Berajah Journal
Jurnal Pembelajaran dan Pengembangan Diri
ISSN (p): **2797-1805** | ISSN (e): **2797-1082**

DAMPAK PENGGUNAAN ARTIFICIAL INTELLIGENCE PADA KEAMANAN SIBER: SEBUAH KAJIAN TERHADAP POTENSI KEUNTUNGAN DAN ANCAMAN

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBERSECURITY: A REVIEW OF POTENTIAL BENEFITS AND THREATS

Rasya Rafika Widalala[1], Amanda Novalina Khairunissa[2], Juhar Ananda Dika[3], Allyssa Az Zahra Wijanarko[4]
UPN "Veteran" Jawa Timur
Email: 23082010098@student.upnjatim.ac.id

ABSTRAK

Kecerdasan Buatan (Artificial Intelligence atau AI) kini banyak dimanfaatkan dalam keamanan siber untuk mendeteksi ancaman sekaligus memaksimalkan keuntungannya. Transformasi teknologi yang cepat menjadikan keamanan siber sebagai isu kritis yang perlu diantisipasi di era digital saat ini. Dalam penelitian ini, dilakukan kajian komprehensif terhadap dampak penggunaan AI dalam keamanan siber, khususnya terhadap potensi keuntungan dan ancaman yang mungkin muncul. Tujuan penelitian ini adalah untuk mengeksplorasi manfaat yang dihasilkan dari penggunaan AI dalam mendeteksi ancaman siber serta mengidentifikasi jenis-jenis serangan siber yang paling signifikan. Metode yang digunakan adalah Systematic Literature Review (SLR), dengan meninjau 39 paper yang diterbitkan antara tahun 2020 hingga 2024. Orisinalitas penelitian ini terletak pada analisis mendalam terkait potensi keuntungan dan risiko ancaman penggunaan AI dalam keamanan siber. Hasil penelitian ini menegaskan bahwa AI mampu meningkatkan efisiensi dan efektivitas deteksi ancaman siber. Penelitian ini diharapkan dapat memberikan wawasan baru tentang dinamika keamanan siber dan membuka peluang untuk pengembangan penelitian lebih lanjut.

Kata Kunci: kecerdasan buatan, keamanan siber, teknologi

ABSTRACT

Artificial Intelligence (AI) is now widely used in cybersecurity to detect threats while maximizing its benefits. The rapid transformation of technology makes cybersecurity a critical issue that needs to be anticipated in today's digital era. In this research, a comprehensive study is conducted on the impact of using AI in cybersecurity, especially on the potential benefits and threats that may arise. The purpose of this research is to explore the benefits resulting from the use of AI in detecting cyber threats and identify the most significant types of cyber attacks. The method used is Systematic Literature Review (SLR), by reviewing 39 papers published between 2020 and 2024. The originality of this research lies in the in-depth analysis of the potential benefits and risks of AI threats in cybersecurity. The results of this study confirm that AI can improve the efficiency and effectiveness of cyber threat detection. This research is expected to provide new insights into the dynamics of cybersecurity and open up opportunities for further research development.

Keywords: *Artificial Intelligence, Cyber Security, Technology*

PENDAHULUAN

Keamanan siber telah menjadi salah satu isu kritis yang semakin relevan di era digitalisasi dan transformasi teknologi yang pesat. Pertumbuhan konektivitas internet serta adopsi berbagai teknologi canggih dalam kehidupan sehari-hari, baik dalam sektor bisnis, pemerintahan, maupun personal, telah meningkatkan risiko terhadap keamanan data dan sistem informasi. Serangan siber yang semakin kompleks dan canggih menuntut adanya solusi keamanan yang mampu merespon ancaman-ancaman baru yang terus berkembang. Metode tradisional dalam

menjaga keamanan siber sering kali tidak lagi memadai untuk mengatasi serangan baru, seperti malware yang lebih kompleks, Distributed Denial of Service (DDoS), dan serangan berbasis kecerdasan buatan (AI). Di sinilah kecerdasan buatan (AI) menawarkan solusi potensial dengan kemampuannya memproses data dalam jumlah besar secara cepat, mengenali pola, serta memprediksi ancaman yang mungkin tidak terdeteksi oleh metode konvensional.

