MONAS: Jurnal Inovasi Aparatur
Vol.6 No.2 (2024): 154-165
e-ISSN: 2656-0194

Kajian Peran Artificial Intelligence untuk Memperkuat Keamanan Siber pada Infrastruktur Informasi Vital

Study of the Artificial Intelligence Role in Achieving Cybersecurity for Critical Information Infrastructure

Agus Kurniati
Badan Siber dan Sandi Negara, Jalan Raya Muchtar No. 70, Bojongsari, Sawangan, Depok
*agus.kurniati@bssn.go.id

Submitted: 01-11-2024 *Accepted: 24-12-2024* *Published: 31-12-2024*

Abstrak: Penelitian ini bertujuan untuk mengkaji peran kecerdasan buatan (*Artificial Intelligence*) dalam memperkuat keamanan siber pada infrastruktur informasi vital (IIV) di Indonesia. Metode penelitian yang digunakan adalah *systematic literature review* (SLR) dengan melakukan proses identifikasi, melakukan kajian dan evaluasi, dengan pengambilan data melalui studi literatur yang relevan dengan topik penelitian. Data yang diperoleh dianalisis menggunakan metode sintesis kritis, *gap analysis* dan analisis srategi SOAR (*Strengths, Opportunities, Aspirations, Results*) kemudian dibandingkan dengan *Cyber Security Framework NIST* untuk menentukan alternatif strategi yang sesuai. Hasil penelitian menunjukkan bahwa AI dapat memperkuat keamanan siber pada sektor IIV dengan meningkatkan kemampuan deteksi dan respons terhadap ancaman, serta mengoptimalkan pengelolaan risiko. Penelitian ini juga mengidentifikasi potensi peluang, seperti kolaborasi lintas sektor dan pengembangan teknologi inovatif, serta tantangan, termasuk kebutuhan untuk menjaga transparansi dan etika penggunaan AI. Selain itu, strategi yang diusulkan untuk mewujudkan AI sebagai alat dalam keamanan siber mencakup penguatan investasi dalam teknologi, peningkatan keterampilan sumber daya manusia, dan pengembangan kebijakan yang mendukung dengan tetap memperhatikan potensi risiko yang dapat timbul, seperti pelanggaran privasi, kebocoran data, dan potensi bias dalam pengambilan keputusan oleh sistem AI. Hasil penelitian ini diharapkan dapat memberikan wawasan bagi pemangku kepentingan dalam upaya umtuk memperkuat keamanan siber pada sektor IIV di Indonesia.
Kata kunci: *artificial intelligence*, infrastruktur informasi vital, keamanan siber, *gap analysis*, SOAR

Abstract: *This research aims to examine the role of Artificial Intelligence (AI) in strengthening cybersecurity for critical information infrastructure (CII) in Indonesia. The research methodology used is a systematic literature review (SLR) involving identification, review, and evaluation, data collected through literature studies relevant to the research topic. Data were analyzed using critical synthesis method, gap analysis and SOAR (Strengths, Opportunities, Aspirations, Results) analysis, compared with the NIST Cybersecurity Framework to determine suitable strategic alternatives. The research results indicate that AI can strengthen cybersecurity in the CII sector by enhancing threat detection and response capabilities and optimizing risk management. The study also identified potential opportunities, such as cross-sector collaboration and the development of innovative technologies, as well as challenges, including the need to maintain transparency and ethical AI. In addition, the proposed strategy to realize AI as a tool in cyber security includes strengthening investment in technology, increasing human resource skills, and supporting development policies while taking into account potential risks that may arise, such as privacy violations, data leaks, and potential bias in decision making by AI systems. It is hoped that the results of this research will provide insight for stakeholders in efforts to strengthen cyber security in the IIV sector in Indonesia.*

Keywords: *artificial intelligence, critical information infrastructure, cyber security, gap analysis,* SOAR

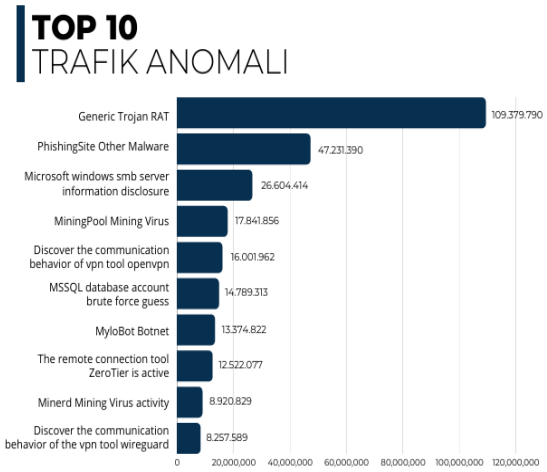
Author(s). (2024). Monas: Jurnal Inovasi Aparatur, 6 (2), page 154-165
https://doi.org/10.54849/monas.v6i2.251

PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, hampir semua lini dalam aspek kehidupan memanfaatkan sistem digital, teknologi internet, perangkat lunak, aplikasi dan perangkat digital. Era digital membawa manfaat besar dalam kecepatan dan aksibilitas informasi. Namun, di sisi lain era digital ini juga menghadirkan tantangan tersendiri, terutama terkait dengan isu keamanan, perlindungan data dan ketergantungan terhadap teknologi. Dengan semakin banyaknya aktivitas digital, risiko terhadap serangan siber juga semakin meningkat. Serangan siber dapat menimbulkan berbagai dampak serius yang dapat mengancam stabilitas nasional, eknonomi, keamanan dan kesejahteraan masyarakat. Keamanan siber menjadi isu yang sangat penting karena menjadi salah satu pilar utama dalam menjaga kestabilan dan keamanan suatu negara, khususnya yang terkait dengan aspek keamanan pada infrastruktur informasi vital (IIV) dimana jika pelayanan publik pada sektor IIV mengalami gangguan baik dari sisi kerahasiaan, keutuhan dan ketersediaan, maka akan mempengaruhi hajat hidup banyak orang. IIV merupakan sistem elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan sistem elektronik lainnya dalam menunjang sektor strategis, yang jika terjadi gangguan, kerusakan, atau kehancuran pada infrastruktur tersebut dapat berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional (Badan Siber dan Sandi Negara, 2023).

