CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 34-41

Systematic Literature Review (SLR): Dampak Pemanfaatan Artificial Intelligence untuk Meningkatkan Cyber Security

Arthur Gregorius Pongoh[1], Rizqy Achmad Fahreza[2], Bilal Al Kindi[3], Feddy Setio Pribadi[4], Rizky Ajie Aprilianto[5]

[1,2,3,4,5] Teknik Komputer, Departemen Teknik Elektro, Universitas Negeri Semarang, Sekaran, Gunungpati, Semarang, 50229
Email: arthurgregorius333@gmail.com, rizqyachmadfahreza@gmail.com, bilal.ww2308@gmail.com, feddy.setio@mail.unnes.ac.id, rizkyajiea@mail.unnes.ac.id

Abstrak

Artificial Intelligence (AI) adalah tambahan kecerdasan pada sistem yang dapat dikelola secara ilmiah dan berkembang di dunia teknologi untuk melayani berbagai aplikasi, termasuk keamanan siber. Kecerdasan buatan memainkan peran penting dalam keamanan siber, memungkinkan deteksi dini ancaman keamanan siber, analisis terperinci terhadap serangan yang muncul, dan respons yang cepat dan akurat. Penelitian ini menggunakan teknik tinjauan literatur sistematis (SLR) untuk menganalisis peran kecerdasan buatan dalam keamanan siber. Pengumpulan data dilakukan dengan mendokumentasikan semua makalah yang memuat temuan penelitian serupa dengan laporan penelitian ini. Makalah yang digunakan dalam penelitian ini adalah 20 makalah dari database *ScienceDirect* dan *Google Scholar*. Kecerdasan buatan telah menjadi elemen kunci dalam mendukung upaya untuk melindungi sistem informasi dan jaringan dari ancaman siber yang semakin kompleks. Dengan kemampuannya untuk belajar dari pola-pola data, AI memungkinkan untuk mendeteksi ancaman yang belum pernah terjadi sebelumnya dan memberikan respons secara real-time. Melalui tinjauan literatur sistematis ini, kami menyelidiki berbagai pendekatan dan teknik AI yang telah diterapkan dalam konteks keamanan siber, termasuk penggunaan jaringan syaraf tiruan, algoritma pembelajaran mesin, dan analisis teks. Hasil analisis kami menyoroti bahwa AI telah berhasil digunakan dalam mendeteksi serangan siber, menganalisis pola-pola perilaku yang mencurigakan, dan mengoptimalkan respons keamanan. Implikasi praktis dari penelitian ini adalah pentingnya terus mengembangkan dan mengadopsi solusi AI yang dapat memperkuat pertahanan siber dalam menghadapi ancaman yang terus berkembang.

Kata Kunci: *Artificial Intelligence, Cyber Security, Systematic Literature Review, Aplikasi Artificial Intelligence*

Systematic Literature Review (SLR): The Impact of Utilizing Artificial Intelligence to Enhance Cyber Security

Abstract

Artificial Intelligence (AI) is an augmentation of intelligence within systems that can be managed scientifically and is evolving in the world of technology to serve various applications, including cyber security. Artificial intelligence plays a crucial role in cyber security, enabling early detection of cyber security threats, detailed analysis of emerging attacks, and swift and accurate responses. This research utilizes the systematic literature review (SLR) technique to analyze the role of artificial intelligence in cyber security. Data collection was conducted by documenting all papers containing research findings similar to this research report. The papers used in this study comprise 20 papers from the ScienceDirect and Google Scholar databases.
Artificial intelligence has become a key element in supporting efforts to protect information systems and networks from increasingly complex cyber threats. With its ability to learn from data patterns, AI enables the detection of previously unseen threats and provides real-time responses. Through this systematic literature review, we investigated various AI approaches and techniques that have been applied in the context of cyber security, including the use of artificial neural networks, machine learning algorithms, and text analysis. Our analysis highlights that AI has been successfully utilized in detecting cyber attacks, analyzing suspicious behavioral patterns, and optimizing security responses. The practical implications of this research underscore the importance of continually developing and adopting AI solutions that can strengthen cyber defense against evolving threats.

Keywords: *Artificial Intelligence, Cyber Security, Systematic Literature Review, Application of Artificial Intelligenc*

1. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, keamanan siber menjadi sebuah isu utama yang memerlukan perhatian serius. Ancaman siber yang memiliki pola kompleks dan beragam mampu untuk menyerang, mencuri dan dapat memberikan dampak yang negatif. Teknologi Artificial Intelligence (AI) telah muncul sebagai sistem yang memiliki potensi untuk memperkuat cyber security.

