PROSIDING Seminar Nasional SISFOTEK ISSN 2597-3584 (Media Online)
Sistem Informasi dan Teknologi
website : www.seminar.iaii.or.id | email : seminar@iaii.or.id

Implementasi Artificial Intelligence dalam Meningkatkan Cyber Security: Analisis ancaman dan Pencegahan

Lim Jong Su[1*], Binastya Anggara Sekti[2]
[1,2]Sistem Informasi, Ilmu Komputer, Universitas Esa Unggul, Tangerang, Indonesia
[1]limjongsu68@gmail.com

Abstract

In today's digital age, cyber threats are becoming more complex and sophisticated.The aim of this study is to analyze the role of artificial intelligence (AI) in improving cybersecurity through threat detection and prevention. By integrating AI techniques such as machine learning and deep learning, cybersecurity systems can detect suspicious behavior patterns and identify threats in real-time.A comprehensive literature review was conducted to explore different AI approaches applied in this field, including anomaly detection analytics, threat intelligence, and automated response. The use of artificial intelligence can significantly improve the accuracy of threat detection and cyber incident response. Moreover, case studies of several organizations that have used AI for cybersecurity have shown increased effectiveness and efficiency in dealing with cyberattacks. However, there are still challenges to overcome, such as: B. Limited training data, interpretability of AI models, and the need for qualified experts. Although AI has great potential to improve cybersecurity, collaboration between technology and human expertise remains crucial to address growing threats.Thus, not only is cybersecurity improving, but there is also an increasing need to develop artificial intelligence (AI) systems that take cybersecurity threats into account in order to attack the security of information systems.

Keywords: *artificial intelligence, threats, cyber security, information systems, threat intelligence*

Abstrak

Di era yang semakin terdigitalisasi saat ini, ancaman siber menjadi semakin kompleks dan canggih. Tujuan dari penelitian ini adalah untuk menganalisis peran kecerdasan buatan (AI) dalam meningkatkan keamanan siber melalui deteksi dan pencegahan ancaman. Dengan mengintegrasikan teknik AI seperti pembelajaran mesin dan pembelajaran mendalam, sistem keamanan siber dapat mendeteksi pola perilaku mencurigakan dan mengidentifikasi ancaman secara real-time. Tinjauan literatur yang komprehensif dilakukan untuk mengeksplorasi berbagai pendekatan AI yang diterapkan di bidang ini, termasuk analisis deteksi anomali, intelijen ancaman, dan respons otomatis. Dengan menerapan kecerdasan buatan dapat meningkatkan akurasi deteksi ancaman dan respons terhadap insiden dunia maya secara signifikan. Selain itu, studi kasus di beberapa organisasi yang telah menggunakan AI untuk keamanan siber telah menunjukkan peningkatan efektivitas dan efisiensi dalam menangani serangan siber. Namun demikian, tantangan-tantangan yang masih perlu diatasi, seperti keterbatasan data pelatihan, kemampuan interpretasi model AI, dan kebutuhan akan tenaga ahli yang berkualifikasi. meskipun AI memiliki potensi besar untuk meningkatkan keamanan siber, kolaborasi antara teknologi dan keahlian manusia tetap penting untuk mengatasi ancaman yang terus berkembang Maka dari itu, tidak hanya keamanan siber yang ditingkatkan keamanannya melainkan sistem kecerdasan buatan (AI) ini juga perlu dikembangkan mengingat ancaman keamanan siber yang terus berkembang untuk menyerang keamanan sistem informasi.

Kata kunci: kecerdasan buatan, ancaman , keamanan siber, sistem informasi, intelijen ancaman

1. Pendahuluan

Beberapa perusahaan teknologi terkemuka telah menerapkan AI ke dalam sistem keamanan siber mereka dengan sukses besar. Misalnya, Google menggunakan AI untuk mendeteksi dan memblokir serangan phishing di Gmail, dan IBM menggunakan Watson untuk menganalisis ancaman keamanan dalam skala besar.

