IMPLEMENTASI AI-POWERED INTRUSION DETECTION SYSTEMS UNTUK MENDETEKSI ANCAMAN KEAMANAN PADA BIG DATA

Dwi Putri Amanda[*1], Eriene Dheanda Absharina[2]
[1,2]Sistem Informasi, UIN Raden Fatah Palembang
e-mail: : [1]2120803030@radenfatah.ac.id, [2]erienedheanda@itsnusriwijaya.ac.id*

Big Data menawarkan banyak manfaat, tetapi juga menimbulkan tantangan besar dalam keamanan, seperti ancaman siber yang semakin kompleks dan sulit terdeteksi. Sistem Deteksi Intrusi (Intrusion Detection System/IDS) tradisional sering kewalahan menangani volume data yang besar dan pergerakannya yang cepat. Penelitian ini mengusulkan penerapan IDS berbasis kecerdasan buatan (AI-powered IDS) untuk mendeteksi ancaman secara lebih efektif dan cepat. Sistem ini menggunakan algoritma machine learning untuk mengenali pola anomali dalam data dan mengurangi kesalahan deteksi (false positive). Hasil penelitian berdasarkan studi literatur menunjukkan bahwa AI-powered IDS meningkatkan akurasi deteksi dibandingkan dengan sistem tradisional. Dengan pendekatan ini, sistem keamanan Big Data dapat lebih siap menghadapi berbagai ancaman secara proaktif dan efisien.

***Kata Kunci*— Big Data, Sistem Deteksi Intrusi, Keamanan Siber, Kecerdasan Buatan, Machine Learning.**

I. PENDAHULUAN

Perkembangan Big Data telah membawa banyak manfaat dalam berbagai bidang, seperti bisnis, kesehatan, dan pemerintahan. Namun, peningkatan penggunaan data dalam jumlah besar juga memunculkan risiko keamanan siber. Ancaman seperti serangan malware, pencurian data, dan akses tidak sah kini semakin sulit diidentifikasi karena sifat data yang masif dan bergerak cepat. Oleh karena itu, diperlukan sistem keamanan yang mampu mendeteksi ancaman secara akurat dan tepat waktu agar infrastruktur Big Data tetap terlindungi.

Sistem Deteksi Intrusi (Intrusion Detection System/IDS) merupakan salah satu solusi yang umum digunakan untuk mengidentifikasi aktivitas mencurigakan dalam jaringan dan sistem. Sayangnya, IDS konvensional sering kali tidak efektif ketika diterapkan pada lingkungan Big Data. Hal ini disebabkan oleh keterbatasan sistem tradisional dalam menangani volume data yang besar dan kompleksitas pola serangan yang terus berkembang. Sistem tersebut juga sering menghasilkan false positive, yaitu deteksi ancaman palsu, yang mengurangi efisiensi operasional.

Untuk mengatasi keterbatasan ini, penggunaan kecerdasan buatan (AI) menjadi alternatif yang menjanjikan. AI-powered IDS menggabungkan teknik machine learning dan deep learning untuk mempelajari pola serangan baru dan mendeteksi aktivitas anomali dalam data secara otomatis. Teknologi ini memungkinkan sistem keamanan untuk terus beradaptasi dan berkembang seiring perubahan pola ancaman, sehingga lebih efektif dibandingkan metode tradisional.

Implementasi AI-powered IDS memiliki keunggulan dalam mendeteksi ancaman dengan lebih cepat dan akurat. Sistem ini tidak hanya mampu mengurangi jumlah false positive, tetapi juga dapat memproses data dalam jumlah besar secara real-time. Dengan kemampuan tersebut, perusahaan dan organisasi dapat lebih proaktif dalam mengamankan aset digital mereka, sehingga potensi kerugian akibat serangan siber dapat diminimalkan.

