seperti isu keamanan siber, privasi data, dan ketergantungan terhadap sistem digital. Secara keseluruhan, Revolusi Industri 4.0 menjadi tonggak penting dalam perjalanan menuju masyarakat cerdas (*smart society*) yang berbasis pada inovasi, kolaborasi, dan keberlanjutan di era digital global.

Bersama dengan adanya perubahan besar yang terjadi pada era Revolusi Industri 4.0, memunculkan berbagai teknologi seperti *Internet of Things* (IoT), *Artificial Intelligence* (AI), cloud computing, big data analytics, dan robotika yang memiliki peran penting dalam membentuk ekosistem digital yang saling terhubung sehingga memungkinkan terjadinya pertukaran data secara *real-time* antara mesin, manusia, dan system. Contohnya teknologi IoT yang memungkinkan perangkat fisik saling terhubung dan berkomunikasi secara real-time untuk mengumpulkan serta mengirimkan data dari berbagai sumber. Data yang dihasilkan kemudian dikelola melalui sistem cloud computing dan dianalisis menggunakan pendekatan big data analytics untuk mendukung proses pengambilan keputusan yang cepat dan berbasis informasi. Sementara itu, penerapan robotika dalam industri modern mempercepat proses produksi dengan tingkat presisi yang tinggi, serta mengurangi ketergantungan terhadap tenaga kerja manual (Hadi, 2025). Integrasi seluruh teknologi ini tidak hanya meningkatkan efisiensi dan produktivitas, tetapi juga menciptakan ekosistem kerja baru yang lebih fleksibel, responsif, dan berbasis data. Namun, semakin luasnya digitalisasi ini juga diiringi dengan peningkatan risiko terhadap keamanan sistem dan kerahasiaan informasi yang menjadi fondasi utama dari transformasi digital tersebut. Seiring waktu dengan kemajuan teknologi digital yang semakin luas, ancaman keamanan cyber kian terus meningkat. Hal ini memunculkan dampak negatif seperti terkenanya serangan *hacking*, *ransomware*, *malware*, *DDos*, dan serangan lainnya. Serangan ini terjadi karena luasnya jaringan yang sangat mudah untuk masuknya serangan cyber yang dimanfaatkan oleh pelaku kejahatan (Yusep Ginanjar, 2022). Perangkat yang terhubung ke internet melalui komputer, ponsel hingga server cloud menjadi titik ancaman bagi pelaku untuk mengeksploitasi sistem. Penggunaan metode lama seperti antivirus tidak cukup dalam menghadapi ancaman digital yang terus modern, karena dengan adanya teknologi yang canggih pelaku dapat memanipulasi mesin untuk menembus sistem.

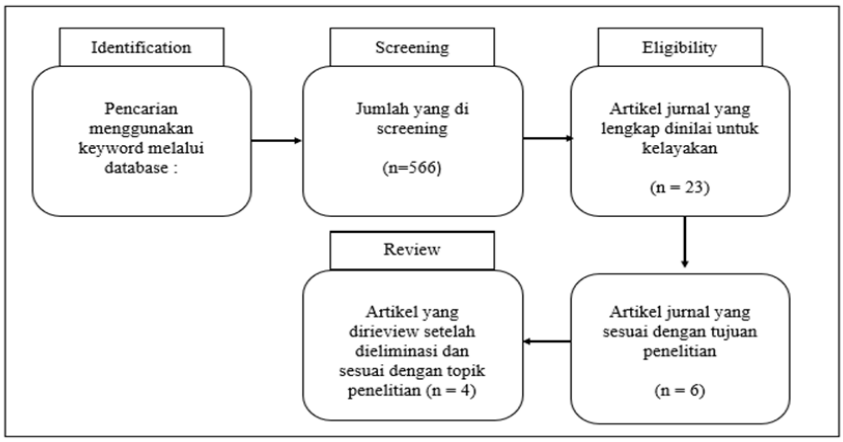
Guna menghadapi peningkatan kompleksitas ancaman siber di era digital, terdapat beberapa teknologi yang dapat mengatasi ancaman tersebut. Teknologi tersebut adalah *Artificial Intelligence* (AI) dan *Machine Learning* (ML) yang dapat menjadi pendekatan baru untuk meningkatkan efektivitas

