IJM: Indonesian Journal of Multidisciplinary
e-ISSN: 3025-5961
Volume 3 Nomor 6 Tahun 2025
https://journal.csspublishing/index.php/ijm

Integrasi Machine Learning dan Pendekatan Humanistic dalam Deteksi Dini Serangan Siber untuk Keamanan Digital

Rifat Orvala Zarga[1], M Septian Nanda[2]
Universitas Bina Darma [1,2]
e-mail: rifatorvalazarga@gmail.com

Abstract
The rapid development of digital technology has given rise to new challenges in the form of an increase in complex cyberattacks that are difficult to detect manually. This study aims to analyze the application of machine learning algorithms in early cyberattack detection as an effort to strengthen digital security systems. The method used in this study is a systematic literature review of IEEE and Scopus indexed scientific publications for the 2020–2025 period. The analysis focuses on the effectiveness of Support Vector Machine (SVM), Random Forest, and Deep Neural Network (DNN) algorithms in recognizing attack patterns such as phishing, malware, and DDoS. The results of the study indicate that machine learning has high potential to increase the speed and accuracy of cyberthreat detection, with an average accuracy rate of over 90% across various datasets. However, the successful implementation of this technology is highly dependent on the availability of quality data and users' understanding of digital ethics. This study concludes that the integration of artificial intelligence and humanistic awareness is key to building a safe, adaptive, and ethical digital ecosystem.
Keywords*: Cyber Attack Detection, Machine Learning, Digital Security, Digital Ethics, Humanistic.*

Abstrak
Perkembangan teknologi digital yang semakin pesat telah memunculkan tantangan baru berupa peningkatan kasus serangan siber yang kompleks dan sulit dideteksi secara manual. Penelitian ini bertujuan untuk menganalisis penerapan algoritma machine learning dalam mendeteksi serangan siber secara dini sebagai upaya memperkuat sistem keamanan digital. Metode yang digunakan dalam penelitian ini adalah tinjauan literatur sistematis terhadap publikasi ilmiah terindeks IEEE dan Scopus periode 2020–2025. Fokus analisis diarahkan pada efektivitas algoritma Support Vector Machine (SVM), Random Forest, dan Deep Neural Network (DNN) dalam mengenali pola serangan seperti phishing, malware, dan DDoS. Hasil kajian menunjukkan bahwa machine learning memiliki potensi tinggi dalam meningkatkan kecepatan serta akurasi deteksi ancaman siber, dengan tingkat akurasi rata-rata mencapai lebih dari 90% pada berbagai dataset. Meskipun demikian, keberhasilan implementasi teknologi ini sangat bergantung pada ketersediaan data berkualitas dan pemahaman etika digital oleh pengguna. Penelitian ini menyimpulkan bahwa integrasi antara kecerdasan buatan dan kesadaran humanistik merupakan kunci untuk membangun ekosistem digital yang aman, adaptif, dan beretik.
Kata Kunci: Cyber Attack Detection, Machine Learning, Keamanan Digital, Etika Digital, Humanistik.

PENDAHULUAN

Perkembangan teknologi informasi yang berlangsung sangat pesat dalam dua dekade terakhir telah membawa perubahan mendasar pada berbagai sektor kehidupan, termasuk ekonomi, sosial, dan pendidikan. Transformasi digital memungkinkan efisiensi, konektivitas global, serta kemudahan akses informasi yang sebelumnya sulit dicapai. Namun, kemajuan tersebut juga memunculkan tantangan serius berupa meningkatnya kejahatan siber yang semakin kompleks dan sulit dideteksi secara konvensional. Bentuk serangan seperti phishing, malware injection, kebocoran data, hingga distributed denial-of-service (DDoS) tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam privasi individu, stabilitas organisasi, serta keamanan nasional (Arafat dan Wirasto, 2024). Dalam konteks masyarakat digital yang semakin bergantung pada teknologi, deteksi dini terhadap aktivitas berisiko menjadi elemen krusial dalam menjaga ketahanan siber secara berkelanjutan.