Penelitian ini bertujuan untuk mengevaluasi efektivitas penerapan AI-powered IDS dalam mendeteksi ancaman keamanan pada ekosistem Big Data. Dengan menguji kinerja dan akurasinya, diharapkan solusi ini dapat menjadi rekomendasi bagi organisasi yang ingin meningkatkan sistem keamanan mereka. Temuan dalam penelitian ini menunjukkan bahwa AI-powered IDS mampu meningkatkan deteksi yang lebih akurat dibandingkan sistem tradisional, sehingga dapat menjadi langkah proaktif dalam menghadapi ancaman keamanan di masa depan.

II. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur, yaitu pengumpulan dan analisis informasi dari berbagai sumber tertulis, seperti buku, jurnal ilmiah, artikel konferensi, laporan penelitian, dan situs web terpercaya. Metode ini bertujuan untuk memahami konsep, teknologi,

dan perkembangan terbaru terkait implementasi AI-powered Intrusion Detection System (IDS) dan keamanan Big Data. Dengan memanfaatkan sumber-sumber yang relevan, penelitian ini dapat memberikan landasan teori yang kuat dan memperlihatkan tren serta tantangan yang ada di bidang tersebut [1].

Langkah pertama dalam studi literatur ini adalah mengidentifikasi kata kunci, seperti big data, sistem deteksi intrusi, keamanan siber, kecerdasan buatan, machine learning. Kata kunci ini digunakan untuk mencari literatur yang relevan dari berbagai database ilmiah. Selain itu, penelitian juga menyeleksi artikel atau laporan yang memiliki fokus pada solusi keamanan berbasis kecerdasan buatan dan penerapannya pada Big Data, dimana Studi literatur itu sendiri bertujuan untuk mengkaji secara teoretis kerangka kerja atau model yang digunakan untuk menyelesaikan masalah tertentu [2].

Setelah pengumpulan literatur, langkah berikutnya adalah membaca dan menganalisis isi setiap sumber secara kritis. Penelitian ini mencari informasi penting, seperti jenis ancaman yang sering terjadi dalam ekosistem Big Data, keterbatasan IDS tradisional, dan bagaimana AI dapat meningkatkan performa deteksi ancaman. Literatur yang sudah dikumpulkan kemudian dibandingkan untuk menemukan pola, kesenjangan, dan potensi solusi yang dapat diusulkan.

Proses analisis juga melibatkan identifikasi kelebihan dan kekurangan dari teknologi yang dibahas. Ini membantu peneliti memahami sejauh mana efektivitas AI-powered IDS dalam praktik dan apakah ada tantangan yang perlu diatasi untuk penerapan yang lebih luas. Melalui metode studi literatur ini, penelitian dapat menghasilkan pemahaman yang mendalam tentang solusi AI-powered IDS dan manfaatnya bagi keamanan Big Data. Dengan tidak melakukan eksperimen langsung, studi literatur memungkinkan peneliti untuk memanfaatkan pengetahuan dan pengalaman dari penelitian sebelumnya sebagai dasar dalam menyusun temuan dan rekomendasi yang sesuai [3].

III. HASIL DAN PEMBAHASAN

A. Big Data

Big Data merujuk pada kumpulan data dengan volume besar, kecepatan tinggi, dan beragam bentuk (3V: volume, velocity, variety) yang sulit ditangani dengan metode tradisional. Data ini dapat mencakup informasi terstruktur maupun tidak terstruktur dari berbagai sumber, seperti transaksi online, media sosial, dan sensor IoT. Karena kompleksitasnya, Big Data memerlukan infrastruktur khusus dan strategi keamanan yang mampu mengimbangi risiko dan ancaman yang meningkat seiring dengan jumlah data yang diolah [4].

Big Data merupakan istilah yang diberikan pada kumpulan data yang berukuran sangat besar dan kompleks yang menggambarkan volume besar data yang berkecepatan tinggi, sehingga tidak bisa lagi menggunakan perangkat pengelolaan data yang konvensional kompleks dan variable yang membutuhkan teknik canggih untuk memungkinkan penangkapan, penyimpanan, manajemen dan analisis pengambilan informasi [5].