Artificial Intelligence (AI) adalah kecerdasan yang ditambahkan ke suatu sistem yang dapat ditempatkan dalam konteks ilmiah, terkadang disingkat sebagai kecerdasan buatan atau AI, dan didefinisikan sebagai kecerdasan suatu entitas ilmiah. (Mangapul Siahaan, dkk., 2020). Yang memiliki kemampuan untuk berpikir dan bertindak seperti manusia, telah menjanjikan solusi inovatif untuk mendeteksi, mencegah, dan merespons ancaman siber dengan lebih cepat dan akurat daripada metode konvensional. Artificial Intelligence (AI) juga dapat menemukan pola aneh atau aktivitas mencurigakan di dalam jaringan yang mungkin sulit dideteksi oleh manusia dengan menggunakan teknik seperti pembelajaran mesin, analisis prediktif, dan pemrosesan bahasa alami. Selain itu, Sistem AI yang aman dibangun untuk menahan dan melindungi dari serangan-serangan risiko siber lainnya. Sistem AI terdesentralisasi adalah solusi yang memungkinkan banyak pemangku kepentingan untuk berkolaborasi dan berbagi data sekaligus memastikan privasi dan kerahasiaan data sensitif. (Ahmed M. Shamsan Saleh, 2024)

Namun, datangnya AI yang menawarkan potensi besar sebagai aset pertahanan digital, AI juga menghadirkan tantangan yang harus dihadapi. perangkat lunak AI rentan terhadap serangan kompleks, yang dapat mengakibatkan pengambilan keputusan yang tidak tepat. Maka dari itu, penelitian perlu terus dilakukan agar menghasilkan solusi keamanan yang dapat mengintegrasikan kecerdasan dengan mekanisme perlindungan yang dapat diandalkan dan responsif.

Dalam konteks ini, Literature Review yang dibuat memiliki tujuan untuk mengeksplorasi dan menganalisis implementasi kecerdasan buatan dalam meningkatkan keamanan cyber. Dengan mempertimbangkan penelitian terkini dan studi kasus yang relevan, Literature Review ini akan meninjau peran AI dalam mendeteksi, mencegah dan merespons terhadapa ancaman cyber, serta mengevaluasi tantangan dan peluan yang terkait dengan penggunaan teknologi ini dalam konteks cyber security.

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi Systematic Literature Review (SLR) yang bertujuan untuk mengidentifikasi, mengkaji, dan mengevaluasi seluruh temuan penelitian yang relevan untuk menentukan jawaban atas pertanyaan penelitian. Penelitian ini terdiri dari beberapa langkah: merumuskan pertanyaan penelitian, mengkaji literatur, menentukan kriteria inklusi dan eksklusi, memilih literatur, menyajikan data, menyiapkan data, dan menarik kesimpulan. Ruang lingkup literatur ini mencakup pencarian literatur ilmiah dari sumber database berikut: ScienceDirect dan Google Scholar. Sumber database ini dianggap mencakup sumber multidisiplin di bidang kecerdasan buatan.

Pertanyaan penelitian sekunder berikut ini akan dipertimbangkan dalam menjawab pertanyaan penelitian utama:

1. Apa dampak positif dan negatif Artificial Intelligence terhadap Cyber Security?
2. Bagaimana peningkatan implementasi Artificial Intelligence dibandingkan dengan cara tradisional yang tidak digerakkan oleh Artificial Intelligence dalam Cyber Security?

2.1. Kriteria Inklusi dan Eksklusi

Tabel 1 menjelaskan kriteria inklusi pada penelitian ini yang digunakan dalam mengidentifikasi studi. Pembentukan kriteria inklusi dan eksklusi didasarkan pada pertanyaan penelitian dan tujuan dari studi ini. Hanya literatur yang telah direview, yang ditulis dalam bahasa Inggris, diterbitkan pada tahun 2019-2024, dan tersedia dengan akses terbuka, yang dimasukkan dalam penelitian ini.

