Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 3 (2025) pp: 3835-3841
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Keamanan Siber Menggunakan Kecerdasan Buatan**:** Tinjauan Pustaka

Muhamad Aria Armada Djojosugito[1], Miri Ardiansyah[2]
[1,2]Departemen Sistem Informasi, Fakultas Ilmu Komputer, Universitas Sains Indonesia
muhammad.aria@lecturer.sains.ac.id , miri.ardiansyah@lecturer.sains.ac.id

Abstrak

Kecerdasan Buatan memiliki manfaat dan kegunaan yang dapat disesuaikan dalam berbagai bidang. Dengan kemampuan kecerdasan buatan (AI) yang semakin maju, manfaat dan kegunaan dari kecerdasan buatan akan semakin meningkat pesat. Salah satu bidang dimana kecerdasan buatan dapat digunakan adalah keamanan siber. Dengan metode tinjauan pustaka, makalah penelitian ini meneliti berbagai cetusan ide penelitian dan eksperimen yang sudah dilakukan oleh berbagai penelitian-penelitian sebelumnya untuk membandingkan manfaat serta kelemahan dari penelitian-penelitian tersebut. Dari tinjauan pustaka yang dilaksakan, ditemukan bahwa AI memberikan deteksi ancaman akurasi tinggi, pengawasan real-time yang meningkat, serta otomasi yang mendukung kemampuan manusia. Kekurangan dari AI berada di kebutuhan yang tinggi akan data berkualitas, kebutuhan sumber daya perhitungan AI yang tinggi dengan waktu latihan model AI yang lama, serta kebutuhan komputasi yang tinggi. Sebagai penutup, penelitian ini merekomendasikan agar penelitian mengenai penggunaan kecerdasan buatan dalam mengamankan dunia siber dari serangan agar terus ditingkatkan dan lebih dikreatifkan.

Kata Kunci: Kecerdasan Buatan, Keamanan Siber, Model AI

1. Latar Belakang

Perkembangan dari teknologi informasi yang pesat dalam dua dekade terakhir telah membawa transformasi besar dalam berbagai aspek kehidupan umat manusia, mulai dari sisi komunikasi, ekonomi, pendidikan, hingga pemerintahan. Dari berbagai aspek kehidupan manusia tersebut, teknologi informasi menjadi sebuah struktur pendukung yang dengan berjalannya waktu menjadi bagian tak terpisahkan yang esensial untuk keberlanjutan proses kehidupan manusia. Namun, seiring dengan meningkatnya ketergantungan aspek kehidupan manusia terhadap sistem digital, ancaman kepada sistem digital tersebut dari bidang keamanan siber (*cybersecurity*) pun menjadi semakin kompleks dan sulit dikendalikan [1]. Serangan-serangan siber seperti *phishing, malware, ransomware,* dan *denial of service* (DoS) [2] menjadi semakin canggih, terorganisir, kompleks, dan semakin sulit dideteksi secara dini dengan metode-metode konvensional yang ada.

Pendekatan tradisional dalam keamanan siber, yang umumnya berbasis pada aturan statis (*rule-based systems*) dan deteksi tanda tangan (*signature-based detection*), terbukti kurang efektif dalam menghadapi serangan yang bersifat dinamis dan adaptif [3]. Untuk menyamakan serangan-serangan siber yang semakin canggih dan melawannya, penerapan dari kecerdasan buatan (*Artificial Intelligence*/AI) dalam bidang keamanan siber menjadi sebuah pendekatan yang menjadi semakin banyak dilirik [4,5]. Kecerdasan buatan memiliki kemampuan untuk menganalisa data dalam jumlah yang tidak mungkin dianalisa secara efektif oleh manusia [6], mengenali pola-pola yang tidak normal [7], dan melakukan deteksi serta respons secara otomatis terhadap potensi ancaman siber [8]. Dengan kemampuan dari pembelajaran mesin (*machine learning*) [9] dan pembelajaran mendalam (*deep learning*) dari kecerdasan buatan, sistem keamanan siber dapat ditingkatkan dengan kemampuan untuk mengenali pola-pola anomali dalam lalu lintas jaringan [10], mengklasifikasikan jenis serangan, serta memberikan respons secara real-time terhadap potensi insiden keamanan [11].