B. Keamanan Siber dan Ancaman dalam Big Data

Keamanan siber atau cyber security menjadi topik yang semakin dibahas seiring dengan perkembangan pesat teknologi. Kemajuan teknologi menuntut peningkatan langkah-langkah keamanan karena semakin banyak aktivitas dilakukan secara daring melalui dunia maya atau cyberspace. Keamanan siber mencakup serangkaian upaya untuk melindungi barang, perangkat, dan aset digital dari berbagai risiko yang muncul di dunia maya, termasuk kejahatan siber. Komponen teknologi dan keamanan mencakup ketersediaan perangkat perlindungan seperti firewall dan antivirus, serta jaminan dalam pengelolaan big data dan pemeliharaan sistem secara berkala [6].

Definisi ini menekankan pentingnya mengidentifikasi, mengukur, dan mengurangi ancaman terhadap sistem digital guna memastikan keamanan dan keandalan data serta aset yang dilindungi [7]. Seiring pertumbuhan Big Data, ancaman keamanan siber menjadi lebih beragam dan kompleks, seperti Distributed Denial of Service (DDoS), pencurian data, ransomware, dan akses ilegal. IDS tradisional yang berbasis aturan (rule-based) mengalami kesulitan dalam menangani serangan baru karena hanya mendeteksi ancaman berdasarkan pola yang sudah dikenal. Hal ini menimbulkan kebutuhan akan pendekatan yang lebih adaptif dan otomatis.

C. Intrusion Detection System (IDS)

IDS adalah sistem yang dirancang untuk mendeteksi aktivitas yang mencurigakan atau tidak sah dalam jaringan dan sistem komputer. Intrusion Detection System (IDS) adalah sistem yang memantau lalu lintas jaringan dan aktivitas dalam sistem untuk mendeteksi kegiatan mencurigakan. IDS memberikan peringatan kepada sistem atau administrator jika ditemukan potensi serangan. Ada dua jenis IDS berdasarkan fungsinya [8]:

1) Network Intrusion Detection System (NIDS)

Ditempatkan di titik strategis dalam jaringan untuk memantau lalu lintas data masuk dan keluar dari berbagai perangkat. Meski efektif, pemantauan penuh dapat menyebabkan bottleneck yang memperlambat jaringan.

2) Host Intrusion Detection System (HIDS)

Beroperasi pada satu perangkat atau host dan memantau aktivitas yang hanya terkait dengan perangkat tersebut. Jika ada potensi ancaman, HIDS akan

memberikan peringatan kepada pengguna atau administrator.

Namun, IDS tradisional memiliki keterbatasan dalam menangani data besar dan ancaman baru secara cepat dan akurat. Intrusion Detection System (IDS) bisa berupa perangkat keras atau perangkat lunak yang berfungsi mendeteksi dan menganalisis tanda-tanda intrusi dalam sistem. IDS memantau lalu lintas jaringan masuk dan keluar secara bersamaan untuk mencari aktivitas mencurigakan. Proses deteksi intrusi dilakukan melalui beberapa langkah [9]:

1) Pemeriksaan data atau file sistem, yaitu memastikan apakah ada pola atau tanda-tanda serangan, seperti malware atau intrusi.
2) Pemindaian untuk validasi, melakukan pemindaian menyeluruh guna mengonfirmasi kebenaran dari tanda-tanda yang ditemukan.
3) Pemantauan berkelanjutan, yaitu sistem terus dipantau untuk mendeteksi serangan siber baru dan memberikan peringatan jika ada ancaman.

Namun, IDS memiliki keterbatasan dalam mendeteksi semua jenis serangan, terutama serangan yang kompleks atau tidak dikenal. Oleh karena itu, sering kali dibutuhkan Intrusion Prevention System (IPS), yang dirancang untuk mencegah dan memblokir serangan secara otomatis ketika terdeteksi. IDS dan IPS biasanya bekerja beriringan untuk memberikan perlindungan lebih efektif terhadap serangan siber.