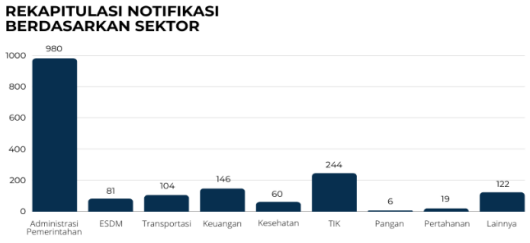
IIV mencakup sistem yang sangat penting bagi kelangsungan hidup masyarakat dan keamanan nasional, yang meliputi sektor administrasi pemerintah, energi dan sumber daya mineral, transportasi, keuangan, kesehatan, teknologi informasi dan komunikasi, pangan, pertahanan dan sektor lain yang ditetapkan presiden (*Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital*, 2022). IIV merupakan tulang punggung yang menopang pelaksanaan penerapan sistem pemerintah berbasis elektronik sebagai upaya pemerintah untuk menyelenggarakan pelayanan publik yang efektif, efisien, transparan. IIV sangat rawan terhadap serangan siber karena beberapa faktor utama yang berkaitan dengan sifat teknologinya, kompleksitasnya, serta ketergantungannya pada jaringan digital yang luas.

BSSN melaporkan jumlah trafik anomali serangan di Indonesia pada tahun 2023 sebesar 403.990.813. Berikut merupakan 10 jenis anomali ancaman tertinggi yang dirilis oleh BSSN:



Gambar 1. Data 10 Besar Anomali Ancaman Siber Indonesia Tahun 2023

Berdasarkan grafik tersebut dapat dilihat bahwa serangan yang paling banyak terjadi adalah trojan sebanyak 109.379.790 juta, diikuti dengan *phising* sebanyak 47.231.390 dan pengungkapan data sebanyak 26.604.414. Dalam laporan tahunan BSSN tersebut juga disampaikan data terkait sebaran sektor yang mengalami potensi serangan siber yang ditindak lanjuti dengan pemberian notifikasi dari BSSN ke isntansi terkait, sebagai upaya untuk pencegahan agar tidak berkembang menjadi insiden serangan siber. Berikut merupakan data notifikasi potensi serangan siber berdasarkan sebaran sektor:



Gambar 2. Rekapitulasi Notifikasi Berdasarkan Sektor

Sektor yang banyak mengalami potensi serangan siber adalah sektor administrasi pemerintah dengan domain go.id, diikuti dengan sektor TIK dan keuangan, Tim Pusat Kontak Siber BSSN mengirimkan sebanyak 1.762 notifikasi indikasi serangan siber ke berbagai sektor. Sebanyak 43% notifikasi direspon dan 57 %

notifikasi tidak direspon (BSSN, 2023). Notifikasi merupakan tindakan dari BSSN untuk mengirimkan pemberitahuan kepada sektor terkait ketika Tim Monitoring BSSN menemukan adanya indikasi serangan. Harapannya notifikasi yang dikirimkan ini akan ditindaklanjuti oleh sektor terkait, untuk mencegah insiden serangan siber yang akan menimbulkan dampak kerugian. Namun tidak semua notifikasi mendapatkan respon dari instansi. Rendahnya kesadaran para pemangku kepentingan untuk merespon notifikasi ini berpeluang menjadi celah kerentanan yang banyak dimanfaatkan pelaku kejahatan siber untuk mengganggu sistem elektronik mereka. Ancaman keamanan dunia maya menimbulkan risiko dan tantangan keamanan yang sangat besar terhadap politik, ekonomi, masyarakat dan pertahanan nasional semua negara (Zeng, 2022).

Semakin maraknya serangan yang terjadi, tentunya diperlukan sebuah mekanisme untuk melindungi sistem elektronik pada IIV agar operasional IIV tidak terganggu dan dapat menjamin keamanan informasi yang meliputi aspek kerahasiaan, keutuhan dan ketersediaan. Sistem deteksi dini sangat penting dalam mencegah serangan siber karena dapat mengidentifikasi ancaman sebelum mereka berkembang menjadi masalah serius. Dengan kemampuan untuk memantau dan menganalisis lalu lintas jaringan secara *real-time*, sistem ini membantu mendeteksi aktivitas yang mencurigakan serta memungkinkan respon yang cepat.

Penanganan insiden siber menjadi tanggung jawab tim tanggap insiden siber (TTIS). Tim ini merupakan sekelompok orang yang bertanggung jawab menangani insiden siber yang mengganggu atau mengancam berjalannya sistem elektronik. TTIS harus bekerja cepat dan tepat dalam menangani insiden serangan siber karena waktu adalah faktor krusial. Setiap detik yang terlewat dapat memperburuk dampak serangan, seperti kehilangan data atau kerugian finansial. Respon yang cepat memungkinkan tim untuk mengidentifikasi, mengisolasi, dan mengatasi ancaman sebelum menyebar lebih luas. Selain itu, ketepatan dalam menentukan langkah yang tepat untuk mengatasi insiden sangat penting untuk meminimalkan kerusakan dan memastikan sistem kembali berfungsi dengan aman. Untuk mencapai hal ini, tim memanfaatkan berbagai alat yang dirancang untuk mendeteksi dan merespons ancaman secara *real-time*. Berbagai teknologi telah dikembangkan untuk merespon dan menangani insiden serangan siber mulai dari proses deteksi, respon dan pemulihan sistem. Beberapa teknologi tersebut antara lain sistem deteksi instrusksi, sistem pencegahan instruksi, *firewall* generasi lanjut, sistem keamanan *endpoint, security information and event management* dan lain sebagainya. Teknologi ini saling bekerja sama untuk memberikan pengamanan berlapis dalam merespon dan melindungi ancaman siber di era digital. Dengan penggunaan teknologi ini, serta disertai dengan peningkatan kapasitas personil, diharapkan dapat membantu organisasi agar lebih tangguh dalam meminimalkan dan menghadapi serangan siber.