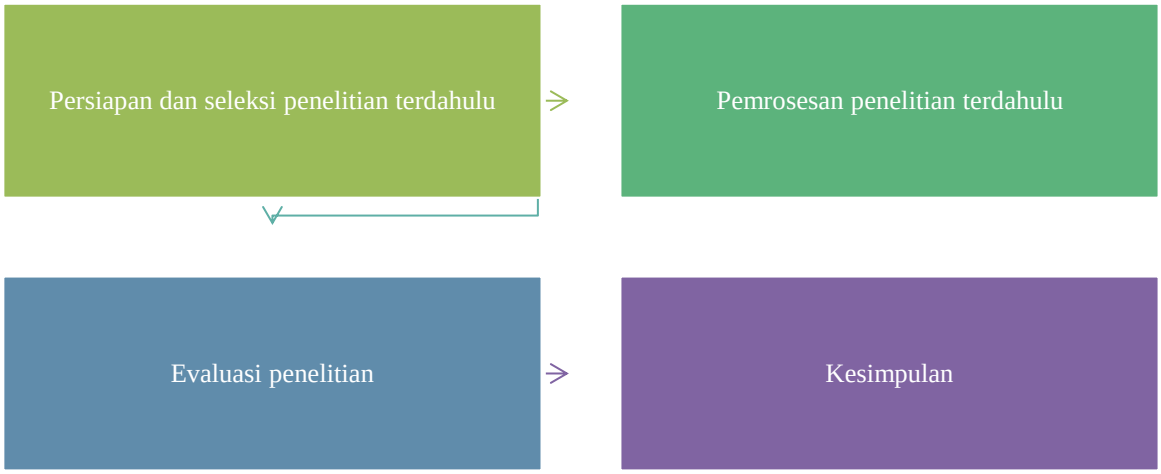
Artikel ini memiliki tujuan untuk mengeksplorasi penerapan kecerdasan buatan dalam domain keamanan siber, dengan fokus utama terhadap penerapan dan manfaat dari teknik kecerdasan buatan dalam keamanan siber. Penelitian ini juga berfokus kepada efektivitas, keunggulan, serta keterbatasan teknis yang masih menjadi tantangan dalam penerapan kecerdasan buatan. Dengan demikian, tulisan ini diharapkan dapat memberikan kontribusi akademik dan praktis terhadap pengembangan sistem keamanan siber yang lebih tangguh dan berkelanjutan di era digital.

1. Metode Penelitian

Menggunakan metode *systematic literature review* (SLR), penelitian ini melaksanakan studi literatur dari penelitian terdahulu. Penelitian ini diambil berdasarkan fokus mereka terhadap penerapan AI di bidang keamanan siber, data empiris hasil penelitian mereka, tipe implementasi, metrik performa, kualitas metodologi, dan tipe studi yang dilaksanakan. Dari penelitian terdahulu yang dikumpulkan, akan dicari metode kecerdasan buatan apa yang digunakan, domain penerapan keamanan siber, serta tipe studi yang digunakan.

Setelah mendapat penelitian terdahulu yang memenuhi syarat diatas, dicari berbagai kekuatan dari AI di bidang keamanan siber, rata-rata tingkat kesuksesan penggunaan dari AI di keamanan siber, serta keterbatasan yang ada dengan kecerdasan buatan yang ada pada saat ini.

Proses dari penelitian dibagi menjadi 4 tahapan seperti yang ditunjukan di Gambar 1 dibawah ini.



Gambar 1. Tahapan Penelitian

Menggunakan metode *systematic literature review* (SLR) yang dijabarkan pada Gambar 1 diatas, diperoleh 10 penelitian terdahulu yang memenuhi kriteria melalui berbagai sumber internasional. Penelitian terdahulu dijabarkan pada Tabel 1 dibawah ini.