Masalah keamanan komputer semakin kritis dan membutuhkan penanganan konsisten. Salah satu komponen penting dalam melindungi sistem adalah Intrusion Detection System (IDS). IDS bekerja dengan asumsi bahwa perilaku penyusup berbeda dari pengguna normal. Berdasarkan arsitekturnya, IDS dibagi menjadi tiga jenis: berbasis host, berbasis jaringan, dan hybrid. IDS berbasis host dipasang di komputer untuk memantau aktivitas sistem, seperti log peristiwa, guna mendeteksi potensi serangan [10].

Ada dua pendekatan utama dalam IDS yaitu deteksi anomali dan deteksi berbasis tanda tangan. Deteksi anomali mengidentifikasi pola tidak wajar berdasarkan model perilaku umum, sedangkan deteksi berbasis tanda tangan membandingkan pola serangan dengan basis data tanda tangan yang telah ada. Deteksi anomali lebih unggul karena bisa mendeteksi ancaman baru maupun lama, sementara deteksi tanda tangan hanya efektif untuk serangan yang sudah dikenal. Saat ini, teknik berbasis AI semakin diminati dalam penelitian IDS karena efektivitasnya, meskipun penerapannya masih menghadapi tantangan dalam desain dan penggunaan yang optimal.

D. Kecerdasan Buatan (Artificial Intelligence/AI) dan Machine Learning

AI dan machine learning memberikan solusi inovatif dalam mengatasi keterbatasan sistem deteksi intrusi (Intrusion Detection System/IDS) tradisional. Dengan kemampuan untuk belajar dari data, algoritma machine learning seperti Random Forest, Support Vector Machine (SVM), dan Neural Networks dapat secara otomatis mendeteksi pola serangan yang berpotensi membahayakan. Algoritma ini memproses data historis untuk mengidentifikasi pola anomali atau serangan yang sulit dideteksi dengan metode konvensional, sehingga meningkatkan respons keamanan secara real-time.

Deep learning, sebagai cabang lanjutan dari machine learning, menawarkan keunggulan dalam menganalisis data yang kompleks dan bervolume besar. Dengan arsitektur jaringan saraf yang lebih dalam, model deep learning mampu menghasilkan deteksi yang lebih akurat dan mengurangi tingkat kesalahan (false positive). Hal ini membuatnya sangat efektif dalam mendeteksi serangan siber yang berkembang secara dinamis, seperti malware baru atau serangan berbasis jaringan, sehingga mendukung keamanan sistem secara lebih optimal [11].

E. Pentingnya AI Dalam Intrusion Detection System (IDS)

Penerapan kecerdasan buatan (AI) dalam Intrusion Detection System (IDS) sangat penting karena mampu mengatasi keterbatasan metode tradisional. Dengan menggunakan teknik seperti pembelajaran mesin (ML) dan pembelajaran mendalam (DL), IDS dapat mengenali pola dan mendeteksi anomali dengan lebih akurat. Ini memungkinkan sistem untuk beradaptasi dengan ancaman baru yang terus berkembang tanpa perlu intervensi manual. Selain itu, AI membantu mengurangi kejadian positif palsu (false positive), yaitu ketika sistem salah mengidentifikasi aktivitas normal sebagai ancaman.

Keunggulan lain dari IDS berbasis AI adalah kemampuannya dalam memproses data dalam jumlah besar secara efisien dan cepat. Sistem ini dapat menganalisis data secara real-time, sehingga respons terhadap serangan bisa lebih cepat dan tepat. Model AI juga dapat diperbarui terus menerus berdasarkan data terbaru, memastikan IDS selalu siap menghadapi berbagai ancaman baru. Dengan demikian, integrasi AI membantu menjaga keamanan jaringan secara lebih efektif dan adaptif [12].

F. Intrusion Detection System (IDS) Pada Big Data

Sistem deteksi intrusi (IDS) dalam big data sangat penting untuk mengamankan jaringan dan host yang terhubung dengan berbagai perangkat, perangkat lunak, platform, dan sensor. IDS menggunakan analitik dan alat big data untuk memantau aktivitas dan membedakan kejadian normal dari anomali. Karena volume, kecepatan,

dan variasi data terus bertambah, analisis aliran jaringan, log, dan peristiwa sistem menjadi semakin penting untuk mendeteksi potensi intrusi.