Keamanan sistem informasi merupakan salah satu faktor yang sangat penting dalam perkembangan teknologi informasi di era saat ini. Di era ini, melalui pemanfaatan teknologi seperti Internet of Things (IoT), kecerdasan buatan (AI), dan robot, kehidupan masyarakat dapat ditingkatkan dengan memobilisasi potensi

produktivitasnya dan memberikan kemudahan bagi kehidupan manusia.

Penggunaan Internet terjadi hampir di setiap bidang kehidupan manusia, termasuk industri, teknologi, pemasaran, dan pendidikan. Perkembangan teknologi informasi juga telah mengubah gaya hidup masyarakat. Sebelumnya, masyarakat hanya berfokus pada lingkungan lokal, namun kini mereka beralih ke kehidupan global dimana segala sesuatu dapat dilakukan di dunia maya[1].

Cyber Security adalah keamanan catatan/statistik, properti, layanan, dan sistem biaya untuk mengurangi kemungkinan kehilangan, kerusakan/korupsi, kompromi, atau penyalahgunaan ke tahap yang sepadan dengan biaya yang dibebankan. Ketika struktur pembagian waktu muncul pada pertengahan hingga akhir tahun 1960-an dan lebih dari satu pekerjaan dan pengguna dapat berjalan pada waktu yang sama, mengendalikan akses ke fakta-fakta dalam sistem menjadi poin utama dari subjek tersebut [2].

Artificial Intelligence dalam Cyber Security bermanfaat karena meningkatkan cara profesional keamanan menyelidiki, menganalisis, dan memahami kejahatan siber. Hal ini melengkapi teknologi keamanan siber yang digunakan bisnis untuk melawan penjahat siber dan membantu menjaga keamanan tim dan pelanggan dari bisnis itu sendiri. Di sisi lain, kecerdasan buatan juga bisa sangat bermanfaat. Meskipun tidak berguna di semua aplikasi, teknologi ini juga dapat berfungsi sebagai gudang senjata bagi penjahat dunia maya yang menggunakan teknologi ini untuk menyempurnakan dan meningkatkan serangan siber mereka[3].

Kecerdasan buatan (AI) telah menjadi sebuah inovasi teknologi yang menawarkan potensi besar di berbagai bidang, termasuk keamanan siber. AI dapat menganalisis data dalam jumlah besar dengan cepat dan akurat, memungkinkan Anda mendeteksi pola mencurigakan, mengidentifikasi ancaman yang sebelumnya tidak diketahui, dan merespons insiden keamanan dengan lebih efisien dibandingkan metode tradisional.

Penerapan AI dalam keamanan siber mencakup berbagai teknik dan pendekatan, termasuk pembelajaran mesin, pembelajaran mendalam, dan analisis prediktif. Teknologi ini memungkinkan pengembangan sistem keamanan yang lebih proaktif dan adaptif yang tidak hanya dapat mendeteksi dan merespons ancaman secara real time, namun juga memprediksi dan mencegah serangan di masa depan.

Namun, meskipun AI memiliki potensi besar untuk meningkatkan keamanan siber, penerapannya juga memiliki tantangan. Salah satunya adalah risiko AI itu sendiri, seperti serangan terhadap sistem AI, data yang bias, dan ketergantungan yang berlebihan pada teknologi ini. Oleh karena itu, penting untuk melakukan analisis menyeluruh terhadap ancaman dan tindakan penanggulangannya sebagai bagian dari penerapan AI dalam keamanan siber[4].

Tujuan dari penelitian ini adalah untuk menganalisis ancaman Cyber Security yang telah terjadi di seluruh dunia seperti Ransomware, Malware, Phising, dll. Maka dari itu dilakukan pencegahan dari dampak terkena Cyber attack dengan menggunakan Artificial Intelligence Untuk meningkatkan Cyber Security yang lebih ketat keamanannya

Dari studi ini berupaya memberikan saran terhadap peningkatan dan pengembangan Cyber Security dengan menggunakan Artificial Intelligence (AI) yang lebih terjaga keamanannya dan juga berfokus mencegah pada macam-macam serangan siber yang akan terjadi kapan saja.