sistem keamanan. Berbeda dengan metode tradisional yang hanya mengandalkan suatu pola serangan yang sudah diketahui, AI dan ML memiliki kemampuan untuk mempelajari data, mengenali pola ketidaknormalan, serta mendeteksi ancaman baru yang belum teridentifikasi sebelumnya (*zero-day attack*). Teknologi ini dapat diterapkan dalam berbagai aspek keamanan siber seperti sistem deteksi intrusi (*Intrusion Detection System*), analisis *malware*, serta pencegahan *phishing* secara otomatis. Menurut (Rosanti, 2025), penerapan algoritma *Support Vector Machine* (SVM) dan Random Forest dalam sistem deteksi phishing berbasis AI di Indonesia menunjukkan efektivitas AI dalam mendeteksi ancaman dinamis. (Amanda, 2025) juga menjelaskan bahwa sistem deteksi intrusi berbasis *AI-powered IDS* mampu melakukan analisis lalu lintas jaringan secara *real-time* dan menurunkan tingkat kesalahan deteksi. Selain itu, integrasi AI dengan *Big Data Analytics* dapat membantu dalam menganalisis jutaan log keamanan dalam waktu singkat untuk menemukan pola serangan tersembunyi. Dengan kemampuan prediksinya, AI dan ML menjadi pilar utama dalam menciptakan sistem keamanan siber yang tangguh dan responsif di tengah teknologi digital yang terus berkembang.

Meskipun teknologi *AI* dan *ML* memberikan solusi inovatif dalam keamanan siber, penerapannya masih mengalami sejumlah tantangan yang cukup signifikan. Salah satu kendala utama adalah kualitas dan ketersediaan data yang diperlukan untuk melatih model pembelajaran mesin. Sistem keamanan berbasis AI memerlukan data dalam jumlah besar dan berkualitas tinggi agar mampu mengenali pola serangan secara akurat, namun data tersebut seringkali terbatas atau tidak representative (Maulani, 2025). Selain itu, kompleksitas algoritma AI menimbulkan tantangan baru dalam hal interpretabilitas model (model *explainability*), di mana keputusan sistem sulit dijelaskan secara transparan kepada pengguna. Tantangan lain juga muncul dari risiko adversarial attack, yaitu manipulasi input data yang dapat mengecoh model AI untuk salah dalam mengenali ancaman. Di Indonesia, keterbatasan infrastruktur teknologi dan sumber daya manusia yang ahli di bidang keamanan siber berbasis AI juga menjadi penghambat utama (Santika & Rianto, 2025). Belum adanya regulasi nasional yang menyeluruh mengenai keamanan berbasis kecerdasan buatan juga menyebabkan penerapan AI dan ML di bidang *cyber* masih memerlukan pendekatan yang bertahap. Dengan demikian, meskipun teknologi ini menjanjikan peningkatan keamanan digital, implementasinya tetap memerlukan strategi yang matang serta dukungan kebijakan dan kesiapan sumber daya. Oleh karena itu, literature review ini dilakukan untuk mengidentifikasi peran teknologi AI dan ML dalam menangani kompleksitas ancaman keamanan *cyber* di era digital. *Literature review* ini juga bertujuan untuk memberikan arah pengembangan riset ke depan yang relevan dengan kebutuhan keamanan digital nasional di tengah percepatan transformasi industri 4.0.

2. METODE

Metode dalam penelitian ini adalah *Systematic Literature Review* (SLR). SLR merupakan teknik penelitian yang bertujuan mengidentifikasi, mengevaluasi, dan mensintesis temuan dari berbagai studi secara sistematis dan objektif (Diah, 2022). Tujuan utama dari metode ini adalah untuk memperoleh pemahaman yang menyeluruh mengenai perkembangan penerapan teknologi *Artificial Intelligence* (AI) dan *Machine Learning* (ML) dalam menghadapi kompleksitas ancaman keamanan siber di era digital. Dalam melakukan penelitian dengan metode SLR tentunya memiliki beberapa langkah. Menurut (Hendrik, 2023) tahapan penelitian dengan metode SLR yaitu, *identification*, *screening*, *eligibility*, dan *review*. Dalam mencari serta mengumpulkan data terkait topik penelitian, yaitu Peran Teknologi AI *Machine Learning* dalam Menangani Kompleksitas Ancaman Keamanan Siber di Era Digital pada kolom pencarian google scholar. Sebagai bentuk transparansi dalam proses seleksi literatur, penelitian ini menyajikan bagan langkah-langkah pencarian dan penyaringan data menggunakan diagram PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses)*. Diagram ini menggambarkan secara visual alur proses mulai dari jumlah artikel yang ditemukan pada tahap awal, jumlah artikel yang dieliminasi pada tahap penyaringan, hingga jumlah akhir artikel yang digunakan dalam analisis. Dengan adanya diagram PRISMA, proses penelitian menjadi lebih terukur, sistematis, dan mudah dipahami, sehingga dapat memperkuat kredibilitas serta akurasi hasil kajian dalam penelitian ini. Berikut merupakan bagan langkah-langkah dalam pencarian data dengan menggunakan diagram PRISMA