Tabel 1. Kriteria Inklusi dan Eksklusi

No.	Inklusi	Eksklusi
1	Studi dengan berfokus pada dampak Artificial Intelligence pada Cyber Security	Studi yang tidak berfokus pada Dampak Artificial Intelligence pada Cyber Security
2	Literatur yang diterbitkan dalam Bahasa Inggris	Literatur yang diterbitkan selain dalam Bahasa Inggris
3	Artikel jurnal yang telah direview yang kontennya muncul di salah satu dari sumber basis data berikut: ScienceDirect, Google Scholar.	Sumber literatur yang belum direview
4	Sumber literatur dengan akses terbuka	Sumber dengan akses terbatas
5	Sumber-sumber literatur yang diterbitkan pada tahun 2020 sampai 2024	Literatur yang diterbitkan sebelum tahun 2019

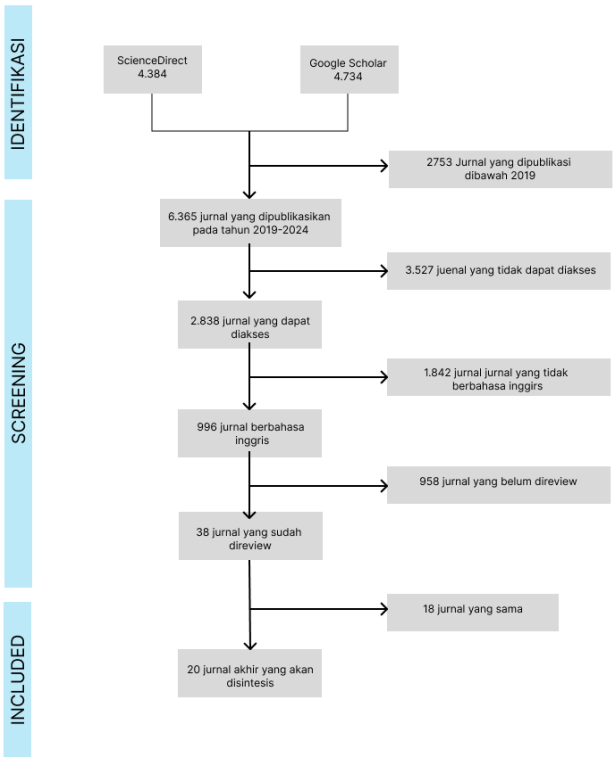
2.2. Kata Kunci Pencarian

Dalam mencari sumber yang relevan di basis data yang dipilih, digunakan kata kunci fleksibel dan relevan. Kombinasi kata kunci tersebut difokuskan pada pertanyaan penelitian. Tabel 2 berisi kata kunci

dan basis data yang digunakan dalam sumber yang dipilih.

Tabel 2. Metadata Pencarian

No.	Basis Data	Kata Kunci Pencarian	Tahun Diterbitkan
1	Science Direct https://www.sciencedirect.com/ 15-3-2024	"Artificial Intelligence" OR "AI" AND "Cyber Security" OR "Cyber Threat"	2019-2024
2	Google Scholar https://scholar.google.com/ 15-3-2024	"Artificial Intelligence" OR "AI" AND "Cyber Security" OR "Cyber Threat"	2019-2024



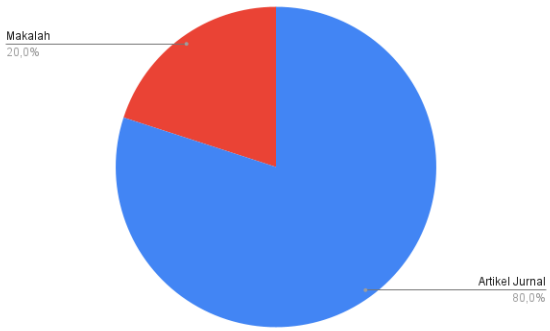
Gambar 1. Diagram Flowchart PRISMA

2.3. Flowchart PRISMA

Diagram flowchart PRISMA yang digambarkan pada Gambar 1 dimanfaatkan dalam penelitian untuk meninjau literatur yang dipilih secara sistematis, dengan menggunakan kata kunci yang dipilih dalam Tabel 1. PRISMA terdiri dari tiga tahap yang berbeda, yaitu Identifikasi, penyaringan, dan sintesis yang juga mencakup aspek pelaporan. Tahap identifikasi berfokus pada identifikasi sumber-sumber literatur yang relevan dalam basis data yang dipilih. Pada tahap ini, hasil pencarian menghasilkan 9.118 hasil gabungan. Pada tahap penyaringan, artikel-artikel tersebut disaring untuk mencari artikel yang diterbitkan pada tahun 2019-2024, dan hal ini menurunkan jumlahnya menjadi 6.365 artikel, kemudian disaring kembali untuk mencari artikel dengan akses yang terbuka dan kemudian didapatkan jumlahnya menjadi 2.838 artikel. Penyaringan dilanjutkan untuk mencari artikel yang diterbitkan dalam bahasa inggris, maka jumlahnya menjadi 996 artikel, dan disaring untuk terakhir kalinya agar ditemukan artikel yang belum direview, maka jumlahnya menjadi 38 artikel. Dari jumlah tersebut, 18 artikel dihapus karena merupakan duplikasi, sehingga tersisa 20 artikel. Itulah artikel yang tersisa yang disintesis dan dilaporkan. Artikel-artikel ini kemudian diimpor ke alat referensi Mendeley untuk disortir dan dianalisis.