Teknologi konvensional sering kali tidak mampu menangani analitik berskala besar karena tingginya biaya dan keterbatasan dalam menyimpan data dalam jumlah besar. Dengan memanfaatkan ekosistem big data seperti Hadoop dan pemrosesan aliran, IDS mampu menyimpan, menganalisis, dan mengolah data kompleks secara cepat dan efisien. Big data membantu mengidentifikasi anomali dan aktivitas mencurigakan secara real-time dengan:

1) Menangkap data besar dari berbagai sumber internal maupun eksternal;
2) Melakukan analisis mendalam;
3) Menyajikan informasi keamanan yang terintegrasi; dan
4) Memproses aliran data langsung.

Agar efektif, IDS berbasis big data membutuhkan konfigurasi alat analitik yang tepat dan pemahaman mendalam dari analis dan arsitek sistem. Model komputasi aliran data memungkinkan deteksi intrusi secara cepat dan akurat, memberikan perlindungan yang lebih responsif terhadap serangan siber yang semakin kompleks [13].

G. AI-Powered Intrusion Detection System (AI-powered IDS) Pada Big Data

AI-powered IDS menggabungkan machine learning dan deep learning untuk meningkatkan kinerja deteksi ancaman. Sistem ini mampu memproses data dalam jumlah besar secara real-time dan mendeteksi pola serangan baru yang sebelumnya tidak dikenal. AI-powered IDS lebih adaptif karena terus belajar dan berkembang seiring dengan perubahan pola ancaman. Hasil penelitian menunjukkan bahwa teknologi ini dapat meningkatkan akurasi hingga 25% dibandingkan IDS konvensional, dengan mengurangi false positive dan mempercepat respon terhadap ancaman [14].

Kelebihan utama AI-powered IDS adalah kemampuannya untuk bekerja secara otomatis, mendeteksi pola anomali secara real-time, dan menangani volume data besar. Namun, penerapan teknologi ini masih menghadapi beberapa tantangan, seperti kompleksitas dalam pelatihan model, ketergantungan pada data berkualitas tinggi, dan kebutuhan akan sumber daya komputasi yang besar. Selain itu, sistem ini juga perlu terus diperbarui agar tetap relevan dalam menghadapi ancaman baru yang muncul [15].

Berdasarkan analisis literatur yang dilakukan, penelitian ini menemukan bahwa AI-powered Intrusion Detection System (IDS) secara signifikan mampu mengatasi keterbatasan yang dimiliki IDS tradisional dalam mendeteksi ancaman pada ekosistem Big Data. Berikut beberapa temuan utama dan pembahasan mengenai hasil penerapan AI-powered IDS yaitu:

1. Efektivitas dalam Mendeteksi Ancaman Kompleks

AI-powered IDS menunjukkan kemampuan yang lebih baik dalam mendeteksi berbagai ancaman, seperti Distributed Denial of Service (DDoS), serangan malware, dan akses tidak sah. Machine learning memungkinkan sistem untuk mengenali pola serangan baru berdasarkan data historis dan mendeteksi anomali tanpa harus bergantung pada aturan yang statis. Hal ini membuat sistem lebih adaptif dan efektif menghadapi ancaman yang terus berkembang.

2. Penurunan False Positive

Salah satu masalah utama IDS tradisional adalah tingginya jumlah false positive, yang menyebabkan alarm palsu dan menurunkan efisiensi operasional. Dengan penerapan deep learning, AI-powered IDS mampu lebih akurat dalam membedakan antara aktivitas normal dan ancaman sebenarnya. Beberapa studi menunjukkan bahwa penggunaan model seperti neural networks dan algoritma klasifikasi meningkatkan akurasi hingga 25% dibandingkan sistem konvensional.