AI telah diterapkan dalam berbagai skenario keamanan siber, mulai dari sistem deteksi intrusi (Intrusion Detection Systems/IDS), deteksi malware, pencegahan serangan DDoS, hingga analisis perilaku pengguna yang mencurigakan. Keunggulan AI dalam mengolah big data dan melakukan pembelajaran otomatis (machine learning) membuatnya semakin diminati oleh para peneliti dan praktisi keamanan siber sebagai alat yang efektif dalam mendeteksi, mencegah, dan merespons berbagai ancaman. Namun, meskipun AI memiliki potensi besar, implementasinya dalam keamanan siber tidak lepas dari tantangan. Serangan siber terus berkembang, dan taktik yang digunakan oleh para pelaku kejahatan siber semakin canggih. Selain itu, teknik AI yang ada saat ini belum tentu efektif dalam menghadapi semua jenis serangan, sehingga diperlukan penelitian yang lebih dalam untuk memetakan metode AI yang paling sesuai untuk menghadapi setiap jenis ancaman.

Salah satu tantangan dalam penerapan AI pada keamanan siber adalah adanya ancaman berupa serangan yang juga menggunakan kecerdasan buatan, yang dikenal sebagai adversarial attacks. Dalam konteks ini, model AI dapat dimanipulasi oleh serangan yang dirancang khusus untuk mengecoh sistem deteksi yang telah dibangun (Nazir et al., 2020). Oleh karena itu, penting bagi penelitian lebih lanjut untuk tidak hanya mengembangkan teknik AI yang lebih kuat, tetapi juga mempertimbangkan potensi ancaman dari penggunaan AI oleh pihak yang berniat jahat.

Penelitian ini bertujuan untuk mengeksplorasi dan memetakan teknik-teknik kecerdasan buatan yang digunakan dalam keamanan siber, serta mengkaji kekuatan dan kelemahan masing-masing metode dalam menghadapi ancaman siber tertentu. Metode yang digunakan dalam penelitian ini adalah Systematic Literature Review (SLR), di mana peneliti akan mengumpulkan, mengevaluasi, dan mensintesis literatur yang relevan dengan topik keamanan siber berbasis AI. Tujuan dari pendekatan ini adalah untuk mengidentifikasi tren, temuan utama, serta celah dalam penelitian yang ada, yang dapat dijadikan dasar untuk pengembangan lebih lanjut. Penelitian ini juga bertujuan untuk mengatasi beberapa kekurangan dalam penelitian sebelumnya, yang cenderung membahas secara terpisah antara jenis serangan siber, metode AI yang digunakan, serta dataset yang mendukung. Dengan adanya sintesis yang komprehensif, diharapkan penelitian ini dapat memberikan pandangan yang lebih mendalam dan strategis mengenai peran AI dalam memperkuat keamanan siber di masa kini dan masa mendatang.

Hasil dari penelitian ini diharapkan dapat menjadi acuan bagi peneliti dan praktisi dalam memilih metode AI yang paling sesuai untuk kategori serangan siber tertentu, serta membantu mengembangkan solusi keamanan yang lebih efektif. Di samping itu, penelitian ini diharapkan dapat berkontribusi dalam meningkatkan keamanan informasi dan menjaga stabilitas sistem informasi dari berbagai ancaman siber yang terus berkembang.

Berajah Journal
Jurnal Pembelajaran dan Pengembangan Diri
ISSN (p): **2797-1805** | ISSN (e): **2797-1082**

TINJAUAN PUSTAKA

Cyber Crime

Cybercrime mencakup berbagai aktivitas ilegal yang dilakukan melalui teknologi digital, termasuk hacking, pencurian identitas, dan distribusi malware. Masalah utama dalam menangani cybercrime adalah perbedaan definisi dan kerangka hukum antar negara, yang sering kali menghambat kerja sama internasional. (Phillips et al., 2022).

Cyber Security/keamanan siber

Keamanan siber merupakan bidang penting yang bertujuan melindungi sistem informasi dari ancaman seperti akses tidak sah, kerusakan, dan eksploitasi. Berdasarkan kerangka kerja NIST, keamanan siber mencakup 5 fungsi utama dan 23 solusi. Fungsi-fungsi ini memberikan panduan strategis untuk meningkatkan perlindungan terhadap ancaman siber. Kategori solusi yang digunakan untuk mengidentifikasi kasus penggunaan AI dalam meningkatkan keamanan siber. (R. Kaur, 2023).