3. HASIL DAN PEMBAHASAN

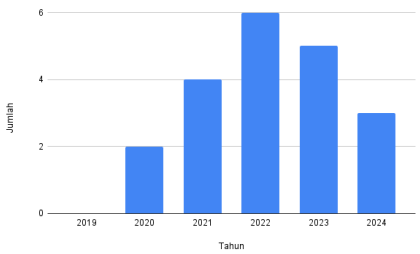
Hasil dari pencarian dan tinjauan literatur menghasilkan total 20 artikel yang tersisa untuk sintesis rinci sesuai dengan pertanyaan-pertanyaan penelitian. Gambar 2 menunjukkan rincian artikel yang disintesis, menyoroti bahwa sebagian besar sumber yang disintesis adalah 16 artikel jurnal dan 4 makalah konferensi, yang merupakan indikasi yang baik bahwa sumber-sumber yang telah ditelaah telah dikonsultasikan untuk mencapai kesimpulan tertentu dalam penelitian ini.



Gambar 2. Rincian Artikel yang Disintesis.

Gambar 3 menggambarkan distribusi artikel yang disintesis per tahun. Dalam hal distribusi artikel penelitian berdasarkan ruang lingkup penelitian kami, yang mencakup 2019-2024, terlihat jelas bahwa studi tentang dampak AI pada keamanan siber organisasi dimulai secara bertahap pada tahun 2020, di mana hanya ada 2 studi yang ditemukan terkait dengan penelitian ini. Dari tahun 2021 hingga 2022, terjadi peningkatan bertahap dari 4 artikel menjadi 6 artikel; pada tahun 2023, terjadi penurunan dimana jumlah publikasi menjadi 5 artikel. Pada tahun 2023, jumlah artikel relevan yang ditemukan adalah 3, yang terlihat seperti penurunan; namun, mengingat pada saat penulisan artikel ini dilakukan di awal tahun, jumlahnya kemungkinan besar akan meningkat pada akhir tahun. Gambar 3 menunjukkan minat yang semakin besar dari para peneliti ilmiah dalam memahami dampak AI

terhadap keamanan siber, yang mungkin disebabkan oleh kemajuan yang sedang berlangsung dalam penggunaan AI dan teknik yang relevan dalam keamanan siber.



Gambar 3. Distribusi Artikel

3.1. Pembahasan

Hasil tinjauan literatur disajikan di bagian ini untuk membahas secara komprehensif dampak keseluruhan dari solusi berbasis AI pada keamanan siber. Analisis ini mempertimbangkan dampak positif dan negatif. Selain itu, untuk mendapatkan pemahaman yang lengkap tentang dampak keseluruhan, peningkatan penggunaan AI pada perlindungan siber untuk mendapatkan pandangan yang lebih luas. Oleh karena itu, tinjauan ini juga memeriksa peningkatan penggunaan AI dibandingkan dari pendekatan tradisional non-AI terhadap keamanan siber.

Tabel 3. Ringkasan Hasil Dampak Positif AI Terhadap Cyber Security

No.	Sub-Tema	Jumlah Artikel	Sumber
1	Mendeteksi ancaman	10	A2, A3, A5, A6, A7, A8, A16, A17, A18, A20
2	Peningkatan perlindungan	6	A2, A9. A13, A14, A15, A19
3	Memprediksi serangan	5	A1, A4, A11, A12, A18
4	Lainnya	2	A5, A9

Tabel 4. Ringkasan Hasil Dampak Negatif AI Terhadap Cyber Security

No.	Sub-Tema	Jumlah Artikel	Sumber
1	Sumber daya/biaya yang besar	2	A1, A16
2	Eksploitasi Sistem AI	3	A9, A10, A19
3	Lainnya	3	A5, A6, A13