2. Metode Penelitian

Metode pada penelitian ini dirancang untuk menginvestigasi ancaman apa saja yang sering maupun jarang menyerang ke Cyber Security untuk mengetahui apakah tingkat keamanan siber ini tergolong lemah atau kuat. Untuk upaya mengatasi dan pencegahannya dengan menganalisis data historis serangan siber, mengidentifikasi pola dan anomali, serta mengimplementasi dan mengembangkan model AI untuk mendeteksi pencegahan ancaman secara real-time.

Latar belakang ancaman Cyber Security yang mencakup berbagai aktivitas jahat dengan mengeksploitasi kerentanan dalam sistem komputer, jaringan, dan perangkat lunak. Sifat ancaman yang terus berubah dan semakin kompleks ini memerlukan kewaspadaan yang berkelanjutan dan strategi pertahanan yang proaktif.

Metode yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif. Metode kuantitatif deskriptif merupakan pendekatan penelitian yang menggambarkan prosedur penelitian yang menghasilkan data berupa angka atau huruf yang mewakili objek yang diamati.

3. Hasil dan Pembahasan

Hampir semua perusahaan memberikan kerangka kerja untuk mengintegrasikan CPS yang cerdas dan fleksibel serta manufaktur adaptif, namun hal ini juga menimbulkan kekhawatiran tentang keamanan siber. Memang benar, munculnya perangkat IoT dan CPS dalam produksi yang terhubung meningkatkan permukaan serangan terhadap sistem dan infrastruktur penting, sehingga berdampak negatif pada proses produksi [5].

Tabel 1 adalah Tabel data sampel deskriptif kuantitatif dalam mengimplementasikan Artificial Intelligence dalam meningkatkan Cyber Security.

Tabel 1. Penggunaan AI dalam Deteksi Ancaman

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

Tabel 1 menunjukkan peningkatan penggunaan teknologi

AI oleh perusahaan untuk mendeteksi ancaman siber dari tahun 2020 hingga 2023. Persentase perusahaan yang menggunakan AI dalam deteksi ancaman meningkat secara signifikan dari 45% pada tahun 2020 menjadi 80% pada tahun 2023. Seiring dengan peningkatan ini, persentase serangan yang berhasil dideteksi oleh sistem berbasis AI juga meningkat dari 65% menjadi 82%.

Tabel 2. Efektivitas AI dalam Pencegahan Serangan

Tahun	Upaya pencegahan serangan	Serangan yang berhasil dicegah
2020	60%	55%
2021	70%	60%
2022	75%	68%
2023	85%	78%

Tabel 2 menggambarkan efektivitas AI dalam pencegahan serangan siber. Persentase upaya pencegahan serangan yang dilakukan oleh perusahaan meningkat dari 60% pada tahun 2020 menjadi 85% pada tahun 2023. Persentase serangan yang berhasil dicegah oleh sistem berbasis AI juga meningkat dari 55% menjadi 78% selama periode yang sama.

Tabel 3. Kepuasan Pengguna Terhadap Sistem Keamanan Berbasis AI

Tahun	Kepuasan Pengguna	Penggunaan AI
2020	70%	45%
2021	75%	55%
2022	82%	68%
2023	88%	80%

Tabel 3 menunjukkan tingkat kepuasan pengguna terhadap sistem keamanan siber berbasis AI dari tahun 2020 hingga 2023. Kepuasan pengguna meningkat dari 70% pada tahun 2020 menjadi 88% pada tahun 2023, seiring dengan peningkatan penggunaan AI dari 45% menjadi 80% pada periode yang sama.

Dengan data ini, dapat dilihat bagaimana AI telah meningkatkan deteksi dan pencegahan ancaman siber serta meningkatkan kepuasan pengguna terhadap sistem keamanan siber. Penelitian lebih lanjut dapat dilakukan untuk mengeksplorasi lebih dalam efektivitas AI dalam berbagai aspek keamanan siber.

