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

Transformasi Sistem Informasi Akuntansi: Optimalisasi Efisiensi dengan AI dan Keamanan Siber

Akmil Maulana Ramadhan[1], Binastya Anggara Sekti[2]
[1,2]Sistem Informasi, Ilmu Komputer, Universitas Esa Unggul
akmilmaulana12@gmail.com

Abstract

Understanding the value of an effective and efficient Accounting Information System (AIS) is crucial for businesses that want to maintain accuracy and speed in financial data processing. Effective and efficient AIS is crucial for companies in maintaining the accuracy and speed of financial data processing. This research aims to explore the level of efficiency of accounting information systems (AIS) by integrating artificial intelligence (AI) and the role of cybersecurity in supporting more optimal operations. This research uses a qualitative method with a case study approach to deeply understand the experiences and perceptions of accounting and information technology professionals involved in the implementation of AI in their AIS. Data were collected through in-depth interviews, direct observation, and analysis of related documents. Data analysis was conducted using a thematic approach to identify relevant patterns and themes regarding the impact of AI on AIS efficiency and the role of cybersecurity in maintaining system reliability. The results show that the integration of AI in AIS can significantly improve the efficiency of data processing and decision making. The findings indicate that implementing AI and cybersecurity in AIS not only improves efficiency but also provides the necessary protection against cyber threats, making the system more reliable and secure.

Keywords: *Transformation, Accounting Information System, Optimization, Artificial intelligence, Cyber Security.*

Abstrak

Memahami nilai Sistem Informasi Akuntansi (SIA) yang efektif dan efisien sangat penting bagi bisnis yang ingin mempertahankan keakuratan dan kecepatan dalam pemrosesan data keuangan. SIA yang efektif dan efisien menjadi krusial bagi perusahaan dalam menjaga akurasi dan kecepatan pengolahan data keuangan. Penelitian ini bertujuan untuk mengeksplorasi tingkat efisiensi sistem informasi akuntansi (SIA) dengan mengintegrasikan kecerdasan buatan (AI) dan peran keamanan siber dalam mendukung operasional yang lebih optimal. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus untuk memahami secara mendalam pengalaman dan persepsi para profesional akuntansi dan teknologi informasi yang terlibat dalam implementasi AI dalam SIA mereka. Data dikumpulkan melalui wawancara mendalam, observasi langsung, dan analisis dokumen terkait. Analisis data dilakukan dengan pendekatan tematik untuk mengidentifikasi pola dan tema yang relevan mengenai dampak AI terhadap efisiensi SIA dan peran keamanan siber dalam menjaga keandalan sistem. Hasil penelitian menunjukkan bahwa integrasi AI dalam SIA dapat meningkatkan efisiensi pengolahan data dan pengambilan keputusan secara signifikan. Temuan ini mengindikasikan bahwa penerapan AI dan keamanan siber dalam SIA tidak hanya meningkatkan efisiensi tetapi juga memberikan perlindungan yang diperlukan terhadap ancaman siber, menjadikan sistem lebih andal dan aman.

Kata kunci: Transformasi, Sistem Informasi Akuntansi, Optimalisasi, AI, Keamanan Siber.

1. Pendahuluan

Teknologi AI telah ada sejak tahun 1950-an, dan kemajuan terbaru telah mengarah pada peningkatan kreativitas dan otomatisasi dalam produksi[1]. AI mencakup berbagai hal, termasuk penalaran, pengetahuan, perencanaan, otomatisasi, pembelajaran mesin, pemrosesan bahasa alami, robot, kecerdasan manusia, dan keamanan siber. Bersama-sama, kedua bidang pengaruh ini dapat merevolusi keamanan digital. Saienko (2023) berfokus pada interaksi antara keamanan siber dan kecerdasan buatan, serta aplikasi teoretis dan praktis AI dalam keamanan siber[2]. Keamanan siber mencakup deteksi kerentanan, perilaku bermusuhan, dan eksploitasi. Kaur dkk. mendefinisikan keamanan siber sebagai penggunaan teknologi, proses, dan praktik untuk melindungi aset organisasi, data pelanggan, dan kekayaan intelektual dari pelanggaran yang tidak sah[3]. Keamanan siber mengacu pada perlindungan jaringan komputer dan seluler, perangkat lunak, server, dan sistem elektronik terhadap virus dan malware[4]. Serangan siber tumbuh semakin kompleks di seluruh dunia. Serangan siber di beberapa area telah meningkat 300% setiap tahunnya[5]. Pemasok dan pelanggan mengungkapkan kekhawatiran keamanan siber terkait penggunaan produk AI yang terus meningkat di dunia.

