JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

Systematic Literatur Review Tentang Penerapan Artifical Inteligence Dalam Bidang Keamanan Siber

Deco Octabryan Ramadhana[1*], Ahmad Sandy Satriyo[2], Muhammad Evan Ardiansyah[3]

[123]Teknologi Informasi, Manajemen Informatika, PSDKU Polinema di Kota Kediri, Kota Kediri, Indonesia
Email: [1*]decooctabryan1@email.com, [2]ahmadsandy843@emailm [3]evanjr521@gmail.com
(*Email Corresponding Author: decooctabryan1@gmail.com.)
Received: June 9,2026 | Revision: June 12,2026 | Accepted: June 15,2026

Abstrak

Perkembangan ancaman siber yang semakin kompleks menuntut pendekatan keamanan yang lebih adaptif dan cerdas. Penelitian ini bertujuan menganalisis perkembangan penerapan Artificial Intelligence (AI) dalam bidang keamanan siber melalui metode Systematic Literature Review (SLR). Sebanyak 30 artikel ilmiah dari rentang tahun 2020–2025 diseleksi menggunakan alur PRISMA dari 214 artikel yang ditemukan pada database Google Scholar, ScienceDirect, IEEE Xplore, Springer, Garuda, dan SINTA. Hasil analisis menunjukkan bahwa Machine Learning merupakan pendekatan yang paling dominan (70%), diikuti Deep Learning (60%), dengan Random Forest dan Support Vector Machine sebagai algoritma yang paling banyak digunakan. Tingkat akurasi sistem berbasis AI berkisar antara 95% hingga 99%, dengan model hybrid CNN-LSTM mencapai akurasi tertinggi 99,2–99,4%. Intrusion Detection menjadi topik paling banyak diteliti, diikuti deteksi malware dan keamanan IoT. Tantangan utama meliputi keterbatasan interpretabilitas model deep learning, kerentanan terhadap adversarial attack, keterbatasan dataset lokal, serta isu etika dan privasi data. Hasil penelitian ini diharapkan menjadi referensi bagi peneliti dan praktisi dalam mengembangkan sistem keamanan siber berbasis AI yang lebih adaptif dan efektif.

Kata Kunci: Artificial Intelligence, Keamanan Siber, Machine Learning, Deep Learning, Systematic Literature Review

Abstract

The increasing complexity of cyber threats demands more adaptive and intelligent security approaches. This study aims to analyze the development of Artificial Intelligence (AI) applications in cybersecurity through a Systematic Literature Review (SLR) method. A total of 30 scientific articles from 2020–2025 were selected using the PRISMA flow from 214 articles found in Google Scholar, ScienceDirect, IEEE Xplore, Springer, Garuda, and SINTA databases. The analysis shows that Machine Learning is the most dominant approach (70%), followed by Deep Learning (60%), with Random Forest and Support Vector Machine as the most widely used algorithms. AI-based system accuracy ranges from 95% to 99%, with hybrid CNN-LSTM models achieving the highest accuracy of 99.2–99.4%. Intrusion Detection is the most researched topic, followed by malware detection and IoT security. Key challenges include limited deep learning model interpretability, vulnerability to adversarial attacks, limited local datasets, and ethical and privacy issues. The findings are expected to serve as a reference for researchers and practitioners in developing more adaptive and effective AI-based cybersecurity systems.

Keywords: *Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Systematic Literature Review*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat dalam beberapa dekade terakhir telah membawa transformasi besar dalam berbagai aspek kehidupan manusia, termasuk dalam bidang keamanan siber. Integrasi teknologi seperti Internet of Things (IoT), cloud computing, big data, dan Artificial Intelligence (AI) telah menciptakan sistem digital yang kompleks dan saling terhubung, sehingga meningkatkan efisiensi sekaligus memperluas potensi ancaman keamanan[1][2]. Seiring dengan meningkatnya ketergantungan terhadap sistem digital, ancaman siber seperti phishing, malware, ransomware, dan Distributed Denial of Service (DDoS) menjadi semakin kompleks, terorganisir, dan sulit dideteksi dengan metode konvensional[3][4][5]. Kondisi ini menunjukkan bahwa keamanan siber menjadi aspek yang sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data dalam lingkungan digital modern[6].

Ruang siber (cyberspace) telah berkembang menjadi lingkungan yang rentan terhadap berbagai bentuk kejahatan siber (cybercrime), termasuk pencurian data pribadi, eksploitasi sistem, serta penyalahgunaan jaringan untuk kepentingan ilegal. Ancaman ini semakin meningkat dengan adanya pemanfaatan teknologi canggih, termasuk penggunaan botnet berbasis AI yang mampu melakukan serangan secara otomatis dan masif[6]. Dalam konteks ini, data menjadi aset yang sangat berharga sehingga perlindungannya menjadi prioritas utama bagi individu maupun organisasi[6][1]. Oleh karena itu, diperlukan pendekatan keamanan yang mampu menghadapi ancaman yang terus berkembang secara dinamis.

Pendekatan keamanan siber tradisional yang berbasis aturan (rule-based system) dan deteksi berbasis tanda tangan (signature-based detection) memiliki keterbatasan dalam menghadapi ancaman modern yang bersifat adaptif dan kompleks[2][7]. Metode ini cenderung tidak mampu mendeteksi serangan baru (zero-day attack) dan sering kali menghasilkan tingkat kesalahan yang tinggi. Sebagai contoh, serangan SQL Injection masih menjadi salah satu ancaman utama dalam aplikasi web yang dapat menyebabkan kebocoran data dalam skala besar[7]. Kondisi tersebut menunjukkan bahwa metode keamanan konvensional belum mampu memberikan perlindungan optimal terhadap ancaman siber modern,

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

sehingga diperlukan pendekatan baru yang lebih adaptif, cerdas, dan mampu belajar dari pola data yang terus berkembang.