DOI: https://doi.org/ 10.31004/riggs.v4i3.2549

Judul Penelitian	Fokus Penelitian	Metode AI	Domain Penerapan Keamanan
Kaur et al., 2023	Penerapan kecerdasan buatan dalam kemanan siber	Tidak dikatakan	Keamanan siber umum
Abdullahi et al., 2022	Metode kecerdasan buatan untuk mendeteksi serangan siber di IoT	*Support Vector Machine* (SVM), *Random Forest*, *Neural Networks*, *Recurrent Neural Network* (RNN), *Convolutional Neural Network* (CNN), *Deep Autoencoders*, *XGBoost*, *Long Short-Term Memory* (LSTM)	Keamanan IoT, Deteksi intrusi
Dalal, 2018	AI di keamanan siber untuk deteksi ancaman dan respons	*Supervised*, *unsupervised*, dan *reinforcement learning*, *Deep learning*, *Natural Language Processing* (NLP)	Deteksi ancaman, Deteksi intrusi, Analisa malware, Keamanan jaringan
Ofusori et al., 2024	AI di keamanan siber	Teknik *machine learning*	Deteksi ancaman, Keamanan jaringan
Jada and Mayayise, 2023	Dampak kecerdasan buatan terhadap keamanan siber organisasi	Tidak dikatakan	Keamanan siber umum
Sankaram et al., 2024	Aplikasi kecerdasan buatan dalam meningkatkan deteksi dan respons terhadap ancaman keamanan siber	Algoritma belajar *supervised* dan *unsupervised*	Deteksi intrusi, Deteksi malware, Deteksi phishing, Intelijen ancaman, Keamanan jaringan, Proteksi endpoint
Salem et al., 2024	Teknik deteksi berbasis kecerdasan buatan dalam keamanan siber	*Machine Learning*, *Deep Learning*, Algoritma metaheuristik	Deteksi ancaman, Deteksi intrusi, Analisa malware, Keamanan jaringan, Deteksi phishing, Deteksi spam
Wiafe et al., 2020	AI untuk keamanan siber	*Support Vector Machines*	Deteksi intrusi
Sharma, 2024	Sistem deteksi dan respons ancaman siber yang ditingkatkan dengan kecerdasan buatan	*Supervised Learning*, *Unsupervised Learning*, *Deep Learning*, *Reinforcement Learning*	Deteksi ancaman, Deteksi intrusi, Deteksi malware
Vadisetty, 2024	Dampak kecerdasan buatan terhadap integritas data dalam keamanan siber	Tidak dikatakan	Keamanan siber umum

Tabel 1. Penelitian terdahulu beserta fokus penelitian, metode AI, dan domain penerapan keamanan

Dari 10 penelitian terdahulu yang terpilih, 6 penelitian berfokus terhadap penerapan AI secara khusus pada bidang keamanan siber, sedangkan 4 penelitian berfokus pada penerapan AI secara umum di bidang keamanan siber. Dari penelitian diatas pula, ditemukan bahwa ada penelitian yang menyatakan penggunaan metode AI secara spesifik dan ada yang tidak. Dari sisi domain penerapan keamanan siber, 6 penelitian meneliti mengenai deteksi intrusi, 4 penelitian meneliti deteksi ancaman, 4 penelitian meneliti keamanan jaringan, 3 penelitian meneliti keamanan siber umum, serta domain penelitian lainnya.

3. Hasil dan Diskusi

Dari penelitian-penelitian terdahulu, diperoleh informasi mengenai kemampuan dari kecerdasan buatan dan kekuatan yang ditambahkan ke bidang keamanan siber yang dijabarkan dibawah ini.