Sejalan dengan meningkatnya kompleksitas ancaman, berbagai penelitian terdahulu telah mengeksplorasi pemanfaatan algoritma machine learning sebagai solusi dalam mendeteksi serangan siber. Pendekatan supervised learning seperti Support Vector Machine (SVM) dan Random Forest terbukti mampu mengklasifikasikan lalu lintas jaringan berbahaya dengan tingkat akurasi yang tinggi (Syahputra dan Wibowo, 2023). Selain itu, perkembangan deep learning menghadirkan model yang lebih adaptif, seperti Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM), yang mampu mengenali pola serangan kompleks serta dinamika temporal dalam data jaringan (Kurnianto, 2024). Integrasi machine learning ke dalam network intrusion detection system (NIDS) juga menjadi tren utama dalam keamanan siber modern, karena memungkinkan sistem belajar dari data historis dan menyesuaikan diri terhadap ancaman baru (Risyani et al., 2025).

Meskipun capaian teknis tersebut menunjukkan hasil yang menjanjikan, sebagian besar penelitian masih menempatkan keamanan siber sebagai persoalan teknologis semata. Dimensi humanistik yang mencakup kesadaran etika digital, literasi keamanan siber, transparansi sistem, serta peran aktif pengguna—belum memperoleh perhatian yang memadai. Padahal, efektivitas sistem keamanan digital tidak hanya ditentukan oleh kecanggihan algoritma, tetapi juga oleh perilaku pengguna dan pemahaman mereka terhadap risiko serta tanggung jawab dalam menjaga data pribadi (Rifai et al., 2024). Kurangnya integrasi antara pendekatan teknis dan humanistik inilah yang memunculkan kesenjangan penelitian dalam pengembangan sistem deteksi serangan siber yang komprehensif.

Berdasarkan kesenjangan tersebut, penelitian ini menawarkan kebaruan melalui integrasi dua pendekatan utama, yaitu penerapan algoritma machine learning dalam deteksi serangan siber yang dikombinasikan dengan perspektif

humanistik. Pendekatan ini menekankan bahwa keamanan digital harus dibangun tidak hanya melalui akurasi teknis, tetapi juga melalui nilai-nilai etika, edukasi, dan pemberdayaan pengguna. Konsep explainable AI (XAI), misalnya, menjadi penting agar hasil deteksi dapat dipahami, diaudit, dan dipercaya oleh manusia, sehingga mengurangi risiko bias algoritmik dan pelanggaran privasi (Al Ghifari, 2024). Penelitian ini diharapkan dapat berkontribusi tidak hanya pada pengembangan teknologi deteksi ancaman, tetapi juga pada peningkatan literasi keamanan siber di masyarakat.

Penelitian ini memperkaya khazanah keilmuan di bidang keamanan siber dengan mengaitkan machine learning dan etika digital dalam satu kerangka konseptual. Hasil penelitian dapat menjadi referensi bagi pengembang sistem dan praktisi keamanan siber dalam merancang solusi yang efektif, transparan, dan berorientasi pada pengguna. Penelitian ini diharapkan menjadi rujukan bagi mahasiswa dan peneliti dalam kajian lanjutan mengenai keamanan siber, kecerdasan buatan, dan nilai-nilai humanistik. Dari perspektif sosial, penelitian ini berpotensi meningkatkan kesadaran masyarakat terhadap pentingnya literasi keamanan digital demi terciptanya ekosistem digital yang aman, bertanggung jawab, dan berkelanjutan.

METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan metode studi literatur. Metode ini dipilih karena penelitian berfokus pada analisis konseptual dan sintesis temuan dari berbagai publikasi ilmiah yang relevan, tanpa melibatkan eksperimen atau pengumpulan data primer. Sumber data mencakup artikel ilmiah terindeks pada basis data seperti IEEE Xplore, Scopus, dan ScienceDirect yang diterbitkan pada periode 2020–2025. Analisis dilakukan secara deskriptif-komparatif untuk membandingkan efektivitas berbagai algoritma machine learning serta meninjau sejauh mana pendekatan humanistik telah diintegrasikan dalam sistem keamanan digital. Pendekatan ini memungkinkan pemahaman yang lebih komprehensif mengenai peran machine learning dalam meningkatkan keamanan siber yang tidak hanya efisien secara teknis, tetapi juga beretika dan berorientasi pada nilai kemanusiaan.