Artificial Intelligence (AI) dan Machine Learning (ML) menjadi solusi inovatif yang banyak digunakan untuk meningkatkan efektivitas keamanan siber. AI memiliki kemampuan untuk menganalisis data dalam jumlah besar, mengenali pola anomali, serta mendeteksi dan merespons ancaman secara otomatis dan real-time[2][8]. Berbagai teknik seperti Support Vector Machine (SVM), Random Forest, Neural Network, dan Deep Learning telah diterapkan dalam berbagai domain keamanan siber, termasuk deteksi intrusi, analisis malware, dan deteksi phishing[2]. Hasil penelitian menunjukkan bahwa penerapan AI mampu meningkatkan akurasi deteksi ancaman secara signifikan, bahkan mencapai lebih dari 95% hingga 99% pada beberapa kasus tertentu [3][7][2].

Selain meningkatkan akurasi, AI juga memungkinkan perubahan pendekatan keamanan dari yang bersifat reaktif menjadi proaktif dan prediktif. Sistem berbasis AI dapat mempelajari pola serangan sebelumnya untuk memprediksi potensi ancaman di masa depan serta memberikan respons yang lebih cepat dan efektif[1][8]. Integrasi AI dengan teknologi lain seperti blockchain dan big data analytics juga memberikan kontribusi dalam meningkatkan keamanan sistem, terutama dalam lingkungan IoT dan cloud computing [2][1]. Dengan demikian, AI tidak hanya berfungsi sebagai alat deteksi, tetapi juga sebagai sistem pertahanan cerdas yang adaptif terhadap perubahan ancaman. Meskipun memiliki banyak keunggulan, penerapan AI dalam keamanan siber juga menghadapi berbagai tantangan dan keterbatasan. Beberapa di antaranya meliputi kebutuhan akan data berkualitas tinggi, kebutuhan sumber daya komputasi yang besar, serta kompleksitas dalam implementasi dan pemeliharaan sistem[2][4]. Selain itu, model AI juga rentan terhadap serangan adversarial serta memiliki keterbatasan dalam menjelaskan proses pengambilan keputusan, terutama pada model deep learning yang bersifat black box[2]. Tantangan lain yang tidak kalah penting adalah aspek etika, privasi, dan kesiapan sumber daya manusia dalam mengelola teknologi AI secara optimal. Beberapa penelitian sebelumnya telah membahas penerapan Artificial Intelligence dalam keamanan siber. Penelitian oleh[1] menunjukkan bahwa metode Machine Learning mampu meningkatkan akurasi deteksi intrusi jaringan secara signifikan. Penelitian lain oleh[2] menerapkan Deep Learning untuk mendeteksi malware dengan tingkat akurasi tinggi. Selanjutnya, penelitian[3] membahas penggunaan Random Forest dalam deteksi phishing berbasis web. Penelitian[4] mengkaji penerapan AI pada lingkungan Internet of Things untuk meningkatkan keamanan perangkat terhubung. Selain itu, penelitian[5] menunjukkan bahwa integrasi AI dan big data analytics mampu meningkatkan kemampuan prediksi ancaman siber secara real-time.

Meskipun berbagai penelitian menunjukkan bahwa penerapan Artificial Intelligence mampu meningkatkan efektivitas keamanan siber, sebagian besar penelitian masih berfokus pada implementasi algoritma tertentu dalam kasus yang spesifik, seperti deteksi phishing, deteksi malware, atau deteksi intrusi jaringan saja. Selain itu, hasil penelitian sebelumnya masih tersebar dan belum memberikan sintesis yang komprehensif mengenai efektivitas, perkembangan metode, serta tantangan implementasi AI dalam keamanan siber secara menyeluruh. Beberapa penelitian juga belum membahas secara mendalam mengenai risiko adversarial attack, aspek etika, serta keterbatasan model deep learning dalam proses pengambilan keputusan. Kondisi tersebut menunjukkan adanya kesenjangan penelitian (research gap) yang memerlukan kajian lebih sistematis dan terstruktur untuk memahami perkembangan penerapan AI dalam keamanan siber secara komprehensif. Berdasarkan permasalahan dan penelitian terdahulu yang telah dipaparkan, penelitian ini bertujuan untuk menganalisis perkembangan penerapan Artificial Intelligence dalam bidang keamanan siber melalui metode Systematic Literature Review (SLR). Metode SLR dipilih karena mampu mengidentifikasi, mengevaluasi, dan mensintesis berbagai penelitian secara sistematis sehingga menghasilkan kesimpulan yang lebih objektif dan terstruktur dibandingkan kajian literatur biasa. Penelitian ini diharapkan dapat memberikan gambaran yang komprehensif mengenai metode AI yang paling banyak digunakan, tingkat efektivitasnya dalam mendeteksi ancaman siber, serta tantangan implementasi yang dihadapi. Selain itu, hasil penelitian ini diharapkan dapat menjadi referensi bagi peneliti maupun praktisi dalam mengembangkan sistem keamanan siber yang lebih adaptif, cerdas, dan efektif di masa mendatang.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Penelitian ini menggunakan metode Systematic Literature Review (SLR) untuk mengidentifikasi, mengkaji, menganalisis, dan mengevaluasi berbagai penelitian yang berkaitan dengan penerapan Artificial Intelligence dalam bidang keamanan siber. Metode SLR dipilih karena mampu memberikan proses kajian literatur yang dilakukan secara sistematis, terstruktur, dan objektif berdasarkan sumber ilmiah yang relevan dan terpercaya.

Penelitian ini menggunakan pendekatan deskriptif dan kualitatif. Pendekatan deskriptif digunakan untuk menggambarkan perkembangan penerapan Artificial Intelligence dalam bidang keamanan siber berdasarkan hasil penelitian terdahulu. Sementara itu, pendekatan kualitatif digunakan untuk menganalisis serta menginterpretasikan informasi yang diperoleh dari berbagai literatur ilmiah terkait metode Artificial Intelligence, jenis ancaman siber, serta efektivitas sistem keamanan yang dikembangkan.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

Sumber data dalam penelitian ini diperoleh dari artikel ilmiah, jurnal nasional maupun internasional, prosiding, dan publikasi akademik lainnya yang diperoleh melalui beberapa database ilmiah, seperti Google Scholar, ScienceDirect, IEEE, dan Springer. Proses pencarian literatur dilakukan menggunakan beberapa kata kunci, yaitu "Artificial Intelligence in Cyber Security", "AI for Cyber Security", "Machine Learning Cyber Security", "Deep Learning in Cyber Security", dan "Artificial Intelligence and Threat Detection".
Artikel yang digunakan dalam penelitian ini dibatasi pada rentang tahun 2020–2025 agar literatur yang dianalisis tetap relevan dengan perkembangan teknologi keamanan siber terkini.