3.1. Kemampuan dan Kelebihan Kecerdasan Buatan pada Keamanan Siber

Dalam perihal kecepatan dan akurasi deteksi ancaman siber, Dalal mencatat bahwa model *Deep Learning* yang dikembangkan untuk mendeteksi intrusi jaringan dapat mendeteksi berbagai bentuk serangan dengan akurasi lebih dari 98%, sementara algoritma *unsupervised machine learning* menunjukkan kemampuan deteksi hingga mendekati 90% terhadap sampel malware yang sebelumnya tidak dikenali [12,13]. Kemampuan dan keunggulan dari kecerdasan buatan ini juga ditegaskan pada penelitian Salem et al. (2024) yang menyoroti kontribusi signifikan kecerdasan buatan dalam meningkatkan efektivitas deteksi serta respons terhadap beberapa ancaman siber [14].

DOI: https://doi.org/ 10.31004/riggs.v4i3.2549

Selain itu, sistem keamanan siber yang diperkuat dengan kecerdasan buatan juga memainkan peran penting dalam melindungi ekosistem IoT (*Internet of Things*) yang bersifat terdistribusi. Dalam konteks ini, integrasi teknologi blockchain menjadi solusi strategis untuk menjaga privasi dan integritas data, sekaligus mendukung lingkungan pembelajaran AI yang aman dan andal bagi sistem keamanan siber [15]. Pendekatan ini tidak hanya memperkuat pertahanan terhadap ancaman, tetapi juga meningkatkan kepercayaan terhadap penerapan AI di infrastruktur digital yang kompleks dan tersebar.

Kemampuan otomasi yang dimiliki oleh kecerdasan buatan mendapat perhatian positif dalam konteks keamanan siber. Otomasi dipandang sebagai salah satu keunggulan utama AI dalam mendeteksi dan merespons ancaman secara efisien, sebagaimana dijelaskan oleh Kaur et al. (2023) [16]. Sejalan dengan itu, Jada dan Mayayise (2023) turut menekankan bahwa otomasi dalam keamanan siber merupakan area strategis di mana kecerdasan buatan dapat memberikan dampak signifikan terhadap peningkatan postur keamanan organisasi secara keseluruhan [17].

Pembelajaran adaptif menjadi pendekatan yang semakin menonjol dalam sistem keamanan siber modern, dimana teknik berbasis kecerdasan buatan terbukti lebih unggul dibandingkan metode tradisional dalam merespons ancaman yang terus berkembang [18]. Selain itu, penggunaan *reinforcement learning* turut digarisbawahi sebagai potensi untuk membangun sistem respons ancaman yang adaptif dan dinamis di organisasi-organisasi berskala besar [19]. Selain itu, sistem AI yang dilengkapi dengan kemampuan *Natural Language Processing* (NLP) juga berperan penting dalam mendeteksi serta merespons berbagai ancaman siber secara lebih cerdas dan kontekstual, sehingga mendukung terbentuknya sistem keamanan yang lebih adaptif dan responsif [20].

3.2. Tantangan dan Keterbatasan Implementasi

Meskipun kecerdasan buatan memiliki keunggulan dalam meningkatkan kapabilitas keamanan siber organisasi dalam menghadapi beragam ancaman, terdapat sejumlah keterbatasan dan tantangan yang tidak dapat diabaikan. Berdasarkan berbagai studi terdahulu, kendala-kendala tersebut dapat diklasifikasikan ke dalam tiga kategori utama, yaitu persyaratan terhadap kualitas data yang tinggi, kebutuhan sumber daya komputasi yang besar, serta hambatan teknis dalam implementasi sistem AI secara efektif.

Salah satu tantangan utama dalam penerapan kecerdasan buatan di bidang keamanan siber adalah syarat kualitas data. Jada dan Mayayise [17] serta Vadisetty [21] secara eksplisit menyatakan bahwa isu kualitas data merupakan hambatan yang signifikan. Hal ini disebabkan karena efektivitas model AI sangat bergantung pada kualitas serta keterwakilan data yang digunakan dalam proses pelatihan model tersebut.