Malware

Malware adalah perangkat lunak berbahaya seperti virus, worm, Trojan, rootkit, dan ransomware, yang dirancang untuk merusak sistem, mencuri data, atau menjalankan kode jarak jauh pada mesin korban (Aslan & Samet, 2020). Kompleksitasnya meningkat karena beberapa malware kini dapat memiliki karakteristik dari berbagai kelas, membuat klasifikasi dan deteksi semakin menantang.

Artificial Intelligence

Kecerdasan buatan merupakan cabang ilmu komputer yang bertujuan untuk mengembangkan sistem dan mesin yang mampu melakukan tugas yang biasanya dikerjakan oleh manusia. Kecerdasan buatan dalam bahasa asing adalah Artificial intelligence dimana mempunyai arti "intelligence" dari bahasa Latin "intelligo" yang mempunyai arti "saya paham". Sehingga arti intelligence adalah suatu kehandalan dalam melaksanakan aksi. Artificial Intelligence (AI) atau Kecerdasan Buatan adalah teknologi berbasis sistem komputer yang memungkinkan memiliki kemampuan untuk melakukan kegiatan manusia yang membutuhkan intelegensi (Healey, 2020)

Machine learning

Machine learning merupakan cabang dari kecerdasan buatan (AI) dan ilmu komputer yang berfokus pada penggunaan data dan algoritma untuk meniru bagaimana cara manusia belajar secara bertahap untuk meningkatkan akurasinya. Dalam hal ini, mesin akan melakukan pendekatan untuk membangun sebuah sistem AI yang mampu mempelajari pola dan hubungan dalam data menggunakan pola tersebut untuk membuat prediksi (Arankalle et al., 2020; Darapureddy et al., 2021; Pulipaka, 2021). Proses pembelajaran dilakukan dari contoh dan pengalaman, dimana manusia tidak perlu memberikan aturan atau instruksi detail secara langsung.

DDoS

Saat ini serangan DDoS (Distributed Denial of Service) termasuk salah satu ancaman terbesar di dunia keamanan siber (Rahman et al.,2024). DDoS adalah Serangan siber yang membanjiri server, jaringan, atau layanan dengan lalu lintas berlebih dari banyak sumber, sehingga membuatnya tidak dapat diakses oleh pengguna normal.

Diketahui bahwa Serangan Distributed Denial of Service (DDoS) semakin tahun ke tahun menjadi ancaman yang serius dalam infrastruktur jaringan dan sistem dalam lingkungan teknologi informasi(Hansen et al.,2023)

Intrusion Detection Systems/IDS

Intrusion Detection Systems (IDS) adalah kombinasi perangkat keras dan perangkat lunak yang memonitor aktivitas jaringan atau host untuk mendeteksi aktivitas mencurigakan, melaporkannya kepada administrator, dan membantu melindungi dari ancaman keamanan internal maupun eksternal. IDS bersifat dinamis, berbeda dari firewall yang hanya memblokir lalu lintas tertentu(Abdulganiyu et al.,2023)

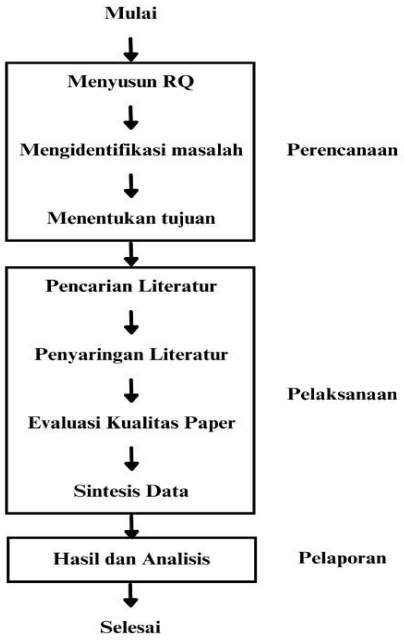
Deep Learning

Deep learning, cabang dari pembelajaran mesin, memungkinkan komputer belajar langsung dari data tanpa memerlukan ekstraksi fitur manual, dengan menggunakan arsitektur jaringan saraf tiruan yang terinspirasi oleh otak manusia dan terdiri dari banyak lapisan tersembunyi (MathWorks, 2024). Teknologi ini menggunakan data besar berlabel untuk melatih jaringan dan mencapai akurasi tinggi dalam tugas seperti klasifikasi dan regresi. (Agarap, 2018).