Keterbatasan manusia dalam memproses dan menganalisis data dalam jumlah besar mendorong untuk mengadopsi teknologi yang lebih maju termasuk teknologi kecerdasan buatan/*Artificial Intelligence* (AI) yang saat ini sudah banyak digunakan untuk berbagai macam kepentingan. Dalam beberapa kasus, implementasi kecerdasan artifisial telah mengubah cara manusia berinteraksi dengan teknologi, menghadirkan kemampuan seperti analisis data yang canggih, pemrosesan bahasa alami, dan pembelajaran mesin otomatis (Menkominfo, 2023). 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 (Shamsan Saleh, 2024). Datangnya AI yang menawarkan potensi besar sebagai aset pertahanan digital, AI juga menghadirkan tantangan yang harus dihadapi. (Pongoh et al., 2024). Teknologi kecerdasan buatan (AI) telah berkembang pesat dan berpotensi untuk mendukung berbagai sektor kehidupan. Namun, penerapan AI juga membawa tantangan besar terkait keamanan, privasi, dan kepatuhan terhadap regulasi yang berlaku (Onno W Purbo, 2024). Perangkat lunak AI rentan terhadap serangan kompleks, yang dapat mengakibatkan pengambilan keputusan yang tidak tepat. AI didefinisikan sebagai sistem atau mesin yang dapat meniru fungsi kognitif manusia, seperti belajar, beradaptasi, dan menyelesaikan masalah (Unesco, 2021). Definisi lain dari AI adalah cabang dari ilmu komputer yang berkonsentrasi pada pembuatan mesin yang dapat melakukan peran yang biasanya dilakukan oleh manusia, seperti memecahkan

masalah, membuat keputusan, dan mengadaptasi dengan situasi (Farid et al., 2023). Kebijakan yang mengatur penggunaan AI di Indonesia terdapat pada Surat Edaran Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial. Dalam dunia pendidikan teknologi ini dapat dimanfaatkan untuk menciptakan konten pembelajaran yang inovatif, membantu personalisasi pembelajaran, dan mendukung pembelajaran inklusif. Namun disamping itu, Generative AI juga dapat memberikan dampak negatif jika tidak digunakan secara bijak (Kemendikbudristek, 2024).

Dalam konteks keamanan siber, AI memungkinkan deteksi ancaman yang lebih cepat dan akurat dengan kemampuan memproses data dalam jumlah besar, menganalisis pola, dan mengenali potensi serangan siber yang sulit diidentifikasi oleh metode konvensional. Dengan demikian, penggunaan AI sebagai alat bantu deteksi tidak hanya mempercepat waktu respons, tetapi juga meningkatkan ketepatan dalam mengidentifikasi dan menanggulangi ancaman siber, sehingga mendukung keamanan IIV secara lebih optimal. Penggunaan AI dalam keamanan siber diharuskan mampu mendeteksi ancaman secara otomatis tanpa mengabaikan potensi risiko, termasuk risiko kesalahan deteksi yang bisa mempengaruhi keamanan sistem secara keseluruhan.

Beberapa penelitian/kajian tentang peran AI dalam keamanan siber telah dilakukan sebelumnya, antara lain menyatakan pentingnya mempertimbangkan evolusi teknologi AI dan potensinya untuk mempertahankan kekuatannya di tengah berkembangnya serangan siber (Das & Sandhane, 2021). Disebutkan juga bahwa masa depan perlindungan terhadap serangan siber akan bergantung pada pembaruan AI yang berkelanjutan metode untuk tetap terdepan dalam trik terbaru peretas (Salem et al., 2024). Riset lain menyatakan bahwa AI secara signifikan meningkatkan ketepatan prediksi dan deteksi ancaman anomali, yang dibuktikan dengan hasil survei yang menunjukkan tingkat persetujuan 44,71% dan 62,35%. Hal ini secara keseluruhan berpotensi mempercepat pengambilan keputusan di perusahaan (Jonas et al., 2023). AI berperan dalam membantu organisasi mengambil keputusan berdasarkan informasi mengenai penerapan AI dengan memberikan pandangan yang tidak memihak mengenai dampaknya (Jada & Mayayise, 2024). Meski ada beberapa kekurangan, tapi tetap saja Kecerdasan Buatan memainkan peran penting dalam hal ini keamanan siber (Jenis Nilkanth Welukar & Gagan Prashant Bajoria, 2021).

Dalam konteks ini, kajian tentang peran AI dalam keamanan siber menjadi krusial untuk memahami bagaimana peran teknologi AI ini dapat diimplementasikan secara efektif dalam melindungi sistem elektronik pada sektor IIV dengan tetap memperhatikan aspek-aspek keamanan dan pemenuhan aturan kebijakan. Penelitian ini berfokus pada analisis bagaimana AI dapat memperkuat kemampuan deteksi dan mitigasi ancaman siber serta mempertimbangkan risiko dan tantangan yang muncul.

Berdasarkan rumusan masalahan tersebut, dibuatlah garis besar pertanyaan penelitian yang akan dijawab dalam jurnal ini, antara lain:

a. Bagaimana peran AI dalam memperkuat keamanan pada IIV?
b. Bagaimana potensi peluang dan tantangan yang ditimbulkan dari pemanfaatan AI dalam mengamankan IIV?
c. Bagaimana strategi dalam mewujudkan AI sebagai upaya untuk membantu mewujudkan keamanan siber pada sektor IIV di Indonesia di Indonesia?

Berdasarkan rumusan masalah tersebut, maka tujuan dari penelitian ini adalah sebagai berikut:

a. Menggambarkan peranan AI dalam memperkuat keamanan siber pada IIV
b. Melakukan analisis potensi peluang dan tantangan yang ditimbulkan dari pemanfaatan AI dalam mengamankan IIV
c. Merumuskan strategi dalam mewujudkan AI sebagai upaya untuk membantu mewujudkan keamanan siber pada sektor IIV di Indonesia di Indonesia.

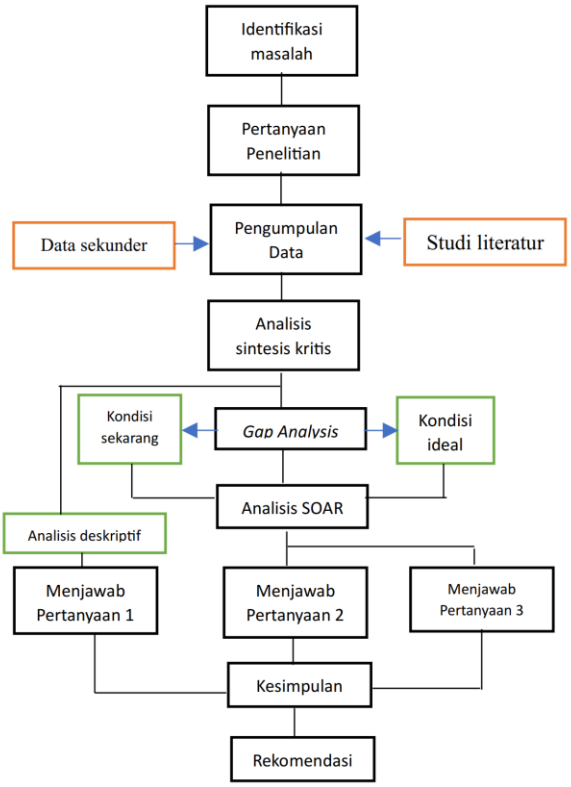
METODE PENELITIAN

Penelitian ini menggunakan metodologi *systematic literature review* (SLR) dengan melakukan proses identifikasi, melakukan kajian dan evaluasi seluruh temuan penelitian yang relevan untuk menjawab pertanyaan penelitian. Penelitian ini terdiri dari beberapa langkah antara lain merumuskan pertanyaan penelitian, mengkaji literatur, menentukan kriteria inklusi dan eksklusi, memilih literatur, menyajikan data, menyiapkan data, dan menarik kesimpulan (Pongoh et al., 2024). Teknik pengumpulan data dilakukan pada bulan November 2024 melalui studi literatur dari sumber yang relevan dan memenuhi kriteria antara lain berasal dari sumber resmi, relevan, dalam