Pada tahap *identification*, peneliti melakukan pencarian awal terhadap literatur yang relevan menggunakan kata kunci yang berkaitan dengan topik penelitian, dalam hal ini mengenai peran AI dan ML dalam menghadapi ancaman keamanan siber. Tahap screening kemudian dilakukan untuk menyaring hasil pencarian dengan menghapus duplikasi dan literatur yang tidak relevan dengan fokus penelitian. Selanjutnya, tahap *eligibility* difokuskan pada peninjauan lebih mendalam terhadap abstrak dan isi artikel guna memastikan kesesuaian dengan kriteria inklusi dan eksklusi yang telah ditentukan. Tahap terakhir, yaitu review, merupakan proses analisis dan sintesis dari seluruh literatur yang telah lolos tahap sebelumnya untuk menghasilkan temuan yang bermakna dan mendukung tujuan penelitian

Kedua *screening* merupakan langkah lanjutan setelah proses identifikasi, di mana seluruh literatur yang telah diperoleh dari hasil pencarian awal diseleksi untuk memastikan kesesuaiannya dengan fokus penelitian. Pada tahap ini, peneliti meninjau judul dan abstrak dari setiap artikel guna menyaring publikasi yang tidak relevan, seperti penelitian yang tidak berkaitan langsung dengan penerapan Artificial Intelligence (AI) dan *Machine Learning* (ML) dalam keamanan siber. Selain itu, artikel duplikat juga dihapus untuk menghindari pengulangan data dalam analisis. Proses penyaringan ini bertujuan untuk mempersempit jumlah literatur sehingga hanya artikel yang benar-benar relevan dan memiliki kontribusi signifikan terhadap topik penelitian yang akan dilanjutkan ke tahap berikutnya.

Tahap berikutnya, yaitu *eligibility*, difokuskan pada pemeriksaan mendalam terhadap isi lengkap atau full text dari artikel yang telah lolos tahap screening. Pada tahap ini, peneliti mengevaluasi kelayakan artikel berdasarkan kriteria inklusi dan eksklusi yang telah ditentukan sebelumnya. Contohnya, hanya artikel yang dipublikasikan dalam lima tahun terakhir, memiliki metode penelitian yang jelas, serta membahas penerapan *AI* dan *ML* secara spesifik dalam keamanan siber yang akan disertakan dalam analisis. Artikel yang tidak memenuhi kriteria atau memiliki kualitas metodologis yang kurang baik akan dikeluarkan. Proses ini memastikan bahwa hanya literatur yang kredibel, relevan, dan berkualitas tinggi yang menjadi dasar kajian penelitian.

Tahap terakhir yaitu *review* yang menjadi inti dari keseluruhan proses S*ystematic Literature Review*. Pada tahap ini, peneliti melakukan analisis secara sistematis terhadap seluruh literatur yang telah dinyatakan layak untuk menelusuri pola, tren, kontribusi, serta celah penelitian (*research gap*) yang ada. Analisis dilakukan dengan membandingkan hasil temuan dari berbagai studi, mengamati pendekatan yang digunakan, serta menilai efektivitas teknologi AI dan ML dalam mendeteksi, mencegah, dan merespons ancaman keamanan siber di berbagai konteks. Hasil analisis ini kemudian disintesis menjadi kesimpulan yang memberikan gambaran menyeluruh tentang perkembangan terkini penerapan AI dan ML dalam bidang keamanan siber, sekaligus menjadi dasar untuk rekomendasi penelitian di masa mendatang.

Pada tahap *identification*, peneliti melakukan pencarian awal terhadap literatur yang relevan menggunakan kata kunci yang berkaitan dengan topik penelitian, dalam hal ini mengenai peran AI dan ML dalam menghadapi ancaman keamanan siber. Tahap screening kemudian dilakukan untuk menyaring hasil pencarian dengan menghapus duplikasi dan literatur yang tidak relevan dengan fokus penelitian. Selanjutnya, tahap eligibility difokuskan pada peninjauan lebih mendalam terhadap abstrak dan isi artikel guna memastikan kesesuaian dengan kriteria inklusi dan eksklusi yang telah ditentukan. Tahap terakhir, yaitu review, merupakan proses analisis dan sintesis dari seluruh literatur yang telah lolos tahap sebelumnya untuk menghasilkan temuan yang bermakna dan mendukung tujuan penelitian