METODE

Penelitian ini dilakukan dengan menggunakan metode Systematic Literature Review (SLR) dengan menggunakan beberapa tahap. Tahap penelitian SLR yang akan digunakan terdiri dari tahap perencanaan, pelaksanaan, dan pelaporan. Metode ini dipilih bertujuan untuk meneliti secara sistematis mengumpulkan, mengevaluasi, dan mensintesis literatur yang relevan terhadap penggunaan Artificial Intelligence (AI) dalam Cyber Security. Melalui metode ini diharapkan dapat mengevaluasi potensi keuntungan dan ancaman dari penggunaannya.

Pada tahap perencanaan dimulai proses penyusunan research question (RQ) untuk mengidentifikasi permasalahan apa yang terjadi sehingga menghasilkan tujuan dan manfaat pentingnya penelitian ini. Setelah mengetahui rumusan masalah maka akan dilanjut ke tahap pelaksanaan yaitu mengumpulkan paper dan mengevaluasi kualitas dari paper tersebut untuk melakukan sintesis data berdasarkan paper yang terpilih. Tahap pelaporan menjadi penutup dalam tahap SLR yaitu memberikan hasil literature review yang mencakup hasil dan pembahasan dari analisis paper, gambaran umum studi, dan jawaban dari setiap research question



Gambar 1. Tahap pelaksanaan SLR

Research Question SLR

No	Research Question
1.	Apa saja jenis-jenis serangan siber yang bersifat teknis dan memiliki

Berajah Journal
Jurnal Pembelajaran dan Pengembangan Diri
ISSN (p): **2797-1805** | ISSN (e): **2797-1082**

	frekuensi tinggi, lalu bagaimana relevansi data yang tersedia dalam mendukung deteksi ancaman siber menggunakan AI, menurut penelitian yang ada?
2.	Apakah AI memiliki dampak signifikan dalam meningkatkan kecepatan, akurasi, dan efektivitas deteksi ancaman siber?
3.	Apakah penerapan AI dalam deteksi ancaman siber lebih memberikan manfaat terhadap keamanan siber atau justru menciptakan potensi risiko baru terhadap sistem keamanan?

HASIL DAN PEMBAHASAN

Serangan siber dapat dibagi menjadi dua yaitu serangan siber bersifat teknis dan serangan siber bersifat sosial. Serangan siber bersifat teknis merupakan serangan yang langsung menargetkan infrastruktur teknis seperti jaringan, perangkat lunak, atau sistem komputer. Jadi fokus dari serangan teknis ini pada manipulasi atau penghancuran teknologi tanpa interaksi langsung dengan manusia. Jenis - jenis serangan siber yang termasuk ke dalam serangan siber bersifat teknis: a) serangan malware yang bertujuan untuk merusak, mencuri, atau mengenkripsi data dan sering kali meminta uang tebusan untuk pemulihan. Serangan malware meliputi Ransomware, Virus, Worm dan Trojan. b) Serangan Ddos Dengan jenis ancaman Distributed Denial of Service (DDoS) yang berupaya melumpuhkan layanan online dengan membanjiri server dengan lalu lintas yang sangat tinggi. Berbeda dengan serangan siber yang bersifat teknis, serangan siber bersifat sosial menggunakan pendekatan sosial dengan memanipulasi pengguna untuk mendapatkan akses atau informasi. Jadi fokusnya pada manipulasi manusia untuk mendapatkan akses atau informasi yang seharusnya bersifat rahasia. Phishing merupakan salah satu jenis serangan siber bersifat sosial yang berupaya mencuri informasi sensitif dengan menipu pengguna agar memberikan informasi pribadi melalui email atau situs web palsu.