periode yang ditentukan yang meliputi laporan hasil monitoring kemanan siber BSSN, artikel jurnal dan buku.

Teknis analisis yang digunakan dalam penelitian ini adalah teknis sintesis kritis, *gap analysis* dan analisis SOAR.

a. Sintesis kritis dengan mengintegrasikan berbagai sumber data untuk menghasilkan temuan baru dengan cara mengidentifikasi, mengevaluasi, dan menghubungkan berbagai konsep (Depraetere et al., 2021).
b. *Gap analysis* untuk memetakan kondisi saat ini dan kondisi ideal. *Gap Analysis* atau analisis kesenjangan digunakan untuk mengetahui kesenjangan antara persepsi dan ekspektasi serta mengidentifikasi tindakan yang diperlukan agar mampu mengurangi kesenjangan tersebut dan mencapai kinerja yang diharapkan pada masa mendatang. (Mutmainah et al., 2022)
c. Analisis SOAR (*Strengths, Opportunities, Aspirations, Results*), merupakan pendekatan strategi bisnis yang berfokus pada elemen positif yang sudah ada dalam sebuah usaha dan dijadikan sebagai keunggulan utama (Rothwell et al., 2015). SOAR menampilkan pendekatan disiplin untuk membantu organisasi mengidentifikasi kekuatannya dengan memperhatikan apa yang terbaik untuk diterapkan peluang untuk pertumbuhan (Stavros & Cole, 2013). Metode ini membantu merumuskan strategi yang efektif dalam memanfaatkan AI untuk meningkatkan keamanan siber di Indonesia dengan cara memetakan setiap komponen strategi sebagai berikut: *Strengths* (Kekuatan): Mengidentifikasi keunggulan teknologi AI, seperti kemampuan analisis data besar dan deteksi pola anomali. *Opportunities* (Peluang): Mencari peluang penerapan AI, termasuk peningkatan dalam respons terhadap ancaman siber dan pengembangan sistem keamanan yang lebih canggih. *Aspirations* (Aspirasai): Menetapkan tujuan untuk meningkatkan keamanan siber melalui integrasi AI yang lebih luas. *Results* (Hasil): Mengukur hasil penerapan AI dalam mengurangi insiden keamanan dan meningkatkan kesadaran siber. Berikut merupakan kerangka berpikir penelitian ini dengan melakukan adaptasi alur kerangka penelitian dengan metode sejenis yang berjudul Tinjauan Strategis Kemanan Siber Indonesia-Teknologi *Cloud* dan Tata Kelola Data (Politeknik Siber dan Sandi Negara& Universitas Indonesia, 2019):



Gambar 3. Kerangka Penelitian

Kerangka penelitian diawali dengan melakukan identifikasi masalah terkait dengan lanskap keamanan siber di Indonesia dan ancaman-ancamanya. Setalah itu melakukan identifikasi permasalahan, kemudian merumuskan pertanyaan penelitian. Sumber data pada studi literatur ini berupa laporan tren keamanan siber, jurnal ilmiah yang relevan dengan topik penelitian. Data ini kemudian diolah dan dianalisis dengan menggunakan mengintegrasikan berbagai sumber data untuk menghasilkan temuan dengan cara mengidentifikasi, mengevaluasi, dan menghubungkan berbagai konsep. Hasil analisis data digunakan untuk memetakan kondisi saat ini dan kondisi ideal melalui *gap analysis*. Kondisi ini akan dianalisis menggunakan metode analisis SOAR untuk menjawab pertanyaan penelitian 2 dan pertanyaan penelitian 3. Dari hasil jawaban pertanyaan penelitian akan didapatkan sebuah kesimpulan dan alternatif rekomendasi strategi.

HASIL DAN PEMBAHASAN

Kondisi Saat Ini

Berdasarkan laporan hasil monitoring yang dilakukan oleh BSSN dalam lima tahun terakhir (2019-2023) kondisi keamanan siber menunjukkan dinamika yang signifikan baik dari segi volume maupun teknik yang digunakan. Berikut disajikan

data hasil monitoring keamanan siber pada sektor IIV di Indonesia:

a. Sektor administasi pemerintah
   Sektor administrasi pemerintahan adalah salah satu target utama serangan siber di Indonesia. Menurut data hasil monitoring BSSN, lebih dari 400 juta potensi serangan siber terjadi di Indonesia pada tahun 2023, banyak di antaranya menargetkan situs dan sistem pemerintah dengan serangan *defacement, phishing, dan Distributed Denial of Service* (DDoS). Serangan terhadap sektor ini mengancam integritas data pemerintah, mengganggu layanan publik, dan dapat menurunkan kepercayaan publik.
b. Sektor energi dan sumber daya mineral
   Sektor energi sangat rentan terhadap serangan siber, terutama pada sistem kontrol industri yang digunakan dalam pengelolaan pembangkit listrik dan jaringan distribusi. Serangan terhadap sektor ini dapat menyebabkan gangguan listrik yang luas dan berdampak besar pada sektor ekonomi dan sosial. BSSN mencatat bahwa sektor energi di Indonesia mulai meningkatkan sistem keamanan setelah beberapa kali mengalami serangan malware yang mengancam kestabilan jaringan energi.
c. Sektor transportasi
   Di sektor transportasi, khususnya bandara dan sistem kereta api, serangan siber dapat mengganggu operasi dan menimbulkan risiko keamanan publik. Sistem manajemen transportasi yang dikendalikan melalui jaringan digital rentan terhadap peretasan.
d. Sektor keuangan
   Sektor keuangan, termasuk perbankan dan asuransi, merupakan salah satu sektor yang paling sering diserang. Serangan dalam bentuk phishing, malware, dan carding kerap digunakan untuk mencuri data nasabah dan dana, yang mengakibatkan kerugian langsung pada institusi dan masyarakat.
e. Sektor Kesehatan
   Sektor kesehatan juga mengalami peningkatan signifikan dalam serangan siber, terutama sejak pandemi COVID-19. Rumah sakit dan pusat data kesehatan diserang untuk mengeksploitasi data pasien dan informasi medis penting. Serangan ransomware di rumah sakit dapat mengakibatkan terganggunya layanan kesehatan, berdampak pada keselamatan pasien, dan menyebabkan kerugian finansial karena biaya tebusan yang diminta.
f. Sektor pangan
   Meskipun jarang terekspos secara luas, sektor pangan juga mengalami ancaman siber. Sistem rantai pasokan dan logistik yang terhubung secara digital berpotensi mengalami gangguan jika diserang, mengakibatkan potensi kekurangan distribusi pangan dan kerugian ekonomi pada sektor ini.
g. Sektor informasi dan teknologi (TIK)
   Sektor TIK, yang mencakup jaringan telekomunikasi dan data, berperan penting sebagai tulang punggung infrastruktur vital lainnya. Serangan pada sektor ini, seperti DDoS atau peretasan jaringan telekomunikasi, dapat mengakibatkan gangguan komunikasi yang meluas dan mempengaruhi layanan publik serta sektor bisnis.
h. Sektor pertahanan
   Sektor pertahanan sangat rentan terhadap serangan spionase siber, yang bertujuan untuk mencuri informasi rahasia atau melemahkan kemampuan pertahanan negara.

Kondisi Ideal

Dalam memetakan kondisi ideal keamanan siber ini, penulis menggunakan kerangka kerja keamanan siber *National Institute of Standards and Technology* (NIST) yang terdiri dari identifikasi, proteksi, deteksi, respon dan *recover* (NIST, 2024). Identifikasi merupakan tahap ini menekankan pentingnya memahami aset, data, perangkat, serta hubungan bisnis dan risiko yang berkaitan. Proteksi menerapkan langkah-langkah untuk melindungi aset dan data penting. Ini termasuk kontrol akses, perlindungan data, kesadaran karyawan, dan pemeliharaan keamanan untuk meminimalkan dampak dari potensi serangan. Deteksi merupakan tahap yang berfokus pada kemampuan organisasi untuk mendeteksi insiden siber secara cepat. Respon mencakup komunikasi, analisis kejadian, mitigasi dampak, dan pembelajaran untuk mencegah kejadian serupa di masa mendatang. Recover merupakan tahap terakhir mencakup langkah-langkah untuk memulihkan sistem dan layanan yang terdampak serangan.

Gambar 4. *NIST Cyber Security Fram*

Salah satu contoh implementasi penerapan tata kelola keamanan siber yakni program pengembangan pedoman keamanan siber komprehensif yang dirancang khusus untuk industri industri Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital, dan Aset Kripto (ITSK) pada instansi Otoritas Jasa Keuangan (OJK). OJK menerbitkan Pedoman Keamanan Siber untuk Industri ITSK yang bertujuan untuk menumbuhkan ekosistem keuangan digital yang seimbang dalam mendorong inovasi dan kerangka manajemen risiko siber. Pedoman tersebut mencakup beberapa area penting (1) Perlindungan data yang mencakup enkripsi data dan penyimpanan data (2) Manajemen risiko, yang mencakup penilaian risiko (3) Respons insiden, yangmencakup deteksi, respons, dan strategi pemulihan (4) Penilaian kematangan, yang mencakup penilaian berkala untuk memastikan bahwa langkah-langkah keamanan siber efektif dan terbaru (5) Program pembangunan kapasitas dan kolaborasi, yang mencakup inisiatif untuk mendidik pemangku kepentingan serta kerja sama antara pelaku industri dan regulator untuk meningkatkan implementasi keamanan siber (Otoritas Jasa Keuangan, 2024). Secara umum kondisi ideal keamanan siber dapat dicapai apabila telah memenuhi semua kriteria yang diterapkan, berikut merupakan gambaran kondisi ideal peran AI bagi organisasi dalam menerapkan tata kelola keamanan siber:

a. Identifikasi
   Fase identifikasi melibatkan pemahaman yang mendalam tentang risiko dan aset yang dimiliki oleh organisasi yang meliputi penilaian aset, manajemen risiko dan kepatuhan terhadap kebijakan. Kondisi ideal dalam fase identifikasi yaitu adanya pemahaman yang jelas tentang aset dan risiko, serta dokumentasi yang komprehensif mengenai kebijakan keamanan yang diterapkan. AI berperan dalam membantu memproses data yang besar dan kompleks untuk mengidentifikasi pola serangan.
b. Proteksi
   Fase proteksi meliputi langkah-langkah proaktif untuk melindungi aset informasi dari ancaman, diantaranya melalui penerapan kontrol akses, mengamankan data, melaksanakan pelatihan dan kesadaran keamanan informasi. Kondisi ideal adalah penerapan langkah-langkah perlindungan yang komprehensif dan terintegrasi, yang dapat meminimalkan potensi dampak dari serangan siber. AI berperan dalam memperkuat langkah perlindungan siber dengan otomatisasi kontrol akses berbasis perilaku, enkripsi data secara dinamis.
c. Deteksi
   Fungsi deteksi berfokus pada kemampuan organisasi untuk mengidentifikasi kejadian keamanan siber dengan cepat, yang meliputi sistem pemantauan dan monitoring, audit dan analisis serta menerapkan sistem deteksi dini. Kondisi ideal adalah memiliki sistem deteksi yang responsif dan efektif, yang mampu mengidentifikasi ancaman sebelum menyebabkan kerugian yang signifikan. AI membantu memantau jaringan secara terus menerus untuk mendeteksi perilaku yang tidak biasa serta memproses log dalam jumlah besar dengan cepat serta mengurangi *false positif* dengan menyaring ancaman yang relevan.
d. Respon
   Tahap respons melibatkan tindakan yang diambil setelah terjadinya insiden keamanan. Kondisi ideal adalah organisasi memiliki kemampuan respons yang cepat dan efisien, sehingga dampak dari insiden dapat diminimalkan dan sistem dapat segera dipulihkan. AI membantu memfasilitasi respon cepat dan terukur terhadap insiden keamanan siber
e. *Recover*
   Kondisi ideal pada tahap pemulihan mencakup langkah-langkah untuk memperbaiki dan memulihkan sistem setelah terjadinya insiden. Kondisi ideal adalah organisasi memiliki proses pemulihan yang terencana dan efisien, memungkinkan pemulihan operasional yang cepat serta memperkuat ketahanan terhadap serangan di masa mendatang. AI dapat mengidentifikasi akar permasalahan insiden dan memberikan rekomendasi untuk pencegahannya, serta memanfaatkan data historis untuk mengembangkan strategi pemulihan yang lebih efektif.