Program SIA membantu menjembatani kesenjangan antara akuntansi dan teknologi[6]. Sistem Informasi Akuntansi (SIA) adalah sistem untuk mengumpulkan, menyimpan, dan memproses data keuangan dan akuntansi. Keamanan siber sangat penting untuk melindungi transaksi keuangan dan data[7].

Sistem informasi akuntansi (Sealehi, 2011) mengumpulkan, memproses, mengkategorikan, dan melaporkan peristiwa keuangan untuk memberikan informasi yang relevan untuk pengambilan keputusan dan pencatatan[8]. Sistem ini juga menghasilkan laporan keuangan harian dan mingguan.

Sistem pengendalian akuntansi sangat penting untuk meningkatkan kualitas informasi akuntansi, menciptakan nilai, dan mencapai kesuksesan perusahaan[9]. Sistem pengendalian akuntansi melindungi aset dari kecurangan dan kesalahan, memastikan data akuntansi yang akurat dan dapat diandalkan untuk pengambilan keputusan, meningkatkan efektivitas operasional, dan mendorong kepatuhan terhadap kebijakan bisnis. (Hayal dan Abu Khadra, 2006)

Masalah keamanan meliputi kejahatan dunia maya, pembajakan perangkat lunak, dan serangan malware, serta serangan berbahaya lainnya[10]. Seiring dengan semakin maraknya transaksi keuangan online dan pengambilan keputusan berbasis data, perusahaan menghadapi masalah dengan sistem informasi mereka.

Namun, langkah-langkah keamanan konvensional tidak dapat digunakan di area yang terus berkembang ini. Ketika ancaman baru muncul, perlu untuk memperbarui kerangka kerja, solusi, dan disiplin untuk mengatasinya.

Dengan meningkatnya frekuensi dan kecanggihan serangan siber, pemahaman menyeluruh tentang komponen, kelemahan, dan potensi konsekuensinya menjadi sangat penting[11]. Jaringan komputer menjadi landasan bagi perkembangan teknologi yang memungkinkan kolaborasi secara global, dan pertukaran budaya yang lebih luas [12].
Teknologi AI seperti machine learning dan neural networks digunakan untuk mengembangkan model prediktif yang dapat membedakan perilaku normal dan mencurigakan dalam jaringan[13]. Kecerdasan Buatan (AI) telah terbukti membantu dalam memprediksi dan mencegah kegiatan kriminal[14].
Namun, mengingat sudut pandang para penulis yang disebutkan di atas, perlu dicatat bahwa ada kekurangan penelitian tentang kecerdasan buatan dalam keamanan informasi sebagai komponen prioritas yang menjanjikan dalam pertahanan siber karena dampak konstan dari faktor eksternal dan internal. Penelitian lebih lanjut diperlukan di banyak bidang yang belum diteliti.

Studi ini bertujuan untuk menganalisis peran kecerdasan buatan dalam keamanan siber, termasuk dalam hal identifikasi ancaman dan pembentukan sistem sistem pertahanan.

Studi ini berupaya memberikan kontribusi substansial terhadap peningkatan dan pengembangan strategi Sistem Informasi Akuntansi yang lebih efisien dan berfokus pada keamanan dalam lanskap teknologi yang terus berkembang saat ini melalui eksplorasi pertanyaan-pertanyaan ini.