Tantangan lain dalam penerapan kecerdasan buatan untuk keamanan siber adalah tingginya kebutuhan sumber daya komputasi. Abdullahi et al. [22] menyatakan bahwa proses pelatihan model AI memerlukan waktu yang lama akibat besarnya dataset masukan serta tingginya kompleksitas perhitungan. Selain itu, Salem et al. [14] juga menekankan bahwa pemrosesan data keamanan siber yang sangat luas menuntut penggunaan sumber daya yang intensif.

Dari sisi teknis, terdapat sejumlah tantangan yang perlu diperhatikan dalam penerapan kecerdasan buatan untuk keamanan siber. Kompleksitas algoritma AI itu sendiri sering kali menyulitkan dalam hal implementasi dan pemeliharaan. Selain itu, sistem AI memerlukan pembaruan secara rutin agar tetap relevan dalam menghadapi dinamika ancaman yang terus berkembang. Tantangan lain yang tidak kalah penting adalah kesulitan dalam menafsirkan proses pengambilan keputusan, khususnya pada model *deep learning*, yang kerap dianggap sebagai *black box* karena rendahnya transparansi dalam penjelasan hasil prediksi.

3.3 Dampak Operasional

Berdasarkan telaah terhadap berbagai penelitian terdahulu, dapat disusun dampak penerapan kecerdasan buatan terhadap kegiatan operasional, sebagaimana ditampilkan pada Tabel 2 dibawah ini.

DOI: https://doi.org/ 10.31004/riggs.v4i3.2549

Domain Keamanan	Solusi Kecerdasan Buatan	Kekuatan Kunci	Keterbatasan
Deteksi Intrusi	*Machine Learning* (e.g.,SVM, *Random Forest*)	Akurasi tinggi, penggunaan memori yang efisien	Waktu CPU yang lama, prediksi real-time yang tidak efektif
Analisa Malware	*Deep Learning, Unsupervised Learning*	Deteksi malware yang belum diketahui sebelumnya, akurasi tinggi	Kebutuhan dataset dan tenaga komputasi yang besar
Keamanan Jaringan	*Supervised* dan *Unsupervised Learning*	Pengawasan real time yang meningkat, penguatan otentifikasi	Perlunya untuk mengatasi volume data dalam jumlah besar, kebutuhan untuk belajar terus menerus
Deteksi Phishing	Email yang diperkuat AI dan Analisa URL	Pengurangan insiden Phishing	Tantangan dengan sinyal positif palsu
Keamanan IoT	Berbagai teknik *Machine Learning* dan *Deep Learning*	Efektif untuk mendeteksi serangan yang beragam	Tantangan dengan dataset besar yang tidak seimbang
Intelijen Ancaman	Analisa Prediktif, Analisa Data Otomatis	Mengungkap ancaman tersembunyi, mengantisipasi serangan	Membutuhkan data ekstensif, potensi untuk alarm palsu
Proteksi Endpoint	Pengawasan dan Respons yang Dikendarai AI	Pertahanan kuat melawan intrusi sistem	Keterbatasan sumber daya, kebutuhan untuk pembaruran reguler
Keamanan Siber Umum	Berbagai Teknik AI	Otomisasi, deteksi ancaman, dan respons yang ditingkatkan	Lemah melawan serangan advesarial, kecemasan etis

Tabel 2. Dampak Operasional Keamanan Siber dari Kecerdasan Buatan

Berdasarkan Tabel 2, terlihat bahwa kekuatan utama dari penerapan kecerdasan buatan dalam berbagai domain keamanan siber terletak pada kemampuannya memberikan tingkat akurasi yang tinggi, efisiensi dalam penggunaan memori, serta peningkatan otomatisasi dan deteksi ancaman. Namun demikian, kecerdasan buatan juga menghadapi sejumlah keterbatasan yang bervariasi tergantung pada domain penerapannya. Beberapa di antaranya mencakup kebutuhan sumber daya komputasi yang besar, tantangan dalam prediksi secara real-time, potensi sinyal positif palsu, serta kesulitan dalam menangani data yang besar dan tidak seimbang. Selain itu, aspek seperti kebutuhan pembaruan rutin, kerentanan terhadap serangan adversarial, dan isu etika turut menjadi perhatian dalam pengembangan dan implementasi solusi AI di bidang keamanan siber secara menyeluruh.