3.1 Kelebihan dan Kekurangan AI untuk Keamanan Cyber

Penting untuk memahami berbagai serangan siber yang ada. Pakar keamanan siber sedang berupaya mengembangkan algoritme untuk menganalisis dan mengidentifikasi ancaman siber yang muncul. Seiring berkembangnya sistem AI, tindakan pencegahan terhadap teknik AI yang menipu bermunculan di dunia maya [6].

Dengan menerapkan teknik AI untuk melindungi ekosistem industri, sistem terus belajar dari upaya serangan. Hasilnya, sistem dapat memperoleh manfaat dari analisis prediktif untuk memerangi serangan siber yang kompleks. AI dapat membantu pengawasan untuk mengidentifikasi pola aktivitas normal dan abnormal yang bersifat ganas. Pemantauan memungkinkan serangan dimitigasi dan dilokalisasi. Teknologi AI tidak menjamin keamanan mutlak di lingkungan industri. Ada juga beberapa masalah etika dalam penerapannya, seperti kurangnya kode moral untuk mesin. Untuk keputusan yang mungkin mempunyai implikasi moral, AI mungkin tidak dapat mendeteksinya.

Oleh karena itu, ketidakmampuan untuk mengenali permasalahan moral dan mengambil keputusan dengan mempertimbangkan permasalahan tersebut merupakan sebuah tantangan[5].

Mengingat manfaat kecerdasan buatan dalam konteks keamanan siber, organisasi yang menggunakannya dapat memperoleh manfaat yang sangat besar. Misalnya, Siemens AG, pionir global dalam elektrifikasi, otomatisasi, dan digitalisasi, menggunakan Amazon Web Services (AWS) untuk menyediakan layanan yang cepat, berbasis AI, dan otonom. Kami telah menciptakan platform yang sangat tangguh. (CDC).

AI yang digunakan mampu memprediksi 60.000 kemungkinan serangan per satuan waktu. Dengan penerapan AI, kapasitas ini dapat dikelola oleh tim yang beranggotakan kurang dari 12 orang tanpa berdampak negatif pada kinerja sistem. AI dalam keamanan siber memungkinkan organisasi menganalisis dan menerapkan kembali pola ancaman masa lalu untuk mengidentifikasi risiko baru. Hal ini menghemat waktu dan tenaga dalam mengidentifikasi insiden, menyelidiki, dan memulihkan ancaman [7].

3.2 Analisis Ancaman dan pencegahan Menggunakan AI

AI dapat menganalisis data dalam jumlah besar dengan cepat dan akurat. AI dapat dilatih untuk mengenali pola normal dalam aktivitas jaringan dan mendeteksi aktivitas abnormal atau mencurigakan. Misalnya, algoritme pembelajaran mesin dapat digunakan untuk membedakan antara aktivitas jaringan normal dan serangan cyber.

AI menggunakan teknik pembelajaran mendalam untuk memantau dan menganalisis perilaku pengguna dan dapat mendeteksi perubahan yang mungkin mengindikasikan adanya ancaman. Contohnya termasuk login yang tidak biasa atau upaya mengakses data sensitif dari lokasi atau perangkat yang tidak diketahui.

AI dapat membantu analisis forensik digital dengan mempercepat proses mengidentifikasi dan menganalisis bukti digital setelah serangan. Algoritme AI memindai log aktivitas untuk mencari bukti serangan guna membantu pemulihan dan pengendalian lebih lanjut.

Selain analisis ancaman, AI juga dapat digunakan untuk pencegahan ancaman dalam beberapa cara.

AI dapat digunakan untuk mengembangkan sistem pencegahan intrusi yang lebih canggih. Sistem dapat mendeteksi tanda-tanda serangan yang akan datang dan mengambil langkah proaktif untuk mencegah akses tidak sah. Algoritme AI terus belajar dari ancaman yang muncul dan beradaptasi terhadap serangan, sehingga sistem

keamanan tetap selangkah lebih maju dari penyerang. Hal ini dapat dilakukan melalui pembaruan otomatis berdasarkan analisis data serangan terbaru. AI dapat mengotomatiskan banyak aspek respons insiden keamanan, termasuk: Contohnya termasuk mengisolasi sistem yang terinfeksi, memperbarui kebijakan keamanan,

dan berkomunikasi dengan tim keamanan. Otomatisasi ini meningkatkan waktu respons dan meminimalkan pemadaman listrik.