Terdapat 2 kategori serangan siber Internet of Things (IoT) yaitu serangan siber perangkat lunak dan serangan siber pada jaringan. Beberapa yang termasuk serangan siber dalam hal serangan perangkat lunak yaitu injeksi kode, butter overflow, malware, dan side channel attack. Sedangkan serangan jaringan meliputi man in the middle, DoS, DDoS, dan serangan RPL(Mohd Yusof & Sulaiman, 2022). Serangan siber yang secara umum yaitu DoS, user to root(U2R), dan remote to local(R2L) (Barik et al., 2022). erangan siber meliputi serangan aplikasi protokol, serangan terhadap ML dan analisis data, serangan injeksi, serangan time delay, spoofing, ransomware, DDos(de Azambuja et al., 2023).

Melalui pencarian yang sistematis, penulis telah mengidentifikasi sekitar 39 paper yang secara spesifik membahas topik ini. Kriteria pencarian yang digunakan mencakup tahun publikasi, kata kunci yang relevan, serta metodologi yang diterapkan dalam masing-masing penelitian. Hasil analisis menunjukkan bahwa banyak studi telah menggunakan berbagai dataset untuk melatih model AI dalam mendeteksi berbagai jenis ancaman siber, seperti malware, phishing, dan serangan DDoS. Selain itu, banyak paper tersebut juga mengeksplorasi teknik dan algoritma yang efektif, termasuk metode machine learning dan deep learning, serta mengidentifikasi tantangan yang

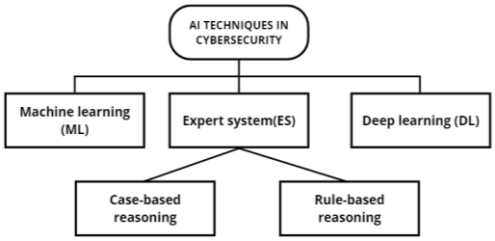
dihadapi dalam implementasi AI di bidang keamanan siber. Berdasarkan temuan ini, dapat disimpulkan bahwa sudah ada kumpulan data yang cukup dan relevan untuk mendukung penelitian dalam mendeteksi ancaman siber menggunakan AI. Meskipun demikian, masih terdapat ruang untuk penelitian lebih lanjut dalam menganalisis kekurangan dan tantangan yang ada, serta optimalisasi penggunaan dataset yang ada untuk pengembangan teknik deteksi yang lebih efektif.

Berdasarkan penelitian sebelumnya dari hasil Systematic Literature Review terhadap 39 paper menunjukkan bahwa AI memberikan dampak yang sangat signifikan dalam mendeteksi ancaman siber. Dengan kemampuan untuk mengolah data dalam skala besar. AI mampu mengidentifikasi pola dan anomali yang menunjukkan adanya potensi ancaman dengan lebih cepat dan akurat dibandingkan metode tradisional.

Menurut penelitian (Katanosh dan Brajendra., 2020) AI dapat bekerja dengan tiga cara:

a) Kecerdasan terbantu, yang meningkatkan apa yang sudah dilakukan manusia
b) Kecerdasan tambahan, yang memberdayakan manusia untuk melakukan hal-hal yang tidak dapat mereka lakukan
c) Kecerdasan otonom, yang merupakan fitur mesin yang bertindak sendiri

Dalam mendeteksi keamanan siber menggunakan AI diperlukannya aplikasi yang akurat untuk mendapatkan bukti yang kuat.



Gambar 2. Aplikasi AI dalam keamanan cyber

AI terbukti memberikan dampak signifikan dalam mendeteksi ancaman cyber berdasarkan hasil SLR yang diperoleh yaitu:

1. Otomatisasi dan kecepatan deteksi : AI mampu menggantikan sistem tradisional yang lambat
2. Pemodelan prediktif: AI dapat memprediksi pola serangan berdasarkan analisis pola masa lalu
3. Pengelolaan big data: AI mampu menganalisis data dalam jumlah besar yang tidak bisa dilakukan secara manual

Tabel 1 menunjukkan teknologi/metode yang digunakan dalam mendeteksi dampak AI pada serangan siber yang dijelaskan dalam penelitian (Katanosh dan Brajendra., 2020)

Tabel 1. Analisis Penerapan Teknik AI dalam Keamanan Siber

Aspek	Teknologi/Metode
Otomatisasi dan kecepatan deteksi	Intrusion Detection Systems (IDS)
Pemodelan prediktif	Support Vector Machine (SVM)
Pengelolaan big data	Indicators of Compromise (IOC)

Pemanfaatan AI dalam keamanan siber dapat menawarkan beberapa kelebihan yang signifikan. Namun, ada beberapa kelemahan yang harus dipertimbangkan dalam pemanfaatan AI untuk keamanan siber.