Peranan AI Dalam Memperkuat Keamanan Siber Pada Sektor IIV

Serangan siber di Indonesia telah meningkat dalam beberapa tahun terakhir, menunjukkan betapa pentingnya perlindungan terhadap infrastruktur informasi vital. Beberapa negara di dunia telah memanfaatkan AI dalam upaya pengamanan siber, misalnya Amerika Serikat. Sistem AI digunakan oleh perusahaan energi untuk melindungi grid listrik nasional dari ancaman siber. AI mendeteksi serangan DDoS pada sistem pengelolaan energi sebelum memengaruhi distribusi listrik. Sistem otomatisasi berbasis AI mengisolasi bagian yang terinfeksi dari jaringan untuk mencegah penyebaran serangan. Negara lain misalnya Inggris memanfaatkan AI dalam sistem kereta api nasional untuk melindungi infrastruktur transportasi dari ancaman siber untuk memantau dan mendeteksi ancaman pada sistem kontrol otomatis kereta. AI mendeteksi percobaan akses tidak sah ke jaringan kontrol kereta dan secara otomatis memblokir aktivitas tersebut serta mencegah penundaan atau kecelakaan akibat manipulasi sistem transportasi digital. Rumah sakit di negara-negara Uni Eropa, seperti Jerman, menggunakan AI untuk melindungi data pasien. AI berbasis *natural language processing (NLP)* digunakan untuk mengenkripsi data pasien dan memantau akses ke sistem rekam medis elektronik. Kemampuan mempelajari pola akses data normal dan mendeteksi aktivitas mencurigakan dengan cepat. Di negara Singapura, AI digunakan dalam proyek *Smart Nation* untuk melindungi infrastruktur teknologi, termasuk kamera pengawasan dan sistem manajemen lalu lintas.

Sektor-sektor kritis menjadi target utama serangan siber. Sebagai contoh, sektor kesehatan dihadapkan pada serangan ransomware yang mengakibatkan gangguan pada layanan medis dan kehilangan data pasien. Serangan semacam ini menunjukkan pentingnya sistem keamanan yang tangguh dan adaptif. Teknologi AI dapat digunakan untuk meningkatkan keamanan sektor-sektor kritis ini dengan menerapkan analitik prediktif. Dengan memanfaatkan data historis dan tren serangan, AI dapat memprediksi potensi ancaman dan secara proaktif menerapkan langkah-langkah perlindungan. Selain itu, AI dapat membantu dalam pemulihan data yang terpengaruh oleh serangan ransomware, melalui teknik pemulihan yang lebih efisien.

Salah satu tantangan utama yang dihadapi oleh banyak organisasi di Indonesia adalah keterbatasan dalam deteksi dan respons terhadap serangan siber. Banyak insiden keamanan tidak terdeteksi hingga setelah kerusakan terjadi, mengakibatkan kerugian yang signifikan. AI dapat meningkatkan kemampuan deteksi dengan menerapkan sistem pemantauan berkelanjutan yang menggunakan analisis perilaku pengguna dan entitas. Dengan memanfaatkan AI, sistem dapat mengidentifikasi aktivitas yang tidak biasa dengan cepat dan merespons secara otomatis, sehingga mengurangi waktu respons dan meminimalkan dampak dari serangan.

Potensi Peluang Dan Tantangan Yang Ditimbulkan Dari Pemanfaatan AI Kaitanya Dengan Ancaman Serangan Siber

Penerapan teknologi AI dalam menjaga keamanan siber pada sektor IIV menghadirkan peluang besar sekaligus tantangan yang signifikan. Melalui analisis SOAR, dapat dilihat bagaimana penerapan AI mampu memperkuat ketahanan siber nasional dengan cara memanfaatkan kekuatan yang dimiliki, mengambil peluang yang ada, mencapai aspirasi yang diharapkan, serta menghasilkan dampak positif dalam jangka panjang. Berikut adalah tabel strategi SOAR untuk memetakan potensi risiko dan ancaman dalam penggunaan teknologi AI dalam mengamankan informasi dari serangan siber:

Tabel 1. Tabel Pemetaan SOAR

Komponen	Strategi
Strengths	AI mampu mendeteksi aktivitas mencurigakan dan pola anomali secara *real-time*, memungkinkan respons cepat terhadap ancaman.
	Pembelajaran mesin pada AI memungkinkan identifikasi pola serangan yang berulang, membantu memprediksi dan mencegah ancaman yang mungkin terjadi.
	AI dapat merespons secara otomatis dan mengisolasi ancaman sebelum terjadi kerusakan yang signifikan.
	AI dapat menganalisis data dalam jumlah besar dengan cepat, memungkinkan pemetaan risiko yang lebih akurat.
Opportunities	Integrasi AI dengan sistem keamanan yang ada membuka peluang untuk menciptakan solusi keamanan yang lebih efisien dan inovatif.
	Adopsi AI dalam keamanan siber dapat mendorong kolaborasi antara pemerintah, sektor swasta, dan institusi akademik untuk berbagi pengetahuan dan praktik terbaik

Komponen	Strategi
	Automasi dengan AI dapat mengurangi beban tugas rutin bagi tim keamanan, memungkinkan mereka untuk fokus pada pengambilan keputusan strategis.
	Pemanfaatan AI dapat lebih efektif dalam melindungi sektor-sektor vital
Aspirations	Aspirasi untuk menciptakan sistem keamanan yang dapat menyesuaikan diri secara otomatis dengan lanskap ancaman yang berubah cepat.
	Dengan meningkatkan keamanan melalui AI, tujuan jangka panjang adalah meningkatkan kepercayaan publik terhadap sistem keamanan digital.
	Peningkatan kemampuan AI dalam mengamankan infrastruktur vital bertujuan untuk membangun ketahanan siber nasional yang lebih kuat.
	Terus mengembangkan teknologi AI dalam keamanan siber untuk selalu dapat mengantisipasi ancaman yang semakin canggih.
Results	Implementasi AI yang efektif meningkatkan ketahanan terhadap serangan siber, sehingga sistem lebih terlindungi dari potensi kerugian dan ancaman.
	Dengan mendeteksi dan mencegah ancaman sejak dini, AI berkontribusi pada pengurangan risiko serta biaya perbaikan setelah insiden terjadi.
	AI membantu mempercepat waktu respons terhadap serangan, mengurangi dampak yang mungkin timbul dari serangan tersebut.
	AI memungkinkan terciptanya sistem keamanan berbasis data yang terintegrasi dan berkelanjutan, sehingga sistem keamanan dapat terus diperbarui berdasarkan data ancaman terbaru.