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode penelitian kualitatif. Penelitian ini dilakukan dengan mencari bahan dan informasi yang berhubungan dengan Kecerdasan Buatan (AI) dan Keamanan Cyber. Data-data tersebut di dapat dari sumber-sumber literatur yang ada, baik itu dari jurnal, buku, maupun artikel-artikel. Kemudian merangkumnya menjadi sebuah literatur baru yang dapat menjadi pedoman bagi pembaca.

2.1. Research Design

Dengan menggunakan teknik deskriptif kualitatif, penelitian ini mengevaluasi tingkat efisiensi sistem informasi akuntansi (SIA) dengan mempertimbangkan dampak kecerdasan buatan (AI) dan fungsi keamanan siber. Pendekatan kualitatif digunakan oleh para peneliti untuk menggali lebih jauh pengalaman dan pandangan pengguna terhadap teknologi yang sedang diteliti. Selain itu, penelitian kualitatif memberikan fleksibilitas dalam memperoleh informasi dari berbagai sumber, sehingga memungkinkan analisis yang lengkap terhadap fenomena yang rumit. Desain deskriptif digunakan untuk menyajikan gambaran yang jelas dan komprehensif tentang bagaimana SIA diterapkan di tempat kerja.

Untuk menghasilkan temuan yang menyeluruh dan terperinci, penelitian ini akan menggunakan berbagai metodologi pengumpulan data kualitatif. Informasi yang relevan akan dikumpulkan melalui observasi langsung, dan wawancara mendalam dengan personel. Berbagai teknik tersebut akan memberikan perspektif yang berbeda namun saling melengkapi, sehingga memungkinkan para akademisi untuk memperoleh pengetahuan yang komprehensif mengenai pengaruh AI dan peran keamanan siber terhadap efisiensi SIA. Selain itu, prosedur triangulasi data akan diimplementasikan untuk meningkatkan validitas dan reliabilitas temuan penelitian.

2.2. Instruments

Dua instrumen utama digunakan untuk mengumpulkan data untuk penelitian ini:

Wawancara akan dilakukan dengan sejumlah karyawan termasuk manajer IT, akuntan, dan pengguna SIA lainnya, untuk menggali lebih dalam pandangan mereka mengenai keuntungan dan kesulitan dalam menggunakan teknologi AI dan keamanan siber dalam SIA.

Kuesioner akan disebarkan kepada pengguna SIA untuk mengumpulkan data mengenai persepsi tentang efisiensi sistem, dampak AI, dan tingkat keamanan siber. Survei ini akan mencakup pertanyaan terbuka dan tertutup untuk mendapatkan data yang kaya dan bervariasi.

3. Hasil dan Pembahasan

3.1. Kecerdasan Buatan (AI)

Istilah "Kecerdasan Buatan" akan dikaitkan dengan nama John McCharty (1927-2011). Dia adalah seorang ilmuwan komputer yang mulai mengajar matematika di MIT dan Universitas Stanford. Pada tahun 1956, ia mengatur proyek penelitian selama sepuluh minggu di Universitas Dartmouth. Dia menyebut upaya tersebut sebagai "studi tentang kecerdasan buatan". Ini adalah pertama kalinya istilah "kecerdasan buatan" digunakan.

Metode Kecerdasan Buatan (AI) dapat diterapkan dalam beberapa cara untuk membantu penegakan hukum dalam menangani kejahatan siber. Metode kecerdasan buatan (AI) yang telah terbukti sangat bermanfaat dalam identifikasi dan pencegahan kejahatan siber meliputi kecerdasan komputasi, jaringan saraf, sistem kekebalan tubuh buatan, pembelajaran mesin, penggalian data, pengenalan pola, logika kabur, dan heuristik.

Faktanya, sudah diketahui bahwa mendefinisikan AI merupakan hal yang menantang. Definisi istilah ini yang luas memungkinkannya untuk merujuk pada berbagai aplikasi, mulai dari teknik pembelajaran mesin yang intensif data seperti jaringan saraf hingga model penalaran logis yang sederhana .