Tabel 2. Hasil Analisis kelebihan pemanfaatan AI dalam Cyber Security

Kelebihan
Meningkatnya tingkat deteksi ancaman

cyber dengan menggunakan teknologi AI dengan pendekatan machine learning dan deep learning,
AI tidak hanya meningkatkan keamanan secara keseluruhan tetapi juga mengurangi risiko dan biaya yang terkait dengan pelanggaran keamanan dan kehilangan data.
Respon AI yang lebih akurat dan efisien dengan memanfaatkan kemampuan untuk melakukan analisis secara real-time terhadap data, sistem AI dapat merespons serangan dengan sangat cepat, sering kali dalam hitungan detik setelah ancaman terdeteksi.
AI dapat membantu pengawasan untuk mengidentifikasi pola aktivitas normal dan abnormal yang terjadi sebagai deteksi dini terhadap serangan siber.
AI memungkinkan tim keamanan untuk fokus pada ancaman yang benar-benar signifikan dan mengalokasikan sumber daya dengan lebih efisien

Tabel 3. Hasil Analisis Kekurangan pemanfaatan AI dalam Cyber Security

Kekurangan
Adanya tantangan dalam pengumpulan dan analisis data yang diperlukan untuk melatih model AI dengan akurat karena pada proses ini memerlukan data yang berkualitas tinggi dan beragam
Biaya tinggi untuk pengembangan dan implementasi teknologi AI juga menjadi kendala yang signifikan.
Pemanfaatan AI dalam mendeteksi serangan kejahatan siber juga berpotensi untuk meningkatkan pengumpulan dan analisis data yang sensitif.
Ancaman terhadap privasi pengguna dan karyawan, terutama dalam hal penggunaan data pribadi untuk tujuan keamanan.

Selain kelebihan dan kekurangan terdapat data kuantitatif yang berasal dari sampel beberapa perusahaan yang memanfaatkan AI dalam Cyber Security.

Tabel 4. data sampel deskriptif kuantitatif dalam mengimplementasikan Artificial Intelligence dalam meningkatkan Cyber Security.

Tahun	**Perusahaan yang menggunakan AI**	**Serangan yang terdeteksi**
2021	55%	70%
2022	68%	75%
2023	80%	82%

Data dari Tabel 4 Hasil penelitian (Lim Jong Su dan Binastya Anggara., 2024) menunjukkan bahwa implementasi Artificial Intelligence (AI) dalam meningkatkan cybersecurity semakin signifikan. Temuan mereka sejalan dengan tren global yang menunjukkan potensi besar AI dalam mendeteksi dan mencegah ancaman siber

Tabel 5. Kepuasan Pengguna Terhadap Sistem Keamanan Berbasis AI

Tahun	Kepuasan Pengguna	Penggunaan AI
2021	75%	55%
2022	82%	68%
2023	88%	80%

Dari data Tabel 5 Hasil penelitian (Lim Jong Su dan Binastya Anggara., 2024) menunjukkan tingkat kepuasan pengguna terhadap sistem keamanan siber berbasis AI dari tahun 2020 hingga 2023. Dari data tersebut menunjukkan peningkatan yang signifikan tiap tahun terhadap kepuasan pengguna terhadap pemanfaatan sistem keamanan berbasis AI.

Meskipun penerapan AI dalam mendeteksi ancaman siber menawarkan banyak manfaat yang signifikan, seperti peningkatan kecepatan dan akurasi deteksi serta respons otomatis, AI juga dapat menciptakan potensi risiko baru.
Kompleksitas teknologi AI sering kali membuat sistem ini sulit untuk diinterpretasi dan diandalkan sepenuhnya. Keterbatasan interpretasi dan kebutuhan data besar yang harus aman dan terlindungi juga menambah risiko.