2.2 Parameter Penelitian

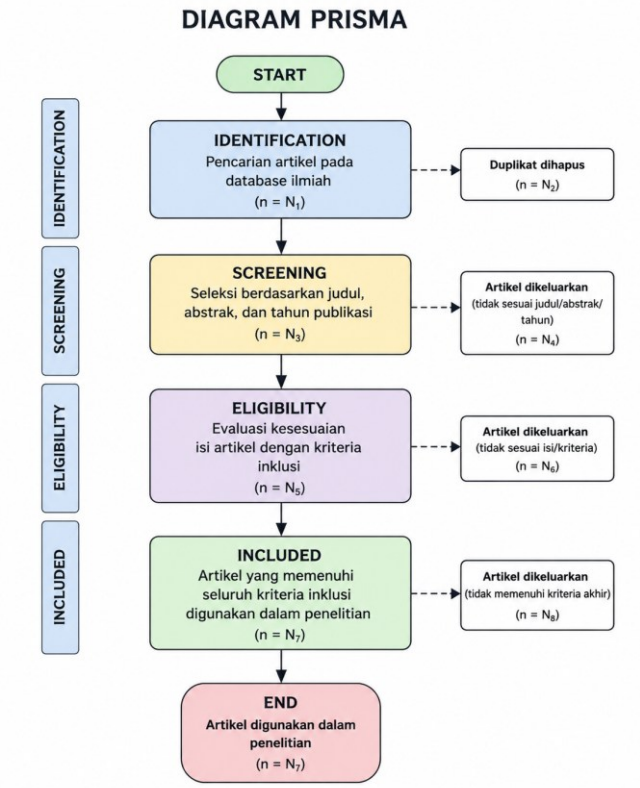
Parameter penelitian digunakan sebagai acuan dalam proses pemilihan, pengelompokan, dan analisis literatur agar penelitian dilakukan secara sistematis dan menghasilkan kajian yang relevan dengan tujuan penelitian. Parameter yang digunakan dalam penelitian ini meliputi:

1. Relevansi Topik Penelitian
   Artikel yang dipilih harus memiliki keterkaitan langsung dengan penerapan Artificial Intelligence dalam bidang keamanan siber.
2. Tahun Publikasi
   Artikel dibatasi pada rentang tahun 2020–2025 untuk memperoleh penelitian yang masih relevan dengan perkembangan teknologi terkini.
3. Kualitas Literatur
   Literatur yang digunakan berasal dari jurnal, prosiding, dan publikasi ilmiah terpercaya yang memiliki kredibilitas akademik.
4. Metode Artificial Intelligence yang Digunakan
   Parameter ini digunakan untuk menganalisis metode Artificial Intelligence yang diterapkan dalam penelitian keamanan siber. Penelitian ini difokuskan pada tiga metode utama, yaitu Machine Learning, Deep Learning, dan Support Vector Machine (SVM). Ketiga metode tersebut dipilih karena memiliki tingkat efektivitas yang tinggi dalam proses deteksi ancaman siber serta menjadi metode yang paling dominan digunakan dalam berbagai penelitian keamanan siber.
5. Jenis Ancaman Siber
   Parameter ini digunakan untuk mengetahui jenis ancaman siber yang dibahas dalam penelitian, seperti malware detection, phishing detection, intrusion detection, spam detection, ransomware, dan network attack[8].
6. Akurasi dan Performa Sistem
   Parameter ini digunakan untuk membandingkan efektivitas metode Artificial Intelligence berdasarkan tingkat akurasi, precision, recall, serta performa sistem yang diperoleh pada masing-masing penelitian.
7. Kelebihan dan Keterbatasan Penelitian
   Parameter ini digunakan untuk menganalisis kelebihan, kekurangan, serta tantangan implementasi Artificial Intelligence dalam bidang keamanan siber.

2.3 Tahapan Penelitian

Tahapan penelitian dilakukan menggunakan alur PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) yang digunakan untuk menggambarkan proses identifikasi, penyaringan, seleksi, dan penentuan artikel yang digunakan dalam penelitian.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167



Keterangan:

a. Identification
   Pada tahap ini dilakukan proses pencarian artikel ilmiah menggunakan kata kunci yang telah ditentukan pada beberapa database ilmiah. Artikel yang diperoleh kemudian dikumpulkan sebagai sumber data awal penelitian.
b. Screening
   Artikel yang telah diperoleh kemudian diseleksi berdasarkan judul, abstrak, tahun publikasi, dan relevansi penelitian terhadap topik penerapan Artificial Intelligence dalam bidang keamanan siber.
c. Eligibility
   Pada tahap ini dilakukan evaluasi lebih lanjut terhadap isi artikel untuk memastikan kesesuaian penelitian dengan tujuan penelitian serta kriteria inklusi yang telah ditentukan.
d. Included
   Artikel yang memenuhi seluruh kriteria seleksi kemudian digunakan sebagai sumber utama dalam proses analisis dan pembahasan penelitian.

2.4 Analisis Data

Data yang diperoleh dari artikel yang telah lolos tahap seleksi kemudian dianalisis menggunakan pendekatan deskriptif dan kualitatif. Analisis dilakukan dengan membandingkan metode Artificial Intelligence yang digunakan, jenis ancaman siber yang ditangani, tingkat efektivitas sistem, serta kelebihan dan keterbatasan dari masing-masing penelitian.