Tabel 5. Ringkasan Peningkatan Aplikasi AI Dibanding Cara Tradisional

No.	Sub-Tema	Jumlah Artikel	Sumber
1	Peningkatan kinerja dan keamanan	13	A1, A3, A5, A7, A9, A10, A11, A13, A14, A15, A16, A17, A19
2	Peningkatan akurasi	5	A2, A6, A8, A12, A18
3	Deteksi intrusi yang meningkat	2	A4, A20

3.1.1. Dampak Positif Artificial Intelligence Terhadap Cyber Security

Untuk mengevaluasi pengaruh keseluruhan artificial intelligence (AI) terhadap cyber security, tinjauan ini berfokus pada pertanyaan: "apa dampak positif dan negatif artificial intelligence terhadap cyber security?" Penelitian yang ada menunjukkan bahwa meningkatnya ancaman dan serangan siber telah mendorong untuk mengadopsi teknologi berbasis AI untuk melindungi aset digital.

Ada beberapa kelemahan pada dasbor intelijen siber saat ini, sebagaimana disebutkan dalam sumber yang dapat dipercaya. Keterbatasan ini mencakup kurangnya statistik historis serangan siber tingkat negara, ketidakmampuan untuk memprediksi ancaman siber spesifik suatu negara, dan ketidakmampuan untuk menggunakan metode deteksi anomali spektrum siber tingkat negara berbasis CNN (Fahim Sufi, 2023). Setelah kerentanan ditemukan dan disebarkan, aturan deteksi yang ada harus terus diperbarui dan ditingkatkan untuk mencegah penyerang mendapatkan akses. Membuat aturan deteksi secara manual untuk serangan yang diketahui memakan waktu dan rawan kesalahan. Oleh karena itu, beberapa orang menyarankan penggunaan cara otomatis untuk menghasilkan aturan deteksi untuk serangan yang diketahui (Yan Jia, dkk., 2023).

Dari perspektif kecerdasan buatan, serangan siber adalah pola jahat yang berbeda dari lalu lintas internet yang sah. Untuk membedakan lalu lintas berbahaya dari lalu lintas sah, sistem deteksi intrusi telah dikembangkan menggunakan teknik kecerdasan buatan yang memiliki kemampuan untuk memeriksa data dalam jumlah besar dan beradaptasi dengan perubahan sifat lalu lintas Internet. Serangan siber baru-baru ini menargetkan infrastruktur jaringan, logika bisnis, dan pengguna (Sherali Zeadally, dkk., 2020). Hal ini melibatkan kecerdasan buatan yang memperoleh sejumlah besar pengetahuan tentang semua aspek aktivitas manusia dan kemampuan untuk menghadapinya. Kecerdasan buatan didefinisikan secara umum sebagai suatu aspek kecerdasan, dan lebih umum lagi sebagai penciptaan perangkat cerdas, misalnya, untuk

memberikan solusi terhadap masalah-masalah sulit yang tidak dapat diselesaikan tanpa kinerja yang unggul atau pengambilan keputusan yang tepat dengan kecerdasan yang unggul. sebagai teknologi yang menyediakan Dalam artikel ini, kami menerapkan pendekatan yang sesuai dan mengusulkan penerapan teknik kecerdasan buatan tertentu untuk masalah pertahanan siber, sebagai respons terhadap kemajuan terkini dalam kecerdasan buatan (Ramanohar Das & Raghav Sandhane, 2021).

Penggunaan AI dalam keamanan siber menawarkan berbagai peluang untuk kolaborasi dan integrasi dengan teknologi lain, di antaranya kombinasi teknologi AI dan blockchain memiliki potensi besar. Konvergensi ini meningkatkan integritas dan transparansi data melalui buku besar blockchain yang tidak dapat diubah, memastikan bahwa wawasan dan tindakan yang dihasilkan oleh AI tidak dapat dimanipulasi dan diverifikasi. Selain itu, lingkungan kolaboratif yang dimungkinkan oleh blockchain memungkinkan deteksi ancaman terdesentralisasi, waktu respons lebih cepat, dan peningkatan akurasi, sehingga memperkuat operasi keamanan siber terhadap ancaman tingkat lanjut yang terus berkembang. Kombinasi teknologi blockchain dan AI yang terdesentralisasi berpotensi mengatasi banyak tantangan yang dihadapi keamanan siber saat ini (B. D. Deebak & Fadi Al Turjman, 2021).