3.4 Pertimbangan dalam Integrasi dan Penerapan Solusi Kecerdasan Buatan

Dalam konteks keamanan siber, kolaborasi yang intensif antara kecerdasan buatan dan manusia menjadi aspek yang krusial. Dalal [12] menekankan pentingnya pengawasan manusia terhadap sistem berbasis kecerdasan buatan serta perlunya membangun kepercayaan manusia terhadap sistem tersebut, terutama karena masih terdapat kesenjangan kemampuan di antara tenaga kerja saat ini untuk mengoperasikan sistem kecerdasan buatan. Oleh karena itu, solusi kecerdasan buatan seharusnya dirancang untuk melengkapi keahlian manusia, bukan untuk menggantikannya sepenuhnya, sehingga tercipta sinergi yang optimal antara otomatisasi dan penilaian manusia.

Kebutuhan akan infrastruktur yang memadai menjadi salah satu faktor penting dalam mendukung implementasi kecerdasan buatan di bidang keamanan siber. Sankaram et al. [18] mencatat bahwa tantangan utama terletak pada kemampuan untuk menangani volume data yang sangat besar, yang secara implisit menunjukkan perlunya sistem penyimpanan dan pemrosesan data yang tangguh. Selain itu, Dalal [12] menyoroti menyoroti kesulitan dalam mengintegrasikan sistem kecerdasan buatan dengan infrastruktur keamanan yang sudah ada, yang sering kali bersifat heterogen dan belum dirancang untuk mendukung teknologi AI secara optimal.

Faktor skalabilitas juga merupakan elemen krusial dalam keberhasilan implementasi kecerdasan buatan di bidang keamanan siber. Meskipun sebagian besar studi yang dikumpulkan tidak menyebutkannya secara eksplisit, berbagai tantangan yang berkaitan dengan keterbatasan komputasi dan kemampuan pemrosesan data mengindikasikan bahwa skalabilitas menjadi kunci untuk memastikan sistem AI mampu beroperasi secara efektif dalam skala besar dan lingkungan yang dinamis.

DOI: https://doi.org/ 10.31004/riggs.v4i3.2549

Dalam penerapan kecerdasan buatan untuk keamanan siber, aspek etis dan hukum juga memegang peranan penting. Sharma [19] menyoroti adanya implikasi etis yang perlu diperhatikan dalam pengembangan dan penggunaan teknologi kecerdasan buatan di bidang ini. Beberapa kekhawatiran utama meliputi isu privasi, perlindungan data pribadi, serta potensi penyalahgunaan sistem kecerdasan buatan untuk tujuan kejahatan, yang semuanya menuntut regulasi dan kebijakan yang matang guna memastikan penggunaan AI secara bertanggung jawab.

Adaptasi dan pembelajaran berkelanjutan merupakan aspek yang sangat penting dalam menjaga efektivitas sistem kecerdasan buatan di tengah lanskap ancaman siber yang terus berkembang. Salem et al. [14] menggarisbawahi tantangan yang dihadapi dalam menyesuaikan sistem terhadap bentuk serangan baru yang semakin kompleks. Sejalan dengan itu, Sankaram et al. [18] menekankan pentingnya mekanisme pembelajaran berkelanjutan agar sistem AI dapat tetap relevan dalam menghadapi ancaman yang akan datang. Untuk mendukung hal tersebut, diperlukan tidak hanya proses teknis seperti pembaruan model dan pelatihan ulang, tetapi juga dukungan dari sisi organisasi dalam bentuk kebijakan dan infrastruktur yang mendorong siklus pembelajaran yang berkelanjutan.