Tabel 6. Analisis Manfaat dan Risiko AI dalam ancaman siber

Aspek	**Manfaat AI**	**Potensi Risiko AI**
Deteksi anomali	IDS dan monitoring real time yang otomatis	False positives dapat menyebabkan alarm berlebihan
Analisis prediktif	AI memprediksi dan mencegah serangan di awal	Risiko manipulasi data input yang mempengaruhi AI
Monito-ring real-time	Monitoring jaringan selama 24/7	Memerlukan infrastruktur dan biaya yang besar
Kapasi-tas data	Mampu menganalisis data dalam skala besar secara efisien	Meningkatkan kompleksitas yang bisa dieksploitasi oleh peretas

SIMPULAN

Hasil dari RQ1 menunjukkan bahwa serangan siber dapat dikategorikan menjadi serangan teknis dan sosial, dengan jenis ancaman seperti malware, DDoS, phishing, serta serangan terhadap perangkat IoT. Selain itu, telah diidentifikasi bahwa tersedia kumpulan data yang cukup untuk mendukung deteksi ancaman siber menggunakan AI. Namun, masih terdapat tantangan dalam optimalisasi data, terutama dalam hal keragaman, kualitas, dan relevansi untuk berbagai skenario serangan.

Berdasarkan hasil analisis RQ2, AI memiliki dampak signifikan dalam mendeteksi ancaman siber. Dengan kemampuan otomatisasi, kecepatan deteksi, dan prediksi pola serangan, AI mampu menganalisis data dalam jumlah besar dengan akurasi yang tinggi. Keunggulan ini menjadikan AI sebagai alat penting untuk meningkatkan efektivitas dan efisiensi dalam mitigasi ancaman siber.

Hasil dari RQ3 menunjukkan bahwa penerapan AI dalam keamanan siber memberikan manfaat besar, terutama dalam meningkatkan kemampuan deteksi ancaman secara real-time. Namun, penerapan ini juga menghadirkan risiko baru, seperti kemungkinan kesalahan deteksi, manipulasi data input yang mempengaruhi keputusan AI, peningkatan kompleksitas sistem yang dapat menjadi target serangan, serta biaya pengembangan dan implementasi yang besar. Oleh karena itu, penting untuk menyeimbangkan manfaat dan risiko dengan menerapkan metode mitigasi yang tepat.

Secara keseluruhan, penelitian ini menegaskan bahwa AI mampu meningkatkan efisiensi dan efektivitas deteksi ancaman siber. Namun, penelitian lebih lanjut diperlukan untuk mengatasi tantangan seperti kualitas dataset, privasi pengguna, serta potensi eksploitasi kerentanan pada sistem berbasis AI. Penelitian mendalam juga disarankan untuk mengeksplorasi kelemahan dan potensi risiko dari penerapan AI, dengan fokus pada pengembangan metode yang lebih aman dan andal untuk sistem keamanan siber di masa depan.

DAFTAR PUSTAKA

Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). International Journal of Information Security, 22(5). https://doi.org/10.1007/s10207-023-00682-2

Anastasya Zalsabilla Hermawan, M. Novianto Anggoro, Ditha Lozera, & Asif Faroqi. (2023). STUDI LITERATUR: ANCAMAN SERANGAN SIBER ARTIFICIAL INTELLIGENCE (AI) TERHADAP KEAMANAN DATA DI INDONESIA. Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, 3(1). https://doi.org/10.33005/sitasi.v3i1.363

Aslam, M. (2024). AI and Cybersecurity: An Ever-Evolving Landscape. In International Journal of Advanced Engineering Technologies and Innovations (Vol. 01).

Azhar, I., & Sr, M. (2020). Artificial Intelligence for Cybersecurity: a Systematic Mapping of Literature. International Journal of Innovations in Engineering Research and Technology [Ijiert], 7(9), 172–176.

Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. Journal of Information Security, 15(02), 245–278. https://doi.org/10.4236/jis.2024.152015

Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications, 13(5). https://doi.org/10.5121/ijsea.2022.13502

Dan, T., Masa, P., Simanjuntak, E. N., Irmayani, D., & Nasution, F. A. (2024). Tinjauan Penerapan Kecerdasan Buatan Dalam Keamanan Jaringan. 7(September), 370–375.

de Azambuja, A. J. G., Giese, T., Schützer, K., Anderl, R., Schleich, B., & Rosa Almeida, V. (2024). Digital Twins in

Industry 4.0 – Opportunities and challenges related to Cyber Security. Procedia CIRP, 121. https://doi.org/10.1016/j.procir.2023.09.225

Fitria, E. Y., & Mutijarsa, K. (2023). Survei Penelitian Metode Kecerdasan Buatan untuk Mendeteksi Ancaman Teknologi Serangan Siber. Jurnal Teknologi Informasi Dan Ilmu Komputer, 10(6). https://doi.org/10.25126/jtiik.1067341

Gustina DM, V., & Ananda, A. (2024). Kecerdasan Buatan untuk Security Orchestration, Automation and Response: Tinjauan Cakupan. Jurnal Komputer Terapan, 10(1), 36–47. https://doi.org/10.35143/jkt.v10i1.6247

Hansen, J., & Sutabri, T. (2023). Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha. Digital Transformation Technology, 3(1), 289–298.

Jonas, D., Aprila Yusuf, N., & Rahmania Az Zahra, A. (2023). Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity. International Transactions on Education Technology (ITEE), 2(1). https://doi.org/10.33050/itee.v2i1.428

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97. https://doi.org/10.1016/j.inffus.2023.101804

Keamanan, A., & Sosial, J. (2024). Technology Sciences Insights Journal. d, 0–3.

Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020). AI in cybersecurity education-a systematic literature review of studies on cybersecurity moocs. Proceedings - IEEE 20th International Conference on Advanced Learning Technologies, ICALT 2020. https://doi.org/10.1109/ICALT49669.2020.00009

Lazic, L. (2019). Benefit From AI in Cybersecurity. The 11th International Conference on Business Information Security, Belgrade, Serbia, October.

Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex and Intelligent Systems, 8(2). https://doi.org/10.1007/s40747-021-00494-8

Nyale, D., & Angolo, S. M. (2022). A Survey of Artificial Intelligence in Cyber Security. International Journal of Computer Applications Technology and Research. https://doi.org/10.7753/ijcatr1112.1014

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Raimundo, R., & Rosário, A. (2021). The impact of artificial intelligence on data system security: A literature review. In Sensors (Vol. 21, Issue 21). https://doi.org/10.3390/s21217029

Rawat, D. B., Doku, R., & Garuba, M. (2021). Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. IEEE Transactions on Services Computing, 14(6), 2055–2072. https://doi.org/10.1109/TSC.2019.2907247

Rjoub, G., Bentahar, J., Abdel Wahab, O., Mizouni, R., Song, A., Cohen, R., Otrok, H., & Mourad, A. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. IEEE Transactions on Network and Service Management, 20(4). https://doi.org/10.1109/TNSM.2023.3282740

Sarker, I. H. (2021). Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. SN Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00535-6

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1). https://doi.org/10.1186/s40537-020-00318-5

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. In SN Computer Science (Vol. 2, Issue 3). https://doi.org/10.1007/s42979-021-00557-0

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space. IEEE Access, 12(April), 53497–53516. https://doi.org/10.1109/ACCESS.2024.3385107

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. In Journal of Big Data (Vol. 11, Issue 1). Springer International Publishing. https://doi.org/10.1186/s40537-024-00957-y

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access, 8. https://doi.org/10.1109/ACCESS.2020.3041951

Sinaga, N. H., Irmayani, D., Nirmala, M., & Hasibuan, S. (2024). Mengoptimalkan Keamanan Jaringan: Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman. 7(September), 364–369.

Sutarti, & Khairunnisa. (2017). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial of Service) Berbasis Honeypot. Jurnal PROSISKO, 4(2), 8.

Sutabri, T., & Hansen, J. (2023). Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha. Digital Transformation Technology, 3(1), 289–298.

Weng, Y., & Wu, J. (2024). Journal of Artificial Intelligence General Science (JAIGS) Leveraging Artificial Intelligence to Enhance Data Security

and Combat Cyber Attacks Keywords: Artificial Intelligence, National Security, Data Security, Data Privacy, Cybersecurity, 5(1).

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access, 8. https://doi.org/10.1109/ACCESS.2020.3013145

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 55(2). https://doi.org/10.1007/s10462-021-09976-0