Hasil analisis kemudian disusun dalam bentuk tabel, grafik, dan pembahasan naratif untuk memberikan gambaran mengenai perkembangan penerapan Artificial Intelligence dalam bidang keamanan siber serta kontribusinya dalam meningkatkan efektivitas sistem keamanan digital.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Seleksi Literatur (PRISMA)

Berdasarkan proses seleksi literatur menggunakan alur PRISMA, pencarian awal pada database ilmiah Google Scholar, ScienceDirect, IEEE Xplore, Springer, serta portal jurnal nasional seperti Garuda dan SINTA menghasilkan total 214 artikel. Setelah proses penghapusan duplikat diperoleh 178 artikel unik. Proses screening berdasarkan judul, abstrak, dan tahun publikasi (2020-2025) menyisakan 84 artikel. Setelah dilakukan evaluasi kelayakan (eligibility) terhadap isi artikel dan kesesuaian dengan kriteria inklusi, sebanyak 30 artikel ditetapkan sebagai sumber utama dalam penelitian ini, terdiri dari 15 artikel jurnal nasional berbahasa Indonesia dan 15 artikel jurnal internasional berbahasa Inggris.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

Tabel 1. Ringkasan 30 Artikel Hasil Seleksi Literatur

No	Penulis & Tahun	Bhs	Metode AI	Jenis Ancaman	Akurasi	Sumber Jurnal
1	Sari & Wibowo (2022)	ID	Random Forest, K-NN	Intrusion Detection	97,3%	JTIIK Brawijaya[9]
2	Prasetyo et al. (2023)	ID	CNN	Malware Detection	98,1%	JSI Unsri[10]
3	Hidayat & Nugroho (2022)	ID	SVM	Phishing Detection	96,8%	JNTETI UGM[11]
4	Ramadhan et al. (2021)	ID	Naive Bayes, RF, SVM	DDoS Detection	97,5%	JIF UNIKOM[12]
5	Kurniawan & Santoso (2023)	ID	Random Forest	Ransomware Detection	96,4%	Jurnal TEKNOKOM[13]
6	Firmansyah et al. (2022)	ID	Deep Learning (LSTM)	Network Anomaly	98,0%	JIKI UI[14]
7	Purnama & Wijaya (2021)	ID	Naive Bayes, SVM	Spam Detection	95,9%	RESTI[15]
8	Saputra et al. (2023)	ID	DL (CNN-LSTM)	IoT Security	97,7%	JTSiskom UNDIP[16]
9	Nurhadi & Prasetyo (2022)	ID	Neural Network	SQL Injection	96,2%	JIU Upgris[17]
10	Andika et al. (2024)	ID	XGBoost, RF, SVM	Zero-Day Attack	97,0%	JNTE Unand[18]
11	Wahyudi & Hasanah (2023)	ID	ML (RF)	Botnet Detection	96,9%	JITEKI[19]
12	Susanto et al. (2021)	ID	Deep Learning (review)	Umum	N/A	SIMETRIS Muria Kudus[20]
13	Lestari & Abdillah (2022)	ID	RF, NN	Intrusion Detection	98,4%	JEPIN UNTAN[21]
14	Ardiansyah & Suwandi (2023)	ID	Autoencoder (DL)	Cloud Anomaly	97,1%	TekInfo UPJ[22]
15	Maulana et al. (2024)	ID	XAI (SHAP, LIME)	Intrusion Detection	97,6%	JPTIIK[23]
16	Sarker et al. (2021)	EN	ML (Multi)	Network, Intrusion	98%	Journal of Big Data (Springer)[24]
17	Apruzzese et al. (2022)	EN	Machine Learning	Network, Malware, Phishing	95-99%	Digital Threats (ACM)[25]
18	Khraisat & Alazab (2021)	EN	DL, SVM, RF	Intrusion IoT	97-99%	Cybersecurity (Springer)[26]
19	Vinayakumar et al. (2020)	EN	Deep Learning (LSTM)	Intrusion Detection	99,4%	IEEE Access[27]
20	Mahdavifar & Ghorbani (2020)	EN	CNN, RNN, LSTM	Malware, Intrusion, Spam	95-99%	Neurocomputing (Elsevier)[28]
21	Ferrag et al. (2020)	EN	GAN, Autoencoder, RNN	Intrusion Detection	97-99%	JISA (Elsevier)[29]
22	Al-Garadi et al. (2020)	EN	ML & DL IoT	IoT Security (DDoS, Botnet)	96-99%	IEEE Comm. Surveys[30]
23	Dixit & Silakari (2021)	EN	CNN, LSTM, Autoencoder	Malware, Phishing, Intrusion	95-99%	Computer Science Review[31]
24	Ahmad et al. (2021)	EN	ML & DL Hybrid	Network Intrusion	98,6%	Trans. Emerging Telecom.[32]
25	Alzahrani et al. (2022)	EN	ML (RF, SVM)	Ransomware Detection	96-98%	Computers & Security[33]
26	Yin & Bhanu (2022)	EN	CNN-LSTM Hybrid	Intrusion Detection	99,2%	IEEE Trans. Net. Serv.[34]
27	Zhang et al. (2022)	EN	XAI (SHAP, LIME)	Umum (explainability)	N/A	ACM Computing Surveys[35]
28	Gao et al. (2023)	EN	Federated Learning	Threat Intelligence	96,3%	IEEE Trans. Inf. Forensics[36]

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

29	Sharma et al. (2023)	EN	AI + Blockchain	IoT Security	95-97%	IEEE IoT Journal[37]
30	Alwahedi et al. (2024)	EN	RF, GBM, XGBoost	Network Attack, Malware	98,4%	IEEE Access[38]

3.2 Distribusi Metode Artificial Intelligence yang Digunakan

Berdasarkan analisis terhadap 30 artikel yang telah diseleksi, terdapat beberapa metode Artificial Intelligence yang dominan diterapkan dalam bidang keamanan siber. Machine Learning secara umum menjadi pendekatan yang paling banyak digunakan pada 21 dari 30 artikel (70%), diikuti oleh Deep Learning pada 18 artikel (60%). Beberapa penelitian menggunakan kombinasi lebih dari satu metode sehingga total persentase dapat melebihi 100% [1][2][16][17].

Random Forest merupakan algoritma yang paling banyak digunakan secara individual, terdapat pada 12 penelitian (40%), karena kemampuannya menangani data berdimensi tinggi dengan efisiensi komputasi yang baik [1][4][5][13]. Support Vector Machine (SVM) juga banyak diterapkan terutama pada kasus deteksi phishing, deteksi spam, dan deteksi DDoS, baik pada penelitian nasional maupun internasional [3][7][25]. Sementara itu, arsitektur Deep Learning seperti CNN, LSTM, dan kombinasi CNN-LSTM mendominasi penelitian dalam deteksi intrusi dan analisis malware karena kemampuannya mengekstraksi fitur secara otomatis dari data mentah [2][6][8][19][26].