3.1.2. Dampak Negatif Artificial Intelligence Terhadap Cyber Security

Meskipun implementasi AI dalam cyber security diakui karena kemampuannya untuk mencapai efisiensi melebihi kemampuan manusia, ada beberapa kelemahan yang terkait dengan adopsinya, terutama pada tingkat organisasi. Tabel 4 memberikan gambaran singkat tentang batasan yang meliputinya. Peningkatan adopsi AI membutuhkan sumber daya dan biaya besar yang tentunya akan menjadi bahan pertimbangan yang besar bagi suatu perusahaan. Keberadaan sistem AI yang tidak aman juga dapat dengan mudah dieksploitasi oleh pihak tertentu dan dapat menimbulkan kerugian besar. Efek negatif ini menghambat atau menunda penerimaan luas solusi AI sebagai pendekatan utama cyber security.

Meskipun terdapat banyak manfaat dalam menggabungkan keamanan siber dan pembelajaran mesin, terdapat juga beberapa permasalahan dan tantangan yang perlu ditangani secara hati-hati. Permasalahan yang dibahas antara lain masalah kompatibilitas. Mengenai masalah kompatibilitas, teknologi keamanan dan algoritma pembelajaran mesin yang berbeda memiliki sumber data yang berbeda dan harus dipilih dengan cermat untuk memastikan kompatibilitas. Selain itu, penggunaan beberapa algoritma dapat mengakibatkan beban kerja sistem yang berlebihan, yang dapat berdampak negatif terhadap kinerja sistem secara keseluruhan. Saat menggunakan mekanisme pembelajaran mesin untuk memprediksi fenomena fisik tertentu, masalah akurasi juga dapat terjadi, terutama jika terdapat kesalahan pada kumpulan data atau pengaturan model pembelajaran mesin. Terakhir, kerentanan dalam mekanisme keamanan juga merupakan masalah serius, karena data sensitif dapat diungkapkan, diubah, atau bahkan tidak tersedia. Oleh karena itu, pengujian keamanan protokol keamanan harus dilakukan dengan hati-hati untuk memastikan keamanan dari serangan, misal menggunakan tes logika AVISPA (Mohammad Wazid, dkk., 2022).

Selain tantangan teknis yang disebutkan di atas, masalah perlindungan data dan etika juga merupakan masalah penting ketika menerapkan AI pada keamanan siber, seperti teknologi XAI. Sepanjang siklus hidup sistem, model XAI harus secara eksplisit mengatasi masalah privasi. Disepakati secara luas bahwa menghormati hak privasi setiap orang adalah hal yang penting, terutama dalam bidang keamanan siber yang paling sensitif seperti autentikasi, email, dan kata sandi. Selain itu, sistem XAI secara alami tunduk pada kekhawatiran etika umum mengenai potensi diskriminasi (rasisme, seksisme, ageisme, dll.) oleh sistem AI. Secara teori, model AI berdasarkan data yang sebelumnya dikumpulkan manusia dapat menghasilkan bias yang sama. Pentingnya mengambil tindakan pencegahan yang bertujuan untuk memastikan bahwa pemeringkatan dan pernyataan terkait yang dibuat oleh sistem XAI tidak menunjukkan diskriminasi, bias, atau ketidakadilan (Zhibo Zhang et al., 2022).

3.1.3. Peningkatan Implementasi Artificial Intelligence Dibandingkan dengan Cara Tradisional dalam Cyber Security

Untuk sepenuhnya mengukur dampak artificial intelligence (AI) terhadap cyber security, disimpulkan bahwa dibutuhkan perbandingan antara pendekatan cyber security tradisional dan pendekatan yang didorong oleh AI kemudian dilihat peningkatan yang ditawarkan oleh cara yang didorong artificial intelligence. Dalam penelitian kontemporer, teknik kecerdasan buatan telah menunjukkan janjinya dalam melawan ancaman keamanan cyber di masa depan. Teknik-teknik ini mengusulkan berbagai perilaku cerdas mulai dari cara mesin dapat berpikir hingga bertindak seperti manusia. Solusi keamanan cyber berbasis kecerdasan buatan yang baru-baru ini diusulkan sebagian besar difokuskan pada teknik pembelajaran mesin yang melibatkan penggunaan agen cerdas untuk membedakan antara lalu lintas serangan dan lalu lintas sah. Dalam hal ini, agen cerdas bertindak seperti manusia yang tugasnya adalah untuk menemukan aturan klasifikasi paling efisien. Salah satu pendorong utama di balik penggunaan kecerdasan buatan dalam manufaktur cerdas adalah

sektor pendidikan, yang membutuhkan adaptabilitas terhadap pembelajar individu. Untuk memenuhi kebutuhan ini, perangkat lunak pendidikan yang menggunakan agen cerdas dikembangkan, untuk menyesuaikan kecepatan pembelajaran siswa dengan menyesuaikan tingkat kesulitan pada latihan yang disajikan (Sherali Zeadally, dkk., 2020).