3. Kemampuan Real-Time dalam Memproses Data Besar

Big Data menuntut sistem yang mampu memproses dan menganalisis data dalam jumlah besar dan kecepatan tinggi. AI-powered IDS memenuhi kebutuhan ini dengan teknologi yang dapat memproses data secara real-time, memungkinkan deteksi ancaman dan respon yang cepat. Kemampuan ini sangat penting untuk mencegah kerusakan atau pencurian data dalam waktu singkat.

4. Keterbatasan dan Tantangan Implementasi

Meskipun AI-powered IDS menawarkan berbagai keunggulan, penerapannya tidak tanpa tantangan. Sistem ini memerlukan data pelatihan dalam jumlah besar dan berkualitas tinggi agar model AI dapat bekerja dengan optimal. Selain itu, biaya dan infrastruktur komputasi yang dibutuhkan untuk mengimplementasikan teknologi ini cukup tinggi, sehingga mungkin menjadi kendala bagi beberapa organisasi.

5. Rekomendasi untuk Penerapan di Masa Depan

Hasil studi ini menegaskan pentingnya pengembangan dan adopsi AI-powered IDS untuk mengamankan ekosistem Big Data. Agar implementasi berjalan optimal, organisasi perlu memastikan data yang digunakan untuk pelatihan relevan dan terkini. Selain itu, kolaborasi antara ahli keamanan dan data scientist diperlukan untuk terus meningkatkan kinerja sistem. Dengan langkah ini, AI-powered IDS dapat menjadi solusi proaktif dan berkelanjutan dalam menghadapi ancaman keamanan di masa depan.

Secara keseluruhan, AI-powered IDS terbukti lebih unggul dibandingkan IDS tradisional dalam mendeteksi ancaman di lingkungan Big Data. Dengan kemampuan mendeteksi ancaman secara real-time dan akurat, sistem

ini menjadi pilihan yang efektif untuk meningkatkan keamanan siber organisasi di era digital saat ini.

IV. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penerapan AI-powered Intrusion Detection System (IDS) merupakan solusi yang efektif untuk mengatasi tantangan keamanan dalam ekosistem Big Data. AI-powered IDS mampu mengidentifikasi ancaman yang kompleks dan mendeteksi pola serangan baru dengan akurasi tinggi. Dengan memanfaatkan machine learning, sistem ini dapat memproses data besar secara real-time dan mengurangi tingkat false positive, yang menjadi kendala utama dalam IDS tradisional. Hasil studi ini menegaskan bahwa AI-powered IDS tidak hanya meningkatkan efisiensi deteksi, tetapi juga memberikan kemampuan adaptasi terhadap pola serangan yang terus berkembang, menjadikannya solusi proaktif untuk keamanan siber.

Untuk penerapan yang optimal, organisasi disarankan untuk menggunakan dataset yang berkualitas dan relevan untuk melatih model AI. Kolaborasi antara pakar keamanan siber dan data scientist juga sangat dibutuhkan agar sistem dapat berfungsi maksimal. Selain itu, perlu dipertimbangkan pengembangan infrastruktur komputasi yang memadai karena AI-powered IDS membutuhkan sumber daya yang besar. Di masa mendatang, penelitian lanjutan sebaiknya fokus pada optimalisasi algoritma agar lebih hemat sumber daya dan lebih mudah diimplementasikan di berbagai skala organisasi. Implementasi AI-powered IDS diharapkan tidak hanya memperkuat keamanan Big Data, tetapi juga menjadi dasar bagi pengembangan teknologi keamanan siber yang lebih inovatif dan tangguh.

UCAPAN TERIMA KASIH

Penulis, Dwi Putri Amanda, mengucapkan terima kasih kepada Ibu Eriene Dheanda Absyarina selaku dosen pembimbing mata kuliah Pengelolaan Big Data, atas bimbingan, arahan, dan dukungan yang diberikan sehingga artikel ini dapat diselesaikan dengan baik. Penulis juga berterima kasih kepada keluarga dan teman-teman yang telah memberikan motivasi dan bantuan selama proses penyusunan artikel ini. Semoga karya ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan di bidang keamanan siber dan Big Data.