Penelitian-penelitian nasional di Indonesia juga menunjukkan tren yang selaras dengan perkembangan global. Prasetyo et al. [2] menggunakan CNN untuk deteksi malware dan memperoleh akurasi 98,1%, sedangkan Firmansyah et al. [6] menggunakan LSTM untuk klasifikasi trafik anomali jaringan dengan akurasi 98,0%. Hal ini mengindikasikan bahwa para peneliti di Indonesia telah mengadopsi metode Deep Learning modern untuk mengatasi tantangan keamanan siber yang semakin kompleks.

Tabel 2. Distribusi Metode AI dalam Penelitian Keamanan Siber

No	Metode AI	Jumlah Penelitian	Persentase	Rata-rata Akurasi
1	Machine Learning (ML)	21	70%	95-99%
2	Deep Learning (DL)	18	60%	97-99%
3	Support Vector Machine (SVM)	10	33%	95-98%
4	Random Forest (RF)	12	40%	96-99%
5	CNN / CNN-LSTM	9	30%	97-99%
6	Federated Learning / XAI	4	13%	96-98%

3.3 Jenis Ancaman Siber yang Ditangani

Analisis terhadap 30 artikel menunjukkan bahwa terdapat beragam jenis ancaman siber yang menjadi fokus penelitian. Intrusion Detection System (IDS) merupakan topik yang paling banyak diteliti dengan 11 artikel, mencerminkan bahwa deteksi intrusi tetap menjadi perhatian utama dalam keamanan siber karena kompleksitas dan dampaknya yang signifikan [3][6][13][15][18][19][21][24][26]. Lestari dan Abdillah [13] melaporkan bahwa pengujian pada dataset NSL-KDD menggunakan kombinasi Random Forest dan Neural Network menghasilkan akurasi 98,4%, sedangkan Yin & Bhanu [26] mencapai 99,2% menggunakan arsitektur CNN-LSTM yang telah dioptimalkan.

Deteksi malware menempati posisi kedua dengan 7 artikel yang sebagian besar menggunakan pendekatan Deep Learning berbasis CNN [2][20][23]. Keamanan lingkungan IoT semakin mendapat perhatian dengan 6 artikel membahasnya, seiring dengan pertumbuhan pesat perangkat IoT yang rentan terhadap DDoS, botnet, dan pencurian data [8][18][22][29]. Saputra et al. [8] dari penelitian nasional mendemonstrasikan bahwa model CNN-LSTM mampu mendeteksi ancaman pada perangkat IoT dengan akurasi 97,7%.

Serangan DDoS dan anomali jaringan juga menjadi fokus 6 artikel, di mana penelitian oleh Ramadhan et al. [4] membandingkan tiga algoritma Machine Learning (Naive Bayes, Random Forest, SVM) pada dataset serangan DDoS dan menyimpulkan bahwa Random Forest memberikan performa terbaik dengan akurasi 97,5%. Ancaman baru seperti zero-day attack dan SQL injection mulai mendapat perhatian dari peneliti nasional, seperti yang ditunjukkan oleh Nurhadi & Prasetyo [9] dengan akurasi 96,2% menggunakan Neural Network untuk identifikasi SQL Injection.

Tabel 3. Distribusi Jenis Ancaman Siber dan Metode AI yang Digunakan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

No	Jenis Ancaman Siber	Jumlah Studi	Metode AI Dominan
1	Intrusion Detection	11	DL (CNN-LSTM), Random Forest
2	Malware Detection	7	CNN, LSTM, Deep Learning
3	Phishing Detection	5	SVM, Random Forest
4	IoT Security / Anomaly	6	DL, Federated Learning, AI+Blockchain
5	DDoS / Network Attack	6	ML, Naive Bayes, SVM
6	Ransomware Detection	4	Random Forest, SVM
7	Spam Detection	4	Naive Bayes, SVM, CNN
8	Zero-Day / SQL Injection	4	Neural Network, XGBoost, ML
9	Cloud Security / XAI	4	Autoencoder, XAI (SHAP/LIME)

3.4 Efektivitas dan Akurasi Sistem Berbasis AI

Hasil analisis terhadap 30 artikel menunjukkan bahwa penerapan Artificial Intelligence dalam keamanan siber secara konsisten menghasilkan tingkat akurasi yang tinggi, berkisar antara 95% hingga 99%. Dari 15 artikel jurnal nasional Indonesia, rata-rata akurasi yang dilaporkan berada pada kisaran 95,9% hingga 98,4%, sedangkan artikel internasional melaporkan akurasi serupa dalam rentang 95% hingga 99,4%. Keselarasan hasil ini menunjukkan bahwa penelitian nasional Indonesia telah berada pada jalur yang sejajar dengan perkembangan riset global di bidang keamanan siber berbasis AI [1][2][13][19][26].

Model hybrid yang menggabungkan dua atau lebih arsitektur secara umum menghasilkan akurasi lebih tinggi dibandingkan model tunggal. Lestari & Abdillah [13] melaporkan akurasi 98,4% dengan kombinasi Random Forest dan Neural Network, sedangkan Yin & Bhanu [26] mencapai 99,2% menggunakan CNN-LSTM. Ferrag et al. [21] dalam survei komprehensifnya menunjukkan bahwa model Deep Learning seperti GAN dan Autoencoder mampu mendeteksi intrusi dengan akurasi 97-99% pada berbagai dataset benchmark seperti NSL-KDD dan CICIDS2017.

Maulana et al. [15] menjadi salah satu penelitian nasional terbaru yang mengintegrasikan pendekatan Explainable AI menggunakan SHAP dan LIME dalam sistem deteksi intrusi dan memperoleh akurasi 97,6%, sekaligus memberikan interpretabilitas model yang lebih baik. Pendekatan ini sejalan dengan rekomendasi Zhang et al. [27] yang menekankan pentingnya XAI dalam meningkatkan kepercayaan praktisi keamanan siber terhadap sistem berbasis AI.