3.3 Jenis Ancaman serta analisis ancaman dan pencegahan dengan AI

Serangan Malware dengan jenis ancaman: Ransomware, Virus, Worm, Trojan.

Analisis ancaman: Serangan ini bertujuan untuk merusak, mencuri, atau mengenkripsi data dan Sering kali meminta uang tebusan untuk pemulihan.

Pencegahan dengan AI: AI dapat mendeteksi pola anomali yang mengindikasikan aktivitas malware, memperbarui basis data ancaman secara real-time, dan menggunakan machine learning untuk memprediksi dan mencegah serangan malware di masa depan.

Phising dengan Jenis ancaman: Email Phising, Spear Phising.

Analisis ancaman: Phishing berupaya mencuri informasi sensitif dengan menipu pengguna agar memberikan informasi pribadi melalui email atau situs web palsu.

Pencegahan dengan AI: AI menganalisis email untuk mencari pola yang mencurigakan, mendeteksi tautan dan lampiran berbahaya, dan menggunakan algoritme pembelajaran mesin untuk mendukung deteksi dan pencegahan phishing otomatis.

Serangan Ddos dengan jenis ancaman Distributed Denial of Service (DDoS).

Analisis ancaman: Serangan- serangan ini berupaya melumpuhkan layanan online dengan membanjiri server dengan lalu lintas yang sangat tinggi.

Pencegahan dengan AI: AI memantau dan menganalisis lalu lintas jaringan secara real-time, mendeteksi lonjakan lalu lintas yang tidak normal, dan memungkinkan perlindungan otomatis dan penyeimbangan beban untuk mengurangi dampak serangan DDoS.

Insider Threats dengan jenis ancaman Aksi Malicious dari Orang Dalam.

Analisis ancaman: Ancaman dari karyawan atau orang dalam perusahaan yang memiliki akses ke sistem atau data sensitif.

Pencegahan dengan AI: AI memantau dan menganalisis lalu lintas jaringan secara real-time, mendeteksi lonjakan lalu lintas yang tidak normal, dan memungkinkan perlindungan otomatis dan penyeimbangan beban untuk mengurangi dampak serangan DDoS.

4. Kesimpulan

Penelitian ini telah mengeksplorasi berbagai aspek implementasi Artificial Intelligence (AI) dalam meningkatkan keamanan siber, dengan fokus pada analisis ancaman dan pencegahan. Temuan menunjukkan bahwa AI, melalui teknik-teknik seperti machine learning dan deep learning, mampu meningkatkan kemampuan deteksi dan respons terhadap ancaman siber secara signifikan. Implementasi AI memungkinkan identifikasi pola perilaku mencurigakan dan ancaman secara real-time, yang sulit dicapai dengan metode konvensional. Studi kasus pada beberapa organisasi menunjukkan bahwa adopsi AI dalam sistem keamanan siber dapat meningkatkan efektivitas dan efisiensi dalam menangani serangan siber. Organisasi yang menerapkan AI melaporkan penurunan insiden keamanan dan peningkatan ketahanan terhadap ancaman siber. Namun, penelitian ini juga mengidentifikasi beberapa tantangan, termasuk keterbatasan data pelatihan, interpretabilitas model AI, dan kebutuhan akan tenaga ahli yang terampil untuk mengelola sistem AI.

Daftar Rujukan

[1] D. Septasari, “The Cyber Security and The Challenge of Society 5.0 Era in Indonesia,” *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*, vol. 5, no. 2, 2023, doi: 10.30604/jti.v5i2.231.

[2] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research,” *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3204051.