Strategi Dalam Mewujudkan AI Sebagai Upaya Untuk Membantu Mewujudkan Keamanan Siber Pada Sektor IIV

Setelah melakukan identifikasi terhadap faktor-faktor dalam SOAR, selanjutnya merumuskan strategi dalam memanfaatkan kekuatan internal dan peluang eksternal dengan tujuan yang jelas dalam penerapan AI, yang pada akhirnya berfokus pada penguatan keamanan infrastruktur informasi vital dari ancaman siber. Strategi ini menekankan efisiensi, kolaborasi, otomatisasi, dan pengembangan SDM untuk mencapai ketahanan siber nasional yang lebih baik. Strategi ini terdiri dari 4 kuadran yakni strategi SA (*Strengths-Aspirations*), SR (*Strengths-Results*), OA (*Opportunities-Aspirations*), dan OR (*Opportunities-Results*). Berikut merupakan hasil pemetaan tabel 4 kuadran perumusan strategi SOAR:

Tabel 2. Tabel Alternatif Strategi

Intern. / Ekst.	***Strengths***	***Opportunities***
Aspirations	Memanfaatkan dan memaksimalkan sumber daya riset dan pengembangan di Indonesia untuk menciptakan model AI yang sesuai dengan kebutuhan keamanan siber nasional serta melakukan kolaborasi dengan BRIN dalam penetapan kebijakan standar AI yang aman.	Memanfaatkan peluang kerjasama dengan negara lain yang memiliki teknologi AI maju untuk mencapai aspirasi keamanan siber nasional. Menerapkan teknologi AI adaptif untuk memenuhi aspirasi perlindungan siber terhadap ancaman yang terus berkembang.
Results	Meningkatkan sistem pengelolaan data keamanan yang didukung AI, sehingga hasil pemantauan dapat tercapai sesuai standar yang ditetapkan	Menggunakan peluang untuk mengevaluasi hasil kebijakan AI secara berkala guna menyesuaikan kebijakan terhadap kebutuhan yang berkembang.

Tabel strategi 4 kuadran di atas menyajikan beberapa alternatif pilihan strategi yang dapat diambil dalam pemanfaatan peranan AI dalam mengamankan IIV daris erangan siber dengan penjelasan sebagai berikut:

a. Strategi SA
   Strategi SA berfokus pada pemanfaatan kekuatan dari teknologi dan riset AI di Indonesia untuk mencapai aspirasi keamanan siber yang lebih tangguh dan mandiri sesuai dengan visi nasional. Strategi ini memaksimalkan potensi AI di Indonesia untuk mendukung aspirasi jangka panjang di bidang keamanan siber.

b. Strategi SR
   Strategi SR mengacu pada pemanfaatan kekuatan teknologi AI untuk mencapai hasil konkret dalam memperkuat keamanan siber. Dengan kekuatan yang ada, Indonesia dapat memastikan hasil yang konsisten dengan

standar keamanan nasional. Strategi ini memanfaatkan kekuatan AI untuk menciptakan hasil nyata dalam keamanan siber yang bisa diukur dan dilaporkan.

c. Strategi OA
   Strategi OA berfokus pada pemanfaatan peluang eksternal untuk memenuhi aspirasi keamanan siber Indonesia yang lebih baik dan selaras dengan kebijakan nasional. Strategi ini mengoptimalkan peluang eksternal untuk mewujudkan aspirasi Indonesia dalam menciptakan keamanan siber yang adaptif dan modern.
b. Strategi OR
   Strategi OR memanfaatkan peluang eksternal untuk menghasilkan hasil yang diinginkan, serta mengukur dampak dari penerapan AI dalam keamanan siber. Strategi ini menggunakan peluang eksternal untuk mencapai hasil nyata dalam penerapan AI, dengan pengukuran dan evaluasi yang berkelanjutan untuk meningkatkan efektivitasnya.

Strategi-strategi di atas dirancang untuk memastikan bahwa pemanfaatan AI dalam keamanan siber pada sektor IIV di Indonesia sejalan dengan kebijakan dan peraturan yang berlaku di Indonesia, memungkinkan pengembangan yang berkelanjutan dan aman serta pencapaian hasil yang dapat diukur untuk memperkuat keamanan nasional. Pemilihan strategi yang paling sesuai akan didasarkan pada analisis yang objektif dan terukur, yang mempertimbangkan berbagai aspek yang relevan dalam konteks keamanan siber dan kebijakan AI di Indonesia. Adapun pemilihan strategi yang paling sesuai menggunakan pertimbangan dari sisi efektivitas yakni sejauh mana strategi yang dipilih akan membantu mencapai tujuan keamanan siber dalam infrastruktur informasi vital.

KESIMPULAN DAN SARAN

Dari analisis data dan alternatif strategi yang dihasilkan, dapat diambil kesimpulan bahwa teknologi AI memiliki peranan penting dalam memperkuat keamanan siber pada sektor IIV di Indonesia. Dengan meningkatnya jumlah serangan siber yang kompleks, kebutuhan untuk menerapkan teknologi canggih seperti AI menjadi semakin mendesak. AI dapat meningkatkan postur keamanan siber mulai dari fase identifikasi, proteksi, deteksi, respon dan *recover* terhadap ancaman siber, memperbaiki pengelolaan ancaman, dan memfasilitasi pembelajaran berkelanjutan untuk menghadapi teknik serangan yang terus berkembang. Namun, tantangan juga harus diperhatikan, termasuk kebutuhan untuk terus mengembangkan teknologi AI yang responsif terhadap ancaman yang semakin canggih, serta pentingnya menciptakan sistem yang transparan dan dapat dipercaya oleh publik. Pemanfaatan teknologi AI untuk mengamankan sektor IIV di Indonesia menunjukkan bahwa terdapat empat kemungkinan strategi yang dapat diambil (SA,SR, OA atau OR) dimana masing-masing strategi memiliki fokus dan tujuan yang berbeda, tetapi semuanya bertujuan untuk memperkuat keamanan siber nasional.