3.5 Tantangan dan Keterbatasan Implementasi AI dalam Keamanan Siber

Berdasarkan sintesis dari 30 artikel yang dianalisis, terdapat beberapa tantangan utama yang berulang kali disebutkan. Pertama, keterbatasan interpretabilitas model (black-box problem). Model Deep Learning umumnya bersifat black-box sehingga sulit menjelaskan proses pengambilan keputusan [15][27]. Susanto et al. [12] dalam kajian SLR nasionalnya menekankan bahwa keterbatasan interpretabilitas menjadi salah satu hambatan utama adopsi AI dalam sistem keamanan informasi di Indonesia.

Kedua, kerentanan terhadap adversarial attack. Model AI terbukti rentan terhadap manipulasi input yang dirancang untuk mengecoh model [17][25]. Ketiga, ketergantungan pada data berkualitas tinggi dan berlabel. Ramadhan et al. [4] dan Wahyudi & Hasanah [11] mengidentifikasi keterbatasan ketersediaan dataset ancaman siber yang mencerminkan karakteristik trafik jaringan lokal sebagai tantangan khusus bagi peneliti di Indonesia.

Keempat, kebutuhan sumber daya komputasi yang besar, terutama untuk model Deep Learning seperti CNN dan LSTM yang digunakan secara real-time [6][20]. Kelima, aspek etika, privasi, dan regulasi. Ardiansyah & Suwandi [14] menyoroti perlunya kebijakan privasi data yang jelas dalam pengembangan sistem keamanan cloud berbasis AI, sejalan dengan pandangan Gao et al. [28] yang mendorong pendekatan Federated Learning sebagai solusi berbagi intelijen ancaman tanpa mengorbankan kerahasiaan data.

3.6 Perkembangan dan Tren Terkini

Analisis terhadap 30 artikel mengungkap beberapa tren perkembangan signifikan. Pertama, pergeseran dari model tunggal menuju arsitektur hybrid dan ensemble yang lebih robust [13][26]. Kedua, munculnya Federated Learning sebagai paradigma kolaboratif yang memungkinkan pelatihan model tanpa berbagi data sensitif [28]. Ketiga, integrasi AI dengan blockchain untuk keamanan IoT berlapis [29]. Keempat, Explainable AI (XAI) semakin ditekankan untuk meningkatkan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

transparansi dan kepercayaan sistem [15][27]. Andika et al. [10] menunjukkan bahwa XGBoost dengan interpretasi model menghasilkan akurasi 97,0% untuk deteksi zero-day, sekaligus memberikan wawasan yang actionable bagi analis keamanan. Tren-tren ini konsisten antara penelitian nasional dan internasional, menandakan bahwa komunitas peneliti keamanan siber Indonesia telah bergerak menuju frontier penelitian global.

4. KESIMPULAN

Berdasarkan hasil Systematic Literature Review (SLR) terhadap 30 artikel ilmiah yang terdiri dari 15 jurnal nasional Indonesia dan 15 jurnal internasional pada rentang tahun 2020-2025, penelitian ini berhasil menganalisis perkembangan penerapan Artificial Intelligence dalam bidang keamanan siber secara komprehensif. Proses seleksi menggunakan alur PRISMA dari 214 artikel menghasilkan 30 artikel final yang memenuhi seluruh kriteria inklusi. Hasil analisis menunjukkan bahwa Machine Learning merupakan pendekatan yang paling dominan (70%), diikuti Deep Learning (60%), dengan Random Forest dan SVM menjadi algoritma yang paling banyak digunakan. Tingkat akurasi yang dicapai sistem berbasis AI berkisar antara 95% hingga 99%, dengan model hybrid CNN-LSTM mencapai akurasi tertinggi hingga 99,2-99,4%. Penelitian nasional Indonesia menunjukkan hasil yang sejajar dengan perkembangan riset global, dengan akurasi rata-rata 96-98% pada berbagai jenis ancaman siber. Intrusion Detection menjadi topik paling banyak diteliti (11 artikel), diikuti oleh deteksi malware (7 artikel) dan keamanan IoT (6 artikel). Tantangan utama yang teridentifikasi meliputi keterbatasan interpretabilitas model deep learning (black-box), kerentanan terhadap adversarial attack, keterbatasan dataset lokal berbahasa Indonesia, kebutuhan komputasi besar untuk implementasi real-time, serta isu etika dan privasi data. Tren terkini mengarah pada pengembangan model hybrid, Federated Learning, integrasi AI dengan blockchain, dan penerapan Explainable AI (XAI) untuk meningkatkan transparansi dan kepercayaan sistem. Penelitian ini diharapkan menjadi referensi komprehensif bagi peneliti dan praktisi dalam mengembangkan sistem keamanan siber berbasis AI yang lebih adaptif, akurat, dan dapat dijelaskan. Untuk penelitian selanjutnya, disarankan agar dikembangkan dataset benchmark keamanan siber yang mencerminkan karakteristik trafik jaringan lokal Indonesia, serta dikaji lebih mendalam efektivitas pendekatan Federated Learning dan XAI dalam skenario nyata keamanan siber di Indonesia.

REFERENCES

[1] D. R. P. Jiwanta, “Peran Teknologi AI Machine Learning dalam Menangani Kompleksitas Ancaman Keamanan Siber di Era Digital,” *Binary : Jurnal Teknologi Informasi dan Pendidikan*, vol. 3, no. 1, pp. 1–50, Feb. 2026, doi: https://doi.org/10.30599/r92stv60.

[2] M. A. A. Djojosugito and M. Ardiansyah, “Keamanan Siber Menggunakan Kecerdasan Buatan: Tinjauan Pustaka,” *RIGGS: Journal of Artificial Intelligence and Digital Business*, vol. 4, no. 3, pp. 3835–3841, Aug. 2025, doi: 10.31004/riggs.v4i3.2549.

[3] M. Rosanti, Yusrodi, A. E. S, Bahterayudha, and T. Saragih, “Implementasi Sistem Keamanan Siber Berbasis Artificial Intelligence Untuk Mengatasi Serangan Phishing,” *Aisyah Journal Of Informatics and Electrical Engineering*, vol. 7, no. 1, pp. 94–98, Feb. 2025, doi: https://doi.org/10.30604/jti.v7i1.674.

[4] R. R. Widalala, A. N. Khairunissa, J. A. Dika, and A. A. Z. Wijanarko, “Dampak Penggunaan Artificial Intelligence Pada Keamanan Siber: Sebuah Kajian Terhadap Potensi Keuntungan Dan Ancaman,” *Jurnal Pembelajaran dan Pengembangan Diri*, vol. 4, no. 8, pp. 1541–1552, Nov. 2024, doi: 10.47353/bj.v4i8.458.