Penggunaan teknik kecerdasan buatan yang lebih mutakhir terus membuka peluang peningkatan kapabilitas sistem keamanan siber berbasis AI. Studi yang dilakukan oleh Capodieci et al. menelusuri dampak penerapan kecerdasan buatan generatif (*Generative AI/GenAI*) dan *Large Language Model* (LLM) terhadap profesi di bidang keamanan siber. Temuan mereka menunjukkan bahwa meskipun para profesional di bidang ini telah mulai memanfaatkan teknologi tersebut dalam praktik kerja mereka, perhatian terhadap aspek etika dan keamanan dari penggunaannya masih relatif minim dan belum menjadi fokus utama [23]. Salah satu pendekatan secara teknologis yang menjanjikan adalah AI neurosimbolik, yang menggabungkan kekuatan pengenalan pola dari sistem pembelajaran mesin modern dengan kemampuan penalaran simbolik yang lebih menyerupai logika manusia [24]. Pendekatan ini memungkinkan sistem AI tidak hanya untuk mendeteksi ancaman berdasarkan data historis, tetapi juga untuk memahami dan menyimpulkan pola ancaman baru secara lebih masuk akal dan terstruktur. Selain itu, sistem AI juga dapat dimanfaatkan untuk memodelkan dan menyimulasikan berbagai skenario serangan siber, sehingga menghasilkan simulator yang berguna untuk pelatihan, pengujian sistem, dan penguatan respons terhadap insiden keamanan [25]

4. Kesimpulan

Berdasarkan kajian terhadap berbagai penelitian terdahulu, dapat disimpulkan bahwa kecerdasan buatan memiliki potensi yang besar dalam mendukung berbagai aspek keamanan siber. Namun, performanya sangat bergantung pada domain penerapannya. Di beberapa area, AI menunjukkan kemampuan luar biasa dalam deteksi ancaman dan otomasi proses, tetapi tetap dihadapkan pada tantangan signifikan, seperti keterbatasan operasional, kebutuhan infrastruktur, serta isu integrasi. Dengan demikian, efektivitas kecerdasan buatan dalam keamanan siber bukanlah solusi yang bersifat menyeluruh, melainkan harus disesuaikan dengan kebutuhan spesifik serta didukung oleh infrastruktur, kebijakan, dan kolaborasi manusia yang memadai.

Referensi

1. C. Novelli, F. Casolari, P. Hacker, G. Spedicato, and L. Floridi, "Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity," *Computer Law & Security Review*, vol. 55, p. 106066, Nov. 2024, doi: 10.1016/j.clsr.2024.106066.
2. M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, "UAV-Assisted IoT Applications, Cybersecurity Threats, AI-Enabled Solutions, Open Challenges With Future Research Directions," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 4, pp. 4583–4605, Apr. 2024, doi: 10.1109/TIV.2023.3309548.
3. M. Hofstetter, R. Riedl, T. Gees, A. Koumpis, and T. Schaberreiter, "Applications of AI in cybersecurity," in *Proceedings - 2020 2nd International Conference on Transdisciplinary AI, TransAI 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 138–141. doi: 10.1109/TransAI49837.2020.00031.
4. N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," *Cogent Eng*, vol. 10, no. 2, 2023, doi: 10.1080/23311916.2023.2272358.
5. F. Kamoun, F. Iqbal, M. A. Esseghir, and T. Baker, "AI and machine learning: A mixed blessing for cybersecurity," in *2020 International Symposium on Networks, Computers and Communications*, IEEE, Oct. 2020. doi: 10.1109/ISNCC49221.2020.9297323.
6. L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction," *Applied Artificial Intelligence*, vol. 38, no. 1, Dec. 2024, doi: 10.1080/08839514.2024.2439609.
7. I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," *IEEE Access*, vol. 8, pp. 146598–146612, 2020, doi: 10.1109/ACCESS.2020.3013145.
8. D. Jain, D. Choudhary, A. Anand, N. K. Trivedi, V. Gautam, and S. K. Mohapatra, "Cybersecurity Solutions Using AI Techniques," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICRITO56286.2022.9965045.
9. I. Bala, M. M. Mijwil, G. Ali, and E. Sadıkoğlu, "Analysing the Connection Between AI and Industry 4.0 from a Cybersecurity Perspective: Defending the Smart Revolution," *Mesopotamian Journal of Big Data*, pp. 63–69, Jun. 2023, doi: 10.58496/mjbd/2023/009.
10. J. Ali *et al.*, "A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks," *Comput Commun*, vol. 229, Jan. 2025, doi: 10.1016/j.comcom.2024.108000.
11. B. Bowman and H. H. Huang, "Towards Next-Generation Cybersecurity with Graph AI," *Operating Systems Review (ACM)*, vol. 55, no. 1, pp. 61–67, Jul. 2021.
12. A. Dalal, "Cybersecurity And Artificial Intelligence- How AI Is Being Used In Cybersecurity To Improve Detection And Response To Cyber Threats," *Turkish Journal of Computer and Mathematics Education*, vol. 9, pp. 1704–1709, 2018.