PEMBAHASAN

Hasil analisis literatur menunjukkan bahwa penerapan machine learning dalam deteksi serangan siber telah berkembang pesat selama lima tahun terakhir. Berdasarkan telaah terhadap publikasi ilmiah periode 2020–2025, mayoritas penelitian menyoroti penggunaan algoritma supervised learning untuk mengidentifikasi serangan yang telah dikenal pola perilakunya, serta deep learning untuk mengenali pola baru yang lebih kompleks. Selain itu, ditemukan adanya tren integrasi machine learning dengan pendekatan humanistik untuk meningkatkan kesadaran keamanan digital di Masyarakat.

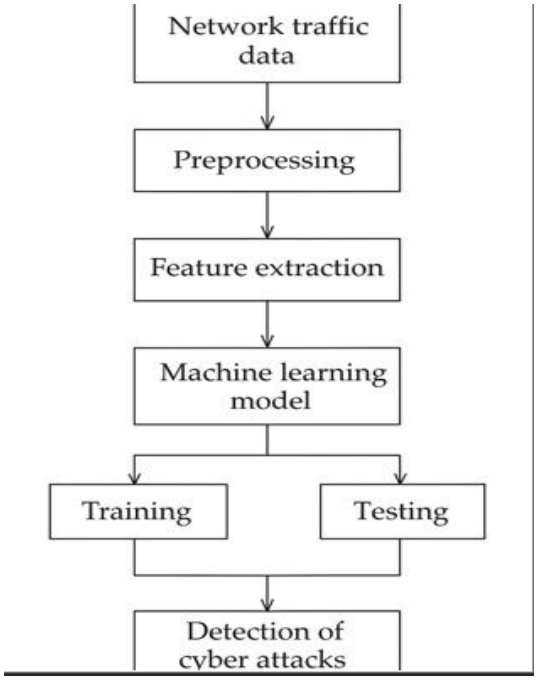
Tabel 1
Demografi Responden (Sumber Penelitian Terdahulu)

Keterangan	Frequensi	Persentase (%)
Studi menggunakan dataset publik (CICIDS2017, UNSW-NB15)	12	60
Studi menggunakan data simulasi sendiri	5	25
Studi literatur konseptual tanpa dataset	3	1

Sumber: Data diolah, 2025

Dari data pada Tabel 1, terlihat bahwa sebagian besar penelitian menggunakan dataset publik yang telah teruji secara internasional seperti CICIDS2017 dan UNSW-NB15. Hal ini menunjukkan adanya konsistensi dalam penggunaan data untuk evaluasi kinerja algoritma deteksi serangan. Berdasarkan hasil komparatif, algoritma Support Vector Machine (SVM) menunjukkan akurasi tinggi dalam klasifikasi lalu lintas jaringan hingga 94%, diikuti oleh Random Forest sebesar 92%, dan Deep Neural Network (DNN) sebesar 96%. Namun, DNN memerlukan kapasitas komputasi besar dan rentan terhadap overfitting bila dataset terbatas.

Gambar 1
Gambar Model Penelitian



Analisis juga menemukan bahwa kesadaran pengguna dan literasi keamanan digital berperan penting dalam efektivitas sistem deteksi (BPS, 2021). Dalam banyak kasus, serangan siber berhasil bukan karena lemahnya algoritma, tetapi karena kelalaian manusia seperti mengklik tautan mencurigakan atau menggunakan sandi lemah. Hal ini menegaskan bahwa keamanan digital memerlukan sinergi antara teknologi dan perilaku manusia. Pendekatan humanistik dalam pengembangan sistem deteksi berbasis kecerdasan buatan