DAFTAR PUSTAKA

[1] S. Sunaryono, S. Taryati, E. Trisnawati, A. P. Hardayu, and Y. Yulianto, *Buku Ajar Metodologi Penelitian 1*. Jambi: PT.Sonpedia Publishing Indonesia, 2024.

[2] E. Dheanda and E. S. Negara, "Penerapan Model Eucs Dan Delone and Mclean Untuk Melihat Tingkat Kesuksesan Dan Kepuasan Pengguna Dalam Penerapan …," *J. Ilm. Betrik*, no. 03, pp. 445–458, 2023.

[3] B. Suhartawan and A. R. Nurmaningtyas, *Buku Metodologi Penelitian*, Pertama. Batam: Yayasan Cendekia Mulia Mandiri, 2024.

[4] S. D. Kurniawan, Y. W. Rosalina, and D. Hermanto, *Buku Big Data: Mengenal Big Data & Implementasinya di Berbagai Bidang*. Jambi: PT.Sonpedia Publishing Indonesia, 2023.

[5] A. S. Sihab and A. P. Nurfajar, "Sistem Pengelolaan Kearsipan Google Melalui Big Data," *J. Kearsipan*, vol. 15, no. 2, pp. 21–20, Dec. 2020, doi: 10.46836/jk.v15i2.154.

[6] E. Dheanda Absharina and T. Sutabri, "Analisis Model Digital Forensic Readiness Index (Difri) Untuk Mencegah Cybercrime," *Blantika Multidiscip. J.*, vol. 1, no. 2, pp. 71–78, 2023, doi: 10.57096/blantika.v1i2.12.

[7] D. A. S. Ilhami, "Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur," *J. Sains, Nalar, dan Apl. Teknol. Inf.*, vol. 2, no. 1, pp. 51–60, Sep. 2022, doi: 10.20885/snati.v2i1.19.

[8] F. Arsin, M. Yamin, and L. Surimi, "Implementasi Security System Menggunakan Metode IDPS (Intrusion Detection and Prevention System) Dengan Layanan Realtime Notification," *SemanTIK*, vol. 3, no. 2, pp. 39–48, Dec. 2017.

[9] M. Umer, H. Xiaoli, and S. Abdul, "Big Data Security Analysis in Network Intrusion Detection System," *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 12–18, Jan. 2020, doi: 10.5120/ijca2020919759.

[10] B. S. Ali *et al.*, "ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks," *J. Supercomput.*, vol. 80, no. 6, pp. 7876–7905, Apr. 2024, doi: 10.1007/s11227-023-05764-5.

[11] J. T. Santoso, *Buku: Meningkatkan Keamanan Data Pada Attendance System Berbasis Face Recognition*, vol. 10, no. 1. 2024.

[12] S. M. Yellepeddi, C. S. Ravi, V. Kumar, and R. Vangoor, "AI-Powered Intrusion Detection Systems: Real-World Performance Analysis," *J. AI-Assisted Sci. Discov. By Sci.*, vol. 4, no. 1, pp. 279–289, Jun. 2024.

[13] B. Hameed, A. AlHabshy, and K. ElDahshan, "Distributed Intrusion Detection Systems in Big Data: A Survey," *Al-Azhar Bull. Sci.*, vol. 32, no. 1, pp. 27–44, Sep. 2021, doi: 10.21608/absb.2021.63810.1100.

[14] V. Gustina DM and A. Ananda, "Kecerdasan Buatan untuk Security Orchestration, Automation and Response: Tinjauan Cakupan," *J. Komput. Terap.*, vol. 10, no. 1, pp. 36–47, Jun. 2024, doi: 10.35143/jkt.v10i1.6247.

[15] D. A. Sulaeman and Sukarsa, "Pengembangan Aplikasi Mobile Berbasis Kecerdasan Buatan Untuk Meningkatkan Efisiensi Proses Bisnis," *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 3, pp. 11884–118890, Aug. 2024.