DOI: https://doi.org/ 10.31004/riggs.v4i3.2549

13. D. Saxena, I. Gupta, R. Gupta, A. K. Singh, and X. Wen, "An AI-Driven VM Threat Prediction Model for Multi-Risks Analysis-Based Cloud Cybersecurity," *IEEE Trans Syst Man Cybern Syst*, vol. 53, no. 11, pp. 6815–6827, Nov. 2023, doi: 10.1109/TSMC.2023.3288081.
14. A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *J Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00957-y.
15. J. Kim and N. Park, "Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments," *Applied Sciences (Switzerland)*, vol. 10, no. 14, Jul. 2020, doi: 10.3390/app10144718.
16. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.
17. I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data Inf Manag*, vol. 8, no. 2, Jun. 2024, doi: 10.1016/j.dim.2023.100063.
18. M. Sankaram, M. Roopesh, S. Rasetti, and N. Nishat, "A COMPREHENSIVE REVIEW OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN ENHANCING CYBERSECURITY THREAT DETECTION AND RESPONSE MECHANISMS," *GLOBAL MAINSTREAM JOURNAL*, vol. 3, no. 5, pp. 1–14, Jul. 2024, doi: 10.62304/jbedpm.v3i05.180.
19. S. K. Sharma, "AI-Enhanced Cyber Threat Detection and Response Systems," *Shodh Sagar Journal of Artificial Intelligence and Machine Learning*, vol. 1, no. 2, pp. 43–48, 2024, doi: 10.36676/ssjaiml.v1.i2.14.
20. W. S. Ismail, "Threat Detection and Response Using AI and NLP in Cybersecurity," *Journal of Internet Services and Information Security*, vol. 14, no. 1, pp. 195–205, Feb. 2024, doi: 10.58346/JISIS.2024.I1.013.
21. R. Vadisetty, "The Effects of Cyber Security Attacks on Data Integrity in AI," in *Intelligent Computing and Emerging Communication Technologies, ICEC 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICEC59683.2024.10837148.
22. M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Jan. 01, 2022, *MDPI*. doi: 10.3390/electronics11020198.
23. N. Capodieci, C. Sanchez-Adames, J. Harris, and U. Tatar, "The Impact of Generative AI and LLMs on the Cybersecurity Profession," in *2024 Systems and Information Engineering Design Symposium, SIEDS 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 448–453. doi: 10.1109/SIEDS61124.2024.10534674.
24. B. Jalaian and N. D. Bastian, "Neurosymbolic AI in Cybersecurity: Bridging Pattern Recognition and Symbolic Reasoning," in *MILCOM 2023 - 2023 IEEE Military Communications Conference: Communications Supporting Military Operations in a Contested Environment*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 268–273. doi: 10.1109/MILCOM58377.2023.10356283.
25. A. Jaber and L. Fritsch, "Towards AI-powered Cybersecurity Attack Modeling with Simulation Tools: Review of Attack Simulators," in *Lecture Notes in Networks and Systems*, Springer Science and Business Media Deutschland GmbH, 2023, pp. 249–257. doi: 10.1007/978-3-031-19945-5_25.

DOI: https://doi.org/ 10.31004/riggs.v4i3.2549