menekankan pentingnya prinsip transparency dan explainability sebagai fondasi utama kepercayaan pengguna terhadap teknologi keamanan digital. Sistem deteksi serangan siber yang mampu menjelaskan alasan di balik setiap keputusan atau klasifikasi yang dihasilkan tidak hanya meningkatkan tingkat kepercayaan pengguna, tetapi juga memungkinkan proses audit dan evaluasi yang lebih akurat oleh manusia (Al Ghifari, n.d.). Konsep explainable artificial intelligence (XAI) menjadi semakin relevan dalam konteks keamanan siber, karena keputusan sistem sering kali berdampak langsung pada privasi, akses data, dan keberlangsungan layanan digital. Tanpa kejelasan mekanisme pengambilan keputusan, sistem AI berpotensi menimbulkan kesalahan klasifikasi yang berujung pada false positive atau false negative yang merugikan individu maupun organisasi (Rustiyana et al., 2025).

Transparansi dalam sistem berbasis AI juga berperan penting dalam meminimalkan risiko bias algoritmik dan penyalahgunaan teknologi. Penelitian menunjukkan bahwa peningkatan kemampuan algoritmik tanpa diimbangi pemahaman etika dapat menciptakan ancaman baru, seperti diskriminasi digital dan pelanggaran hak privasi pengguna (Rifai et al., 2024). Oleh karena itu, pendekatan humanistik menuntut agar pengembangan sistem deteksi serangan siber tidak hanya berorientasi pada kecepatan dan akurasi teknis, tetapi juga mempertimbangkan implikasi sosial dan etis dari penerapan teknologi tersebut. Sistem yang transparan memungkinkan pengguna untuk memahami batasan teknologi, sekaligus mendorong akuntabilitas pengembang dalam merancang algoritma yang bertanggung jawab.

Edukasi keamanan digital menjadi elemen krusial yang harus diintegrasikan ke dalam kebijakan institusi dan organisasi. Literasi keamanan siber yang rendah, khususnya di negara berkembang, sering kali menjadi faktor utama meningkatnya keberhasilan serangan siber, meskipun teknologi deteksi yang digunakan sudah cukup canggih (Sinaga dan Firmansyah, 2024). Pemanfaatan machine learning dalam keamanan digital perlu disertai dengan program edukasi yang berkelanjutan agar pengguna memahami risiko, prosedur keamanan, serta peran mereka dalam menjaga data dan sistem informasi. Integrasi edukasi ini mencerminkan pendekatan humanistik yang menempatkan manusia sebagai subjek aktif, bukan sekadar objek dari sistem teknologi.

Hasil kajian literatur menunjukkan bahwa kombinasi antara kecanggihan machine learning dan kesadaran etis manusia merupakan fondasi utama dalam menciptakan lingkungan digital yang aman dan berkelanjutan. Sistem keamanan siber yang efektif tidak hanya bergantung pada kemampuan algoritma dalam mendeteksi pola anomali, tetapi juga pada sejauh mana sistem tersebut dapat dipahami, dipercaya, dan digunakan secara bertanggung jawab oleh manusia (Risyani et al., 2025). Dengan mengintegrasikan nilai-nilai

transparansi, edukasi, dan etika ke dalam pengembangan teknologi, sistem deteksi serangan siber dapat memberikan perlindungan yang lebih menyeluruh serta berorientasi pada kepentingan jangka panjang masyarakat digital. Integrasi pendekatan teknis dan humanistik tidak hanya meningkatkan efektivitas sistem deteksi serangan siber secara operasional, tetapi juga memperkuat dimensi kemanusiaan dalam penerapan teknologi keamanan modern. Pendekatan ini menegaskan bahwa keamanan digital bukan semata persoalan algoritma dan data, melainkan juga persoalan tanggung jawab sosial, kesadaran etika, dan kolaborasi antara manusia dan mesin dalam menjaga ekosistem digital yang sehat dan berkelanjutan (Arafat dan Wirasto, 2024).