Misalnya, ketika versi baru protokol komunikasi web HTTP/2 diperkenalkan, pemodelan dan deteksi serangan DoS baru diusulkan. Penulis menunjukkan cara melewati sistem deteksi intrusi. HTTP/2 memiliki mekanisme kontrol aliran pada lapisan aplikasi yang tidak ada di HTTP/1.1. Jenis serangan banjir kontrol aliran ini mematikan server yang menjalankan layanan HTTP/2 sambil mempertahankan sejumlah kecil koneksi ke server target. Hal ini menghindari sistem deteksi yang diketahui yang menafsirkan peristiwa jaringan karena sejumlah besar koneksi sebagai serangan. Ketika lalu lintas banjir HTTP/2 yang diusulkan dimulai ke layanan HTTP/2, teknik kecerdasan buatan (Naive Bayes, Decision Trees, dan Rule Learning) mendeteksi HTTP DDoS menggunakan teknik kecerdasan buatan yang sama. Tingkat positif palsu akan lebih tinggi dibandingkan jika Serangan tersebut menggunakan /1.1, yang menunjukkan bahwa serangan tersebut melewati sistem deteksi intrusi yang diketahui. Saat mendeteksi serangan, SVM (Support Vector Machine) tidak menampilkan positif palsu mengingat rangkaian fitur yang diusulkan terkait dengan deteksi HTTP/2 (Mohammad Wazid, dkk., 2022).

Meningkatnya penggunaan kecerdasan buatan dalam keamanan siber merupakan respons terhadap meningkatnya kompleksitas dan frekuensi serangan siber. Dengan kemampuan analitis yang lebih baik, sistem keamanan yang menggunakan AI dapat secara efisien mengidentifikasi pola-pola aneh dalam data yang mengindikasikan adanya serangan. Ini juga mempercepat deteksi serangan, karena AI dapat secara otomatis memantau lalu lintas jaringan dan mendeteksi aktivitas mencurigakan secara real-time. Kemampuan AI untuk beradaptasi terhadap perubahan lingkungan keamanan siber juga memberikan nilai tambah, karena sistem dapat secara dinamis beradaptasi terhadap serangan baru dan teknik serangan yang terus berkembang. Selain itu, dengan kemampuan untuk mengotomatiskan tindakan respons, AI memungkinkan sistem merespons serangan dengan cepat dan efisien, seperti mengisolasi sistem yang terinfeksi atau memblokir alamat IP yang mencurigakan. Analisis data terperinci memungkinkan perusahaan mendapatkan wawasan lebih dalam mengenai ancaman dunia maya dan mengambil keputusan yang lebih cerdas saat mengelola keamanan. Di masa depan, alat yang lebih canggih dan modern harus digunakan untuk mengembangkan algoritma inovatif untuk menciptakan indeks ancaman siber (Fahim Sufi, 2023).

3.2. Rekomendasi untuk Penelitian di Masa Depan

Studi ini berkonsentrasi pada pemeriksaan bagaimana AI mempengaruhi keamanan siber. Upaya penelitian di masa depan dapat mengarahkan perhatian untuk menyelidiki dampak spesifik AI pada berbagai jenis institusi, seperti institusi di sektor keuangan, manufaktur, perawatan kesehatan, pendidikan, infrastruktur penting, dan pemerintah. Eksplorasi yang lebih terarah pada area-area ini dapat menghasilkan wawasan yang lebih dalam, membantu pemanfaatan AI yang optimal untuk meningkatkan keamanan siber. Selain itu, hal ini akan memfasilitasi pengembangan langkah-langkah untuk memitigasi potensi eksploitasi berbahaya di mana alat AI digunakan dengan tujuan yang berbahaya, yang secara khusus menargetkan institusi tertentu.

4. KESIMPULAN

Penggunaan artificial intelligence dan deep learning dalam meningkatkan cyber security, termasuk deteksi dan mitigasi serangan siber, pemanfaatan blockchain, dan aplikasi kecerdasan buatan dalam sistem keamanan. Beberapa studi juga menekankan pentingnya integrasi keamanan siber dan pembelajaran mesin untuk meningkatkan kemampuan sistem keamanan. Penelitian yang di lakukan ini menggunakan Systematic Literature Review (SLR) guna menganalisis dampak pemanfaatan Kecerdasan Buatan dalam meningkatkan keamanan siber. AI memainkan peran penting dalam mendeteksi, menganalisis, dan merespons ancaman keamanan siber dengan cepat dan akurat.