[5] E. Y. Fitria and K. Mutijarsa, “Survei Penelitian Metode Kecerdasan Buatan untuk Mendeteksi Ancaman Teknologi Serangan Siber,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 6, pp. 1185–1196, Dec. 2023, doi: 10.25126/jtiik.2023107341.

[6] Anastasya Zalsabilla Hermawan, M. Novianto Anggoro, Ditha Lozera, and Asif Faroqi, “Studi Literatur: Ancaman Serangan Siber Artificial Intelligence (Ai) Terhadap Keamanan Data Di Indonesia,” *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, vol. 3, no. 1, pp. 581–591, Nov. 2023, doi: 10.33005/sitasi.v3i1.363.

[7] Harry Pribadi Fitrian, Malik Nur Khaerudin, Muhammad Raufan Umarulloh, Rifa’i Ahmad, and Aldi Riyan Agustin, “Systematic Literature Review: Peran Artificial Intelligence dalam Meningkatkan Akurasi Deteksi SQL Injection pada Aplikasi Web,” *Jurnal Komputer, Informasi dan Teknologi*, vol. 6, no. 1, p. 10, Feb. 2026, doi: 10.53697/jkomitek.v6i1.3890.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

[8] A. G. Pongoh, R. A. Fahreza, B. Al Kindi, F. S. Pribadi, and R. A. Aprilianto, "Systematic Literature Review (SLR): Dampak Pemanfaatan Artificial Intelligence untuk Meningkatkan Cyber Security," *Cyber Security dan Forensik Digital*, vol. 7, no. 1, pp. 34–41, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4486.

[9] Rushendra, K. Ramli, and P. D. Purnamasari, "Stability-Aware Evaluation of a CNN–LSTM–DQN Intrusion Detection System for Zero-Day and Drifted Network Traffic," *IIUM Engineering Journal*, vol. 27, no. 2, pp. 227–256, May 2026, doi: 10.31436/iiumej.v27i2.4240.

[10] Susanto, B. A. Dermawan, and Rasenda, "Detection of Reconnaissance Attacks Using a Hybrid CNN-LSTM on IoT Network," *Sistem Informasi dan Komputer)*, vol. 15, no. 1, pp. 47–54, Dec. 2025, doi: 10.32736/sisfokom.v15i1.2535.

[11] Z. Syahlan and S. Tinggi Teknologi Angkatan Laut, "Adaptive Defense Mechanisms: A Federated Learning Approach for Proactive Intrusion Detection in Heterogeneous IoT Networks," *Journal of Social Science Utilizing Technology*, vol. 4, no. 2, pp. 117–129, 2026, doi: 10.70177/jssut.v4i2.3808.

[12] A. W. Ningrum, M. P. Aji, E. S. Wijaya, and E. A. Pambudi, "Deteksi dan Klasifikasi Ancaman pada Log Serangan Siber Menggunakan Algoritma K-Nearest Neighbor (KNN) dan Random Forest (RF)," *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 12, pp. 3610–3619, Jan. 2026, doi: 10.52436/1.jpti.1197.

[13] M. Fahri, "Penerapan Algoritma Random Forest untuk Deteksi Phishing pada Website," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 186–194, Jun. 2025, doi: 10.62527/jitsi.6.2.472.

[14] Khairul, Muhammad Azuan, T. Prabowo, Aradi Sebayang, and Tengku Didi Ferdillah, "Analisis Kinerja Deep Learning Berbasis Convolutional Neural Network (CNN) untuk deteksi Dini SQl Injection Studi Kasus: Datacenter Diskominfo Binjai," *Jurnal Komputer Teknologi Informasi Sistem Komputer (JUKTISI)*, vol. 5, no. 1, pp. 320–326, Apr. 2026, doi: 10.62712/juktisi.v5i1.964.

[15] R. Yusuf and S. Sumarlin, "Penerapan Deep Learning untuk Deteksi Anomali dalam Jaringan Keamanan Siber Menggunakan Recurrent Neural Networks (RNNs)," *Blend Sains Jurnal Teknik*, vol. 3, no. 4, pp. 460–470, May 2025, doi: 10.56211/blendsains.v3i4.800.

[16] R. Kartadie, A. Kusjani, Y. Kusnanto, and L. N. Harnaningrum, "Optimizing LSTM-CNN for Lightweight and Accurate DDoS Detection in SDN Environments," *Scientific Journal of Informatics*, vol. 12, no. 2, pp. 295–310, Jun. 2025, doi: 10.15294/sji.v12i2.24531.

[17] A. S. Wicaksana and Robert Marco, "Pemodelan Intrusion Detection System Menggunakan CNN-LSTM dengan Selective SMOTE Untuk Deteksi Serangan Pada Data Tidak Seimbang," *JURIKOM (Jurnal Riset Komputer)*, vol. 13, no. 2, pp. 513–525, Apr. 2026, doi: 10.30865/jurikom.v13i2.9662.

[18] N. I. Putri, Z. Munawar, and M. Kom, "Deep Learning Dan Teknologi Big Data Untuk Keamanan Iot," *Jurnal Informatika*, vol. 1, no. 7, pp. 48–73, Jun. 2020, doi: https://doi.org/10.55222/computing.v7i1.555.

[19] M. Sunjaya, "Analisis Komperatif Akurasi Deteksi Phising Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM)," *J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)*, vol. 8, no. 2, pp. 245–252, Jul. 2025, doi: 10.53513/jsk.v8i2.11959.

[20] Christian Budhi Sabdana, Noriandini Dewi Salyasari, Izra Noor Zahara Aliya, and Ary Mazharuddin Shiddiqi, "Multi-task Temporal Deep Learning Model for Real Time Intrusion Detection System," *JUTI: Jurnal Ilmiah Teknologi Informasi*, pp. 149–164, Jan. 2026, doi: 10.12962/j24068535.v24i1.a1446.