Kedua *screening* merupakan langkah lanjutan setelah proses identifikasi, di mana seluruh literatur yang telah diperoleh dari hasil pencarian awal diseleksi untuk memastikan kesesuaiannya dengan fokus penelitian. Pada tahap ini, peneliti meninjau judul dan abstrak dari setiap artikel guna menyaring publikasi yang tidak relevan, seperti penelitian yang tidak berkaitan langsung dengan penerapan *Artificial Intelligence* (AI) dan *Machine Learning* (ML) dalam keamanan siber. Selain itu, artikel duplikat juga dihapus untuk menghindari pengulangan data dalam analisis. Proses penyaringan ini bertujuan untuk mempersempit jumlah literatur sehingga hanya artikel yang benar-benar relevan dan memiliki kontribusi signifikan terhadap topik penelitian yang akan dilanjutkan ke tahap berikutnya.

Tahap berikutnya, yaitu *eligibility*, difokuskan pada pemeriksaan mendalam terhadap isi lengkap atau full text dari artikel yang telah lolos tahap screening. Pada tahap ini, peneliti mengevaluasi kelayakan artikel berdasarkan kriteria inklusi dan eksklusi yang telah ditentukan sebelumnya. Contohnya, hanya artikel yang dipublikasikan dalam lima tahun terakhir, memiliki metode penelitian yang jelas, serta membahas penerapan AI dan ML secara spesifik dalam keamanan siber yang akan disertakan dalam analisis. Artikel yang tidak memenuhi kriteria atau memiliki kualitas metodologis yang kurang baik akan dikeluarkan. Proses ini memastikan bahwa hanya literatur yang kredibel, relevan, dan berkualitas tinggi yang menjadi dasar kajian penelitian.

Tahap terakhir yaitu *review* yang menjadi inti dari keseluruhan proses Systematic Literature Review. Pada tahap ini, peneliti melakukan analisis secara sistematis terhadap seluruh literatur yang telah dinyatakan layak untuk menelusuri pola, tren, kontribusi, serta celah penelitian (*research gap*) yang ada. Analisis dilakukan dengan membandingkan hasil temuan dari berbagai studi, mengamati pendekatan yang digunakan, serta menilai efektivitas teknologi AI dan ML dalam mendeteksi, mencegah, dan merespons ancaman keamanan siber di berbagai konteks. Hasil analisis ini kemudian disintesis menjadi kesimpulan yang memberikan gambaran menyeluruh tentang perkembangan terkini penerapan AI dan ML dalam bidang keamanan siber, sekaligus menjadi dasar untuk rekomendasi penelitian di masa mendatang.

3. HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan ini hendaknya peneliti menjabar hasil yang diperoleh dari setiap tahapan yang sudah dicantumkan pada bagian metode. Misalnya penelitian dimulai dengan tahapan observasi, maka uraikan secara runut apa saja yang dilakukan dan bagaimana caranya tahapan observasi ini dirampungkan sehingga mendapatkan hasil observasi yang diharapkan.

3.1 Hasil

Penelitian ini dilakukan menggunakan metode *Systematic Literature Review* (SLR), di mana proses penelusuran data dilakukan secara sistematis melalui tahapan *identification*, *screening*, dan *eligibility* hingga diperoleh artikel yang benar-benar relevan dengan fokus penelitian. Pada tahap awal penelusuran literatur, sejumlah artikel ditemukan melalui basis data ilmiah seperti Google Scholar menggunakan kata kunci terkait teknologi *Artificial Intelligence* (AI), *Machine Learning* (ML), dan keamanan siber. Setelah dilakukan penyaringan terhadap judul dan abstrak, kemudian eliminasi artikel duplikat serta peninjauan lebih lanjut terhadap kelayakan isi (*full-text review*), hanya empat artikel ilmiah yang memenuhi seluruh kriteria inklusi.

Kriteria pemilihan tersebut mencakup relevansi dengan topik keamanan siber berbasis AI dan ML, publikasi dalam kurun lima tahun terakhir agar mendukung kebaruan penelitian, adanya temuan kuantitatif atau deskriptif terkait akurasi, metode, atau performa model, dan keterkaitan langsung dengan sistem deteksi, pencegahan, atau pengamanan data digital. Keempat artikel tersebut dianalisis untuk mengetahui bagaimana AI dan ML digunakan sebagai pendekatan teknologi perlindungan digital, jenis serangan siber yang diatasi, algoritma yang digunakan, serta kelebihan dan keterbatasan penerapannya pada industri digital. Ringkasan karakteristik artikel terdapat pada tabel berikut:

Tabel 3.1. Tabel karakteristik artikel terkait

Peneliti & Tahun	Algoritma	Jenis Ancaman	Akurasi	Kelebihan dan Keterbatasan
(Wiranda et al., 2022)	SVM, RF, K-Means, DNN	Malware, Phishing, DDoS	96%	Efektif untuk dataset besar, tetapi membutuhkan waktu komputasi tinggi.
(Taufik, 2025)	Clustering, Classification, Anomaly Detection	Intrusion & Data Breach	94%	Mampu mengenali pola baru; sulit dioptimalkan untuk data real-time
(Pongoh et al., 2024)	Deep Learning, Neural Network	Multi-layer Threat Detection	95%	Akurasi tinggi, namun kurang efisien untuk sistem resource-limited
(Asnawi, 2025)	AES, Blockchain-based AI	Cloud & IoT Security	-	Melindungi integritas data, tetapi belum teruji pada skala nasional
Enhancing Cyber Security through AI & ML (2024)	SVM, Random Forest, CNN, Deep Learning	Malware, Intrusion Detection, Anomaly Detection	90–99%	Cakupan luas, komprehensif, namun Tidak melakukan eksperimen langsung
AI in Cybersecurity: Review & Case Study (2024)	Neural Network, ML-based IDS	Network intrusion, cyber attacks	96%	Ada studi kasus nyata Namun Dataset terbatas
Applications of ML in Cyber Security (2024)	KNN, SVM, Decision Tree, DL	Phishing, malware, IDS	-	Analisis komparatif algoritma namun Tidak fokus pada real-time system
AI-Powered Security Mechanisms (2024)	NLP, Deep Learning, Behavioral AI	Phishing, social engineering	-	Fokus mekanisme pertahanan modern tetapi Kurang detail evaluasi performa
AI & ML in Cybersecurit	DL, GAN, XAI,	Advanced Persistent	-	Membahas masa depan & tantangan

y: State-of-the-art (2025)	Federated Learning	Threats (APT), adversarial attacks		namun Kompleks, sulit diimplementasikan
Ekowati, Poernomo & Nindyatama (2025)	ML + AI-based model untuk ancaman kuantum	Ancaman pascakomputasi kuantum	-	Integrasi AI + post-quantum namun Masih bersifat simulasi, dan bukan real-world

Berdasarkan tabel tersebut dapat disimpulkan bahwa seluruh penelitian memperlihatkan peningkatan kinerja sistem keamanan digital melalui penggunaan AI dan ML, meskipun masih ditemukan sejumlah kendala teknis dalam implementasinya.

3.2 Pembahasan

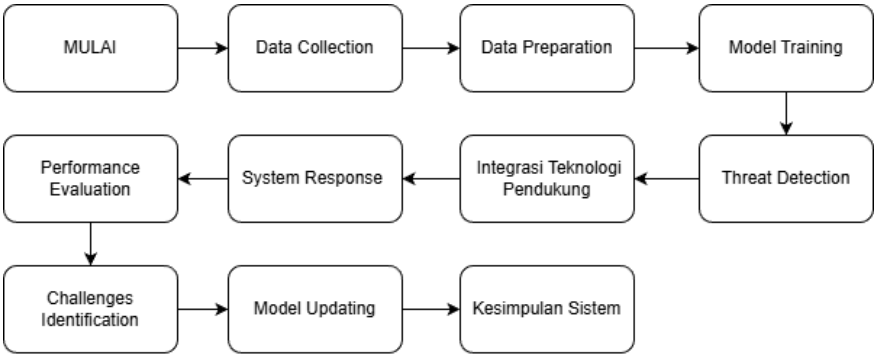
Penerapan Artificial Intelligence (AI) dan Machine Learning (ML) dalam keamanan siber menunjukkan transformasi signifikan dalam cara sistem mendeteksi dan menghadapi ancaman digital. Berdasarkan hasil analisis literatur yang diperoleh melalui metode Systematic Literature Review (SLR), dapat dilihat bahwa sebagian besar penelitian sepakat bahwa AI dan ML mampu meningkatkan efektivitas deteksi ancaman dibandingkan metode tradisional berbasis tanda tangan (signature-based system). Teknologi ini memungkinkan sistem untuk belajar secara mandiri dari pola data dan mengidentifikasi aktivitas mencurigakan yang tidak selalu terlihat oleh sistem keamanan konvensional. Penelitian oleh (Wiranda et al., 2022) dan (Pongoh et al., 2024) menunjukkan bahwa model deep learning, seperti Deep Neural Network (DNN), mampu memberikan tingkat akurasi yang sangat tinggi dalam klasifikasi ancaman. Hal ini menunjukkan bahwa semakin kompleks algoritma yang digunakan, semakin tinggi kemampuan sistem dalam memahami variasi serangan siber. Bahkan, beberapa algoritma mampu bekerja secara real-time sehingga memberikan peringatan lebih cepat sebelum serangan berlangsung lebih jauh. Dengan demikian, dapat disimpulkan bahwa AI dan ML berkontribusi penting dalam peningkatan kualitas sistem keamanan digital modern.