AI dibagi menjadi tiga yaitu, artificial narrow intelligence (ANI), artificial general intelligence (AGI), dan artificial super intelligence (ASI) adalah tiga kategori yang dapat diklasifikasikan ke dalam AI. Dengan menggunakan sistem AI, dapat mempersonalisasi pelajaran sesuai dengan kebutuhan setiap orang. Solusi berbasis AI juga memudahkan untuk menerima umpan balik secara real-time, yang meningkatkan efisiensi proses pembelajaran [15].

Solusi berbasis AI juga memudahkan untuk menerima umpan balik secara real-time, yang meningkatkan efisiensi proses pembelajaran. Efisiensi, ketepatan, dan pendekatan yang lebih individual terhadap instruksi semuanya ditingkatkan dengan integrasi AI.

Meskipun AI masih terus berkembang, penerapannya dalam berbagai aspek kehidupan sehari-hari semakin meluas dan semakin penting. Keputusan di masa depan, cara kita bekerja, berinteraksi dengan teknologi, dan cara kita mengambil keputusan, semuanya dapat dipengaruhi secara signifikan oleh AI [16] .

3.2. Keamanan Cyber

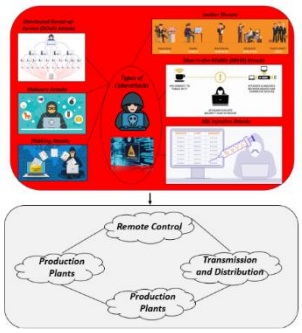
Saat ini, sebagian besar bisnis dikendalikan melalui internet, membuat organisasi rentan terhadap serangan keamanan siber yang merusak aktivitas penting perusahaan. Keamanan siber menggunakan berbagai teknik, strategi, dan prosedur untuk menjamin bahwa sistem dilindungi dari potensi ancaman dan kelemahan. Serangan siber berusaha melanggar kerahasiaan, integritas, dan ketersediaan layanan, sumber daya, atau sistem yang terhubung dengan mendapatkan akses ke sana.

Keamanan siber menggunakan berbagai teknik, strategi, dan prosedur untuk menjamin bahwa sistem dilindungi dari potensi ancaman dan kelemahan. Serangan siber berusaha melanggar kerahasiaan, integritas, dan ketersediaan layanan, sumber daya, atau sistem yang terhubung dengan mendapatkan akses ke sana [17].

Untuk meningkatkan keamanan dunia maya, strategi canggih untuk melawan serangan yang bervariasi dalam sifat dan kecepatan harus dirancang. Seiring berjalannya waktu, keamanan dunia maya telah berubah dari bidang teknis yang berpusat pada keamanan jaringan menjadi masalah di seluruh dunia. Ini adalah subjek yang semakin ditekankan oleh para eksekutif perusahaan.

Keamanan siber mengacu pada kumpulan lengkap metode dan tindakan yang dirancang untuk melindungi sistem komputer dan jaringan dari serangan yang disengaja, pelanggaran yang tidak disengaja, dan semua jenis akses tidak sah lainnya di lingkungan digital. Perlindungan ini dilakukan dengan cara seperti audit sistem, kerahasiaan data, memastikan integritas data, otentikasi pengguna, menjaga ketersediaan sistem, teknik enkripsi, dan penggunaan tanda tangan digital.

Smart grid rentan terhadap berbagai serangan siber (Gambar 1), yang menargetkan sistem dan infrastruktur yang saling terhubung. Berikut adalah beberapa serangan siber yang umum terjadi pada jaringan pintar**.**



Gambar 1. hubungan yang saling terkait antara pabrik produksi, jalur transmisi

Denial-of-Service (DoS) Attacks: Serangan ini bertujuan untuk membuat sistem yang ditargetkan tidak dapat diakses oleh pengguna yang sah untuk sementara waktu, seperti jaringan komunikasi atau sistem kontrol, dengan volume permintaan yang berlebihan dan membanjiri mereka dengan lalu lintas dalam jumlah besar, semuanya dimulai dari satu perangkat. Hal ini mengganggu operasi jaringan dan dapat menyebabkan gangguan layanan.

Malware mengacu pada penyusupan file berbahaya ke dalam sistem, jaringan, atau jaringan. Malware menginfeksi sistem kontrol jaringan pintar, atau