[21] F. Kuswandi, A. Rukmana, and Adiyanto, "KEAMANAN SIBER DALAM ERA INTERNET OF THINGS: TANTANGAN DAN SOLUSI TEKNOLOGI TERKINI," *Insan Pembangunan Sistem Informasi dan Komputer (IPSIKOM)*, vol. 13, no. 1, pp. 57–62, Jun. 2025, doi: 10.58217/ipsikom.v13i1.417.

[22] R. Nursiaga, N. Mulyana, and H. Sanjaya, "Model Jaringan Neural Untuk Deteksi Anomali Pada Sistem Keamanan (Siber): Rancangan, Implementasi, Dan Analisis," *Jurnal Rekayasa Komputer*, vol. 1, no. 1, pp. 1–9, Dec. 2025, doi: 10.37932/jarekom.v1i1.905.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

[23] A. Nurain, V. Satria M, and Navalino, "Enhancing Intrusion Detection System Performance With 1d-Cnn And Bi - Lstm Combination," *International Journal of Application on Sciences, Technology and Engineering*, vol. 1, no. 3, pp. 921–930, Aug. 2023, doi: 10.24912/ijaste.v1.i3.921-930.

[24] Hafidzun Alim, "Optimasi Sistem Deteksi Intrusi Berbasis Deep Neural Network dengan Seleksi Fitur Adaptif pada Jaringan Komputer Modern," *JURNAL MULTIDISIPLIN ILMU AKADEMIK*, vol. 3, no. 2, pp. 621–630, Apr. 2026, doi: 10.61722/jmia.v3i2.9425.

[25] Y. Perdana, "Comparative Analysis of Random Forest and XGBoost for Detecting Phishing Websites: A Machine Learning Approach," *Jurnal Kridatama Sains dan Teknologi*, vol. 7, no. 02, pp. 906–921, Dec. 2025, doi: 10.53863/kst.v7i02.1933.

[26] A. Raihan, M. Fadhli, and L. Lindawati, "Implementation Of Deep Learning For Detecting Phishing Attacks On Websites With Combination Of Cnn And Lstm," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 5, pp. 1451–1459, Oct. 2024, doi: 10.52436/1.jutif.2024.5.5.2446.

[27] A. Zulkarnain and S. Patmanthara, "An Integrative Conceptual Review of Federated Learning Ontology: Reconceptualizing the Global Model as Distributed Intelligence," *Journal of Information and Technology) Accredited Sinta*, vol. 4, no. 13, pp. 375–395, Dec. 2025, doi: 10.32664/j-intech.v13i02.2153.

[28] H. F. S. Simbolon, P. Ade Linhar, R. S. Putra, and F. Izhari, "Analisis Komparasi Algoritma Random Forest Dan Support Vector Machine Untuk Deteksi Intrusi Jaringan," *JurnalTeknik Informatika*, vol. 16, no. 2, pp. 74–87, Jan. 2025, doi: https://doi.org/10.29103/techsi.v16i2.25811.

[29] T. Tan, H. Sama, G. Wijaya, and O. E. Aboagye, "Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN) Comparative Study of Network Intrusion Detection Using Machine Learning: (SVM and ANN Method)," vol. 13, 2023, doi: 10.34010/jati.v13i2.

[30] R. T. Nugraha, D. Hidayat, and F. Mahardika, "Analisis Perbandingan Algoritma Random Forest, SVM, dan Neural Network untuk Klasifikasi Risiko Keamanan E-Learning," *Jurnal Teknologi dan Informasi*, vol. 16, no. 1, pp. 1–10, Mar. 2026, doi: 10.34010/jati.v16i1.17191.

[31] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 531–540, Mar. 2025, doi: 10.57152/malcom.v5i2.1968.

[32] M. A. Fathurrahman and D. W. Prabowo, "Perbandingan Performa Algoritma Random Forest dan SVM Dalam Mendeteksi serangan DDoS di Jaringan Cloud," *Jurnal Riset Rekayasa Elektro*, vol. 7, no. 2, pp. 193–202, Dec. 2025, doi: 10.30595/jrre.v7i2.27866.

[33] C. Mariano Benny Nara Sanjaya, Y. Suban Belutowe, and S. Juszandri Bulan, "Implementasi Intrusion Detection System (Ids) Berbasis Random Forest Untuk Deteksi Serangan Phishing Pada Jaringan Wi-Fi Publik," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 10, no. 2, pp. 3617–3622, Mar. 2026, doi: 10.36040/jati.v10i2.18239.

[34] A. Purnomo, A. Kurniasih, A. Nuarminah, and S. Hartati, "Peran Artificial Intelligence dalam Deteksi Dini Ancaman Keamanan Jaringan," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 2044–2048, Dec. 2024, doi: 10.33395/jmp.v13i2.14356.

[35] Y. Risyani, S. Japit, C. Bombongan, T. Selamat, and Y. Yuliana, "Sistem Keamanan Siber Adaptif Berbasis AI: Analisis Kinerja, Arsitektur, dan Penerapannya pada Organisasi Modern," *Jurnal Minfo Polgan*, vol. 14, no. 2, pp. 2999–3006, Nov. 2025, doi: 10.33395/jmp.v14i2.15630.

[36] D. Hidayat, "Analisis Sistem E-Learning Berbasis ISO 27005:2018 Menggunakan Algoritma Klasifikasi Random Forest," *Jurnal Teknologi dan Informasi*, vol. 15, no. 2, pp. 110–120, Sep. 2025, doi: 10.34010/jati.v15i2.16173.

[37] M. Rosanti, yusrodi, A. E. S, Bahterayudha, and T. Saragih, "Implementasi Sistem Keamanan Siber Berbasis Artificial Intelligence Untuk Mengatasi Serangan Phishing," *Aisyah Journal of Informatics and Electrical Engineering Universitas Aisyah Pringsewu*, vol. 7, no. 1, pp. 94–98, Feb. 2025, doi: https://doi.org/10.30604/jti.v7i1.674.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 835-845
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1167

[38] I. Elan Maulani, D. Rayhan Sunandar Putra, and K. Komarudin, "Sistem Deteksi Intrusi Cerdas: Studi Perbandingan Algoritma Pembelajaran Mesin Untuk Keamanan Siber," *Jurnal Sosial Teknologi*, vol. 3, no. 11, pp. 918–923, Nov. 2023, doi: 10.59188/jurnalsostech.v3i11.987.