Kemampuan deteksi terhadap ancaman baru atau serangan zero-day merupakan salah satu keunggulan utama teknologi berbasis machine learning dibandingkan sistem keamanan tradisional. Dalam penelitian (Taufik, 2025), teknik anomaly detection dan clustering terbukti mampu mengenali pola serangan yang tidak memiliki tanda tangan atau database serangan terdahulu. Ini berarti bahwa sistem tidak hanya mengandalkan data serangan masa lalu, tetapi juga mampu mendeteksi penyimpangan perilaku sistem yang mengindikasikan adanya ancaman baru. Keunggulan ini sangat relevan mengingat pelaku kejahatan siber terus mengembangkan metode serangan yang lebih canggih dan sulit dilacak. Selain itu, kemampuan pembelajaran berkelanjutan (continuous learning) memungkinkan model AI untuk meningkatkan akurasi deteksi ancaman seiring bertambahnya data baru yang dipelajari. Namun, penerapan metode ini masih memerlukan kemampuan analisis tingkat lanjut agar tidak terjadi false positive yang dapat mengganggu aktivitas sistem. Oleh karena itu, kecerdasan adaptif menjadi salah satu karakter unik AI dan ML dalam menghadapi dinamika ancaman digital.

Selain peran AI dalam deteksi serangan, integrasi teknologi keamanan tambahan seperti blockchain dan Advanced Encryption Standard (AES) memperluas cakupan penggunaan inovasi digital dalam keamanan siber. Penelitian (Asnawi, 2025) menunjukkan bahwa integrasi AI dengan blockchain menciptakan model keamanan yang tidak hanya responsif tetapi juga mampu menjaga integritas data. Blockchain memungkinkan setiap perubahan sistem terekam secara permanen dan tidak dapat dimanipulasi sehingga memperkuat transparansi dan akuntabilitas proses keamanan digital. AI kemudian berfungsi sebagai sistem pengawas yang memantau setiap hash data untuk mengidentifikasi pola-pola tidak wajar yang dapat menunjukkan adanya upaya peretasan. Pendekatan ini dinilai sangat relevan terutama pada Internet of Things (IoT) dan cloud computing yang memiliki banyak jalur akses rentan serangan. Meski pendekatan ini menjanjikan, penelitian lanjutan masih diperlukan karena belum

banyak diuji dalam skala implementasi nasional. Dengan demikian, integrasi antara AI, ML, dan teknologi keamanan modern lainnya dapat menjadi langkah strategis dalam membangun sistem keamanan yang berlapis dan sulit ditembus. Namun, meskipun berbagai penelitian menunjukkan potensi besar AI dan ML dalam memperkuat keamanan digital, penerapannya masih menghadapi sejumlah tantangan teknis maupun non-teknis. Salah satu kendala terbesar adalah kebutuhan dataset yang besar dan berkualitas untuk melatih model AI agar mampu menghasilkan prediksi yang akurat. Apabila dataset tidak representatif, maka model rentan mengalami error atau gagal mendeteksi ancaman kompleks. Di samping itu, komputasi untuk menjalankan algoritma tingkat lanjut seperti deep learning membutuhkan perangkat keras berkapasitas tinggi, sehingga implementasi di lingkungan nyata memerlukan investasi infrastruktur yang tidak sedikit. Selain itu, muncul ancaman baru berupa adversarial attack, yaitu manipulasi input data yang secara sengaja dibuat untuk mengecoh model AI agar memberikan hasil analisis yang salah. Tantangan-tantangan ini menunjukkan bahwa penerapan AI bukan hanya soal teknologi, tetapi juga kesiapan sumber daya manusia, kebijakan tata kelola data, dan penanganan risiko yang tepat. Tahapan-tahapan tersebut dapat dilihat dalam diagram flow chart berikut.