Berikut merupakan saran yang relevan dengan hasil kajian:

a. Pengembangan model AI yang transparan
   Penting untuk merancang algoritma AI yang dapat dipahami dan dijelaskan. Transparansi dalam proses pengambilan keputusan AI akan membantu *stakeholder* memahami bagaimana dan mengapa keputusan tertentu dibuat, sehingga meningkatkan kepercayaan terhadap teknologi ini.
b. Audit dan penilaian berkala
   Melakukan audit secara berkala terhadap sistem AI untuk memastikan bahwa tidak ada bias dalam algoritma dan bahwa teknologi tersebut beroperasi sesuai dengan norma dan etika yang telah ditetapkan. Penilaian ini harus mencakup evaluasi terhadap data yang digunakan untuk pelatihan model, memastikan bahwa data tersebut representatif dan tidak mengandung diskriminasi.
c. Penggunaan data yang etis
   Organisasi harus memastikan bahwa data yang digunakan untuk melatih model AI diperoleh dengan cara yang etis, mematuhi regulasi perlindungan data, dan menghormati privasi individu. Kebijakan privasi yang jelas dan prosedur untuk mendapatkan izin data harus diterapkan.
d. Pelatihan dan keterampilan SDM
   Memberikan pelatihan yang tepat kepada tim keamanan siber untuk memahami cara kerja dan keterbatasan AI. Keterampilan dalam analisis data dan pengoperasian sistem AI sangat penting untuk memastikan bahwa penggunaan teknologi ini dilakukan dengan benar dan efektif.
e. Penerapan kebijakan dan standar keamanan yang ketat
   Mengembangkan dan menerapkan kebijakan keamanan yang ketat untuk penggunaan AI

dalam keamanan siber, termasuk pedoman tentang bagaimana sistem harus beroperasi, tanggung jawab dalam pengambilan keputusan, serta prosedur untuk penanganan insiden. Penting untuk menjaga AI tetap terkendali dengan mempertimbangkan risiko yang dapat timbul, seperti kebocoran data, pelanggaran privasi, dan potensi bias dalam pengambilan keputusan oleh sistem AI.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2023). Peraturan BSSN No.8 Tahun 2023 Kerangka Kerja Pelindungan Infrastruktur Informasi Vital. In *Bssn* (1st ed.). Badan Siber dan Sandi Negara.

Badan Siber Dan Sandi Negara. (2023). *Lanskap Keamanan Siber Indonesia Tahun 2023* (Badan Siber dan Sandi Negara (ed.); 1st ed., Issue 70). Badan Siber dan Sandi Negara.

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

Farid, I., Reksoprodjo, A. H., & Suhirwan. (2023). Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* , *10*(2), 779–788. http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Jenis Nilkanth Welukar, & Gagan Prashant Bajoria. (2021). Artificial Intelligence in Cyber Security - A Review. *International Journal of Scientific Research in Science and Technology*, 488–491. https://doi.org/10.32628/ijsrst218675

Joke Depraetere, Christopher Vandeviver, Ines Keygnaert, & Tom Vander Beken. (2020). The Critical Interpretive Syntesis: an assessment of reporting practices. 669-689. https://doi.org/10.1080/13645579.2020.1799637

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), 83–91. https://doi.org/10.33050/itee.v2i1.428

Kemendikbudristek. (2024). Panduan Penggunaan Generative Artificial Intelligence (Genai). *Panduan Penggunaan Generative Artificial Intelligence (Genai) Pada Pembelajaran Di Perguruan Tinggi*.

Menkominfo. (2023). Pelaku Usaha Aktivitas. In *Surat Edaran Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial* (pp. 1–10).

Mutmainah, I., Yulia, I. A., Marnilin, F., & Mahfudi, A. Z. (2022). GAP Analysis Untuk Mengetahui Kinerja Implementasi Program Merdeka Belajar Kampus Merdeka. *Jurnal Ilmiah Manajemen Kesatuan*, *10*(1), 19–34. https://doi.org/10.37641/jimkes.v10i1.934

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, *NIST CSWP*(1), 6–26. https://doi.org/10.6028/NIST.CSWP.29

Onno W Purbo. (2024). Menjaga AI Tetap Terkendali : Compliance dalam Era Teknologi Cerdas. *Menjaga AI Tetap Terkendali : Compliance Dalam Era Teknologi Cerdas*, *1*.

Otoritas Jasa Keuangan. (2024). Pengembangan dan Penguatan Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital dan Aset Kripto. Otoritas Jasa Keuangan.

Peraturan Presiden (PERPRES) Nomor 82 Tahun 2022 Tentang Pelindungan Infrastruktur Informasi Vital, BSSN 1 (2022).

Politeknik Siber dan Sandi Negara. (2019). Tinjauan Strategis Kemanan Siber Indonesia (Teknologi Cloud dan Tata Kelola Data). *Tinjauan Strategis Kemanan Siber Indonesia (Teknologi Cloud Dan Tata Kelola Data)*, *11*(1), 1–14. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

Pongoh, A. G., Fahreza, R. A., Kindi, B. Al, Pribadi, F. S., & Ajie, R. (2024). *Systematic Literature Review (SLR): Dampak Pemanfaatan Artificial Intelligence untuk*

Meningkatkan Cyber Security Systematic Literature Review (SLR): The Impact of Utilizing Artificial Intelligence to Enhance Cyber Security. *7*(1), 34–41.

Rothwell, W. J., Stavros, J. M., & Sullivan, R. L. (2015). Practicing Organization Development: Leading Transformational Change: Fourth Edition. *Practicing Organization Development: Leading Transformational Change: Fourth Edition*, 1–480. https://doi.org/10.1002/9781119176626

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

Shamsan Saleh, A. M. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*, *5*(3), 100193. https://doi.org/10.1016/j.bcra.2024.100193

Stavros, J., & Cole, M. (2013). SOARing Towards Positive Transformation and Change. *Development Policy Review*, *1*(November 2013), 10–34. https://www.researchgate.net/publication/259975881_SOARing_towards_positive_transformation_and_change

Unesco. (2021). UNESCO. In *Recommendation on the Ethics of Artificial Intelligence: Vol. SHS/BIO/PI* (Issue November).

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