[3] Syed Khurram Hassan and Asif Ibrahim, “The role of Artificial Intelligence in Cyber Security and Incident Response,” *International Journal for Electronic Crime Investigation*, vol. 7, no. 2, 2023, doi: 10.54692/ijeci.2023.0702154.

[4] M. Alowaidi, S. K. Sharma, A. AlEnizi, and S. Bhardwaj, “Integrating artificial intelligence in cyber security for cyber-physical systems,” *Electronic Research Archive*, vol. 31, no. 4, 2023, doi: 10.3934/era.2023097.

[5] A. J. G. de Azambuja, C. Plesker, K. Schützer, =R. Anderl, B. Schleich, and V. R. Almeida, “Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey,” *Electronics (Switzerland)*, vol. 12, no. 8, 2023, doi: 10.3390/electronics12081920.

[6] R. Maurya, “Analyzing the Role of AI in Cyber Security Threat Detection & Prevention,” *Int J Res Appl Sci Eng Technol*, vol. 11, no. 11, 2023, doi: 10.22214/ijraset.2023.56510.

[7] “ARTIFICIAL INTELLIGENCE BASED CYBER-SECURITY PROGRAM,” *International Research Journal of Modernization in Engineering Technology and Science*, 2022, doi: 10.56726/irjmets30115.

[8] Dr. P. KALARANI, “Empowering Artificial Intelligence and Cyber Security Challenges in Smart Manufacturing,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 6, 2021, doi: 10.17762/turcomat.v12i6.1280.

[9] S. G. Naqvi, S. Sheraz, I. Mehmood, and M. Yasin, “Cyber-physical Systems and Artificial Intelligence: The Role of Cyber Security, Machine Learning, Threats and benefits to Modern Economies and Industries,” *Pakistan Journal of Humanities and Social Sciences*, vol. 11, no. 2, 2023, doi: 10.52131/pjhss.2023.1102.0454.

[10] W. S. Admass, Y. Y. Munaye, and A. A. Diro, “Cyber security: State of the art, challenges and future directions,”n 2024. doi: 10.1016/j.csa.2023.100031.

[11] Y. Zeng, “AI Empowers Security Threats and Strategies for Cyber Attacks,” in *Procedia Computer Science*, 2022. doi: 10.1016/j.procs.2022.10.025.

[12] M. Tetaly and P. Kulkarni, “Artificial intelligence in cyber security - A threat or a solution,” in *AIP Conference Proceedings*, 2022. doi: 10.1063/5.0109664.

[13] P. R. J. Trim and Y. I. Lee, "Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience," *Big Data and Cognitive Computing*, vol. 6, no. 4, 2022, doi: 10.3390/bdcc6040110.

[14] 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, 2024, doi: 10.1016/j.dim.2023.100063.

[15] S. HURZHII, "The special features of using the artificial intelligence in the matters of cybersecurity," *INFORMATION AND LAW*, no. 4(47), 2023, doi: 10.37750/2616-6798.2023.4(47).291669.

[16] P. S. Dandge, U. I. Dawre, and R. F. Shirshikar, "Journal of Advanced Zoology Artificial Intelligence In Cyber Security," vol. 44, pp. 69– 72, 2023.

[17] S. K. Das - and P. P. -, "Use of Artificial Intelligence on Cyber Security and the New- generation Cyber-attacks," *International Journal For Multidisciplinary Research*, vol. 6, no. 2, 2024, doi: 10.36948/ijfmr.2024.v06i02.14521.

[18] Syed Khurram Hassan and Asif Ibrahim, "The role of Artificial Intelligence in Cyber Security and Incident Response," *International Journal for Electronic Crime Investigation*, vol. 7, no. 2, 2023, doi: 10.54692/ijeci.2023.0702154.

[19] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, no. 2, 2019, doi: 10.1007/s11192-019-03222-9.

[20] D. Nyale and S. M. Angolo, "A Survey of Artificial Intelligence in Cyber Security," *International Journal of Computer Applications Technology and Research*, 2022, doi: 10.7753/ijcatr1112.1014.