Gambar 3.1 Diagram Flow Chart Tahapan Menangani Kompleksitas Ancaman Keamanan Siber



Berdasarkan keseluruhan pembahasan tersebut, dapat dilihat bahwa AI dan ML bukan hanya alat komputasi pendukung, tetapi telah berkembang menjadi fondasi baru dalam model keamanan digital modern. Banyak temuan dalam literatur menunjukkan bahwa teknologi ini mampu merespons serangan siber secara lebih dinamis dan adaptif dibandingkan sistem keamanan tradisional. Dengan kemampuan pembelajaran otomatis dan analisis berbasis data dalam skala besar, AI dan ML secara bertahap mengubah pendekatan keamanan dari reaktif menjadi prediktif. Namun demikian, keberhasilan penerapan teknologi ini sangat bergantung pada sinergi antara infrastruktur digital, regulasi yang memadai, kesiapan sumber daya manusia, dan evaluasi berkelanjutan terhadap performa sistem. Jika seluruh aspek tersebut terpenuhi, maka teknologi AI dan ML berpotensi menjadi solusi utama dalam menghadapi kompleksitas ancaman keamanan digital di masa depan. Dengan demikian, integrasi sistem keamanan berbasis kecerdasan buatan bukan hanya sebuah pilihan, tetapi menjadi kebutuhan strategis di era transformasi digital saat ini.

4. KESIMPULAN

Berdasarkan hasil Systematic Literature Review (SLR) terhadap artikel-artikel ilmiah yang dianalisis, dapat ditarik beberapa kesimpulan utama sebagai berikut:

a) Hasil kajian menunjukkan bahwa penerapan teknologi *Artificial Intelligence* (AI) dan *Machine Learning* (ML) telah mengubah paradigma keamanan siber dari pendekatan yang bersifat reaktif menjadi lebih proaktif dan prediktif. AI memungkinkan pemrosesan data keamanan dalam skala besar dan kompleks, sementara ML berperan dalam mempelajari pola serangan dari data historis sehingga sistem mampu mengantisipasi ancaman sebelum berdampak signifikan terhadap infrastruktur digital.
b) Berbagai algoritma seperti *Support Vector Machine (SVM)*, *Random Forest*, *K-Nearest Neighbor (KNN)*, *Decision Tree*, *Neural Network*, dan *Deep Learning* terbukti efektif dalam menangani ancaman keamanan siber, termasuk malware, *intrusion detection*, phishing, *anomaly detection*,

hingga *Advanced Persistent Threats (APT)*. Beberapa studi melaporkan tingkat akurasi deteksi yang tinggi, bahkan mencapai lebih dari 90%, yang menunjukkan potensi besar AI dan ML dalam meningkatkan ketepatan dan kecepatan respons sistem keamanan.

c) Artikel yang menyertakan studi kasus nyata memberikan bukti empiris bahwa sistem keamanan berbasis AI dan ML dapat diimplementasikan secara efektif dalam lingkungan operasional. Sementara itu, pendekatan analisis komparatif antar algoritma membantu mengidentifikasi kelebihan dan keterbatasan masing-masing metode, meskipun sebagian besar penelitian masih belum sepenuhnya berfokus pada penerapan sistem secara *real-time*.

d) Integrasi AI dan ML dengan teknologi pendukung seperti *deep learning-based intrusion detection systems*, *Natural Language Processing (NLP)*, *behavioral analysis*, serta pendekatan kriptografi modern, termasuk *blockchain-based encryption* dan *post-quantum security models*, memberikan lapisan perlindungan tambahan terhadap privasi dan integritas data. Namun, sebagian besar pendekatan tersebut masih berada pada tahap konseptual atau simulasi dan memerlukan validasi lebih lanjut dalam skenario dunia nyata.

e) Meskipun menunjukkan potensi yang besar, penerapan AI dan ML dalam keamanan siber masih menghadapi sejumlah tantangan, antara lain kebutuhan akan dataset yang besar dan representatif, keterbatasan sumber daya komputasi, risiko *adversarial attacks* terhadap model AI, serta isu etika dan perlindungan privasi data. Tantangan ini menuntut pendekatan yang lebih holistik dan berkelanjutan dalam pengembangan sistem keamanan berbasis AI.

f) Oleh karena itu, keberhasilan penerapan AI dan ML dalam keamanan siber tidak hanya bergantung pada aspek teknologi, tetapi juga pada dukungan kebijakan, kesiapan infrastruktur, tata kelola data yang baik, serta pengembangan sumber daya manusia yang kompeten. Kolaborasi antara akademisi, industri, dan pemerintah menjadi faktor kunci agar teknologi AI dan ML dapat dikembangkan secara bertanggung jawab dan berkelanjutan sebagai fondasi utama dalam membangun ekosistem digital yang aman dan tangguh.

DAFTAR PUSTAKA

Akhtar, Z. B., & Rawol, A. T. (2024). *Enhancing Cybersecurity through AI-Powered Security Mechanisms*. IT Journal Research and Development. https://doi.org/10.25299/itjrd.2024.16852

Amanda, D. P., & Absharina, E. D. (2025). *Implementasi AI-Powered Intrusion Detection Systems untuk Mendeteksi Ancaman Keamanan Pada Big Data*. Simtek: jurnal sistem informasi dan teknik komputer, 10(1), 29-33.