Meskipun AI memiliki dampak positif dalam deteksi ancaman, peningkatan perlindungan, dan prediksi serangan siber, ada juga dampak negatif seperti biaya tinggi dan potensi eksploitasi sistem AI. Implementasi AI dalam cyber security memiliki dampak positif dan negatif. Meskipun AI dapat meningkatkan efisiensi dalam mendeteksi ancaman siber, adopsinya membutuhkan sumber daya dan biaya yang signifikan, dan sistem AI yang tidak aman dapat dieksploitasi oleh entitas jahat.

DAFTAR PUSTAKA

Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.02.531

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. Sustainable Cities and Society, 66.

https://doi.org/10.1016/j.scs.2020.102655

Das, R., & Sandhane, R. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series, 1964(4). https://doi.org/10.1088/1742-6596/1964/4/042072

Deebak, B. D., & AL-Turjman, F. (2021). Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. Journal of Information Security and Applications, 58. https://doi.org/10.1016/j.jisa.2021.102749

Ghillani, D. (2022). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. American Journal of Artificial Intelligence, x, No. x, x–x. https://doi.org/10.22541/au.166379475.54266021/v1

Jia, Y., Gu, Z., Du, L., Long, Y., Wang, Y., Li, J., & Zhang, Y. (2023). Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. Knowledge-Based Systems, 276. https://doi.org/10.1016/j.knosys.2023.110781

Kalai C., T., Gnanaprakasam, C., Indumathy, M., Khilar, R., & Sathish Kumar, P. J. (2022). Artificial intelligence based optimization for mapping IP addresses to prevent cyber-based attacks. Measurement: Sensors, 24. https://doi.org/10.1016/j.measen.2022.100508

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence. Journal of Computers, Mechanical and Management, 2(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

Moorthy, R. S. S., & Nathiya, N. (2022). Botnet Detection Using Artificial Intelligence. Procedia Computer Science, 218, 1405–1413. https://doi.org/10.1016/j.procs.2023.01.119

Nabil, S., Mohamed, B., Bersini, H., & Bourennane, E.-B. (n.d.). Artificial Intelligence and Cyber Security: Protecting and Maintaining Industry 4.0 Power Networks.

Shamsan Saleh, A. M. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain: Research and Applications, 100193. https://doi.org/10.1016/j.bcra.2024.100193

Shyam Mohan, J. S., Thirunavukkarasu, M., Kumaran, N., & Thamaraiselvi, D. (2024). Deep learning with blockchain based cyber security threat intelligence and situational awareness system for intrusion alert prediction. Sustainable Computing: Informatics and Systems, 42. https://doi.org/10.1016/j.suscom.2023.100955

Siahaan, M., Harsana Jasa, C., Anderson, K., Rosiana, M. V., Lim, S., & Yudianto, W. (2020). Penerapan Artificial Intelligence (AI) Terhadap Seorang Penyandang Disabilitas Tunanetra. In Journal of Information System and Technology (Vol. 01).

Srinivas, K., Singh, L., Chavva, S. R., Dappuri, B., Chandrasekaran, S., & Qamar, S. (2022). Multi-modal cyber security based object detection by classification using deep learning and background suppression techniques. Computers and Electrical Engineering, 103. https://doi.org/10.1016/j.compeleceng.2022.108333

Sufi, F. (2023). A global cyber-threat intelligence system with artificial intelligence and convolutional neural network. Decision Analytics Journal, 9. https://doi.org/10.1016/j.dajour.2023.100364

Syed Khurram Hassan, & Asif Ibrahim. (2023). The role of Artificial Intelligence in Cyber Security and Incident Response. International Journal for Electronic Crime Investigation, 7(2). https://doi.org/10.54692/ijeci.2023.0702154

Tabassum, T., Lim, S., & Khalghani, M. R. (2024). Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control. Electric Power Systems Research, 226. https://doi.org/10.1016/j.epsr.2023.109925

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. In ICT Express (Vol. 8, Issue 3, pp. 313–321). Korean Institute of Communication Sciences. https://doi.org/10.1016/j.icte.2022.04.007

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access, 8, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. Procedia Computer Science, 208, 170–175.

https://doi.org/10.1016/j.procs.2022.10.025

Zhang, Z., Hamadi, H. Al, Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE Access, 10, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051