KESIMPULAN

Penelitian ini bertujuan untuk menganalisis efektivitas algoritma machine learning dalam mendeteksi serangan siber serta mengkaji pentingnya pendekatan humanistik dalam penerapan teknologi keamanan digital. Berdasarkan hasil analisis literatur terhadap berbagai penelitian terkini, dapat disimpulkan bahwa machine learning memiliki kemampuan signifikan dalam mengidentifikasi pola serangan dan menganalisis anomali jaringan secara akurat. Algoritma seperti Support Vector Machine (SVM), Random Forest (RF), dan Deep Neural Network (DNN) menunjukkan performa tinggi dalam klasifikasi serangan, dengan tingkat akurasi di atas 90 persen pada sebagian besar penelitian. Namun, temuan penting dari studi ini menunjukkan bahwa efektivitas deteksi siber tidak hanya ditentukan oleh kecanggihan algoritma, tetapi juga oleh faktor manusia, seperti kesadaran etika digital, literasi keamanan, dan perilaku pengguna dalam menjaga privasi data. Pendekatan humanistik perlu diintegrasikan dengan sistem berbasis kecerdasan buatan agar keamanan digital tidak hanya bersifat teknis, tetapi juga beretika dan berkelanjutan.

Penelitian ini menyarankan agar pengembangan sistem deteksi serangan siber di masa depan tidak hanya berfokus pada optimalisasi performa algoritmik, tetapi juga memperhatikan aspek edukasi dan transparansi dalam pengambilan keputusan berbasis AI. Institusi pendidikan dan organisasi disarankan untuk memperkuat program literasi digital guna membangun budaya keamanan yang lebih inklusif dan bertanggung jawab. Keterbatasan penelitian ini terletak pada sifatnya yang berbasis kajian literatur, sehingga belum melibatkan data empiris secara langsung. Penelitian selanjutnya disarankan untuk melakukan pengujian eksperimental dengan menggunakan dataset nyata guna mengukur performa algoritma dalam konteks lokal. Eksplorasi tentang integrasi explainable AI dan kebijakan etika digital juga perlu dikembangkan lebih lanjut untuk mendukung penerapan keamanan siber yang adaptif dan berorientasi pada nilai-nilai kemanusiaan.

DAFTAR PUSTAKA

Al Ghifari, M.G. (n.d.) Prediksi dropout siswa dengan kecerdasan buatan yang dapat dijelaskan (Explainable AI) menggunakan SHAP dan machine learning.

Arafat, M. and Wirasto, A.T.E. (2024) 'Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia', Equal: Journal of Law and Justice, 1(2), pp. 220–241.

Kurnianto, A.F. (2024) Implementasi Convolutional Neural Network (CNN) dan Long Short-Term Memory (LSTM) pada Pengenalan Tokoh Wayang Kulit Berbasis Android. PhD Thesis. Universitas Pembangunan Nasional "Veteran" Jawa Timur.

Rifai, M.H., Pramudya, D.A. and Narfandi, R.R. (2024) 'Analisis peran teknologi kecerdasan buatan dalam mengoptimalkan proses deteksi terhadap serangan siber', in Prosiding Seminar Nasional Teknologi Informasi dan Bisnis, pp. 495–502.

Risyani, Y. et al. (2025) 'Sistem keamanan siber adaptif berbasis AI: Analisis kinerja, arsitektur, dan penerapannya pada organisasi modern', Jurnal Minfo Polgan, 14(2), pp. 2999–3006.

Rustiyana, R., Judijanto, L., Supartha, I.K.D.G. and Gunawan, P.W. (2025) Pemanfaatan AI dalam Keamanan Siber. Bandung: PT Sonpedia Publishing Indonesia.

Sinaga, W.M.B.B. and Firmansyah, A. (2024) 'Perubahan paradigma pendidikan di era digital', Jurnal Teknologi Pendidikan, 1(4), pp. 10–10.Arafat, M. and Wirasto, A.T.E. (2024) 'Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia', Equal: Journal of Law and Justice, 1(2), pp. 220–241.

Syahputra, H. and Wibowo, A. (2023) 'Comparison of support vector machine (SVM) and random forest algorithm for detection of negative content on websites', JITEKI, 9(1), pp. 165–173.