Asnawi. (2025). *Tinjauan Pustaka Sistematis Tentang Teknologi Keamanan Data : Tren Dan Tantangan*. *2*(2), 72–79.

Diah. (2022). *Systematic Literature Review Di Bidang Sistem Informasi Dan Systematic Literature Review In Information Systems And Computer Engineering : A Guideline*. *9*(2), 263–268. https://doi.org/10.25126/jtiik.202293884

Ekowati, M. A. S., Poernomo, M. H., & Nindyatama, Z. P. (2025). *Integration of artificial intelligence in cyber security systems to counter quantum computing threats*. Jurnal Mandiri IT, 13(4), 389–398. https://doi.org/10.35335/mandiri.v13i4.388

Hasibuan, M. A. A., Pyung, D., Saktiawan, G. A., Al-fandi, D., Fatahillah, M., Syahputra, B. D., ... & Albais, R. (2025). *Pemanfaatan Teknologi Komputer Dalam Meningkatkan Efisiensi Kerja Di Era Digital*. Jurnal Intelek Insan Cendikia, 2(8), 14388-14393.

Hendrik, B. (2023). *Penggunaan Metode Systematic Literatur Review Untuk Menganalisis Artikel Sistem Pakar Metode Forward Chaining*. *1*(2), 1–5.

Maulani, G., Hasan, F. N., Setiawan, D., Bowo, I. T., Ardhana, V. Y. P., Ramdhani, Y., ... & Safitri, R. (2025). Machine Learning. Mega Press Nusantara.

Merlano, C. (2024). *Enhancing Cyber Security through Artificial Intelligence and Machine Learning: A Literature Review*. Journal of Cyber Security, 6(1), 89–116. https://doi.org/10.32604/jcs.2024.056164

Mohamed, N. (2025). *Artificial intelligence and machine learning in cybersecurity: State-of-the-art and future paradigms. Knowledge & Information Systems,* 67(8), 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Okdem, S., & Okdem, S. (2024). *Artificial Intelligence in Cybersecurity: A Review and a Case Study. Applied Sciences,* 14(22), 10487. https://doi.org/10.3390/app142210487

Prasetyo, B., & Trisyanti, U. (2018). *Revolusi industri 4.0 dan tantangan perubahan sosial*. IPTEK Journal of Proceedings Series, (5), 22-27.

Pongoh, A. G., Fahreza, R. A., Kindi, B. Al, Pribadi, F. S., & Ajie, R. (2024). *Systematic Literature Review (SLR): Dampak Pemanfaatan Artificial Intelligence untuk Meningkatkan Cyber Security Systematic Literature Review (SLR): The Impact of Utilizing Artificial Intelligence to Enhance Cyber Security*. *7*(1), 34–41.

Purba, N., Yahya, M., & Nurbaiti, N. (2021). *Revolusi industri 4.0: Peran teknologi dalam eksistensi penguasaan bisnis dan implementasinya*. Jurnal perilaku dan strategi bisnis, 9(2), 91-98.

Rosanti, M., Saragih, Y., & Saragih, T. (2025). *Implementasi Sistem Keamanan Siber Berbasis Artificial Intelligence untuk Mengatasi Serangan Phishing*. Aisyah Journal Of Informatics and Electrical Engineering (AJIEE), 7(1), 94-98.

Santika, Y. Y., Rianto, R., & Ujianto, E. I. H. (2025). Studi Komprehensif Keamanan Siber: Perbandingan Teknologi AI dengan Sistem Non-AI dalam Deteksi dan Pencegahan Ancaman. Jurnal Komtika (Komputasi dan Informatika), 9(1), 45-64.

Setya Hadi, H. (2025). Internet Of Thing (IOT): Prinsip dan Implementasinya.

Taufik, R. (2025). *Systematic Literature Review: Teknik Deteksi Serangan Siber Berbasis AI dan Data Mining*. AT-TAKLIM: Jurnal Pendidikan Multidisiplin, 2(2), 158-169.

Vourganas, I. J., & Michala, A. L. (2024). *Applications of Machine Learning in Cyber Security: A Review*. Journal of Cybersecurity and Privacy, 4(4), 972–992. https://doi.org/10.3390/jcp4040045

Wiranda, N., Sadikin, F., & Saputra, W. A. *Pembelajaran Mesin untuk Sistem Keamanan-Literatur Review. IJEIS (Indonesian Journal of Electronics and Instrumentation Systems)*, 12(1), 37-46.

Yusep Ginanjar. (2022). *Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui*. *7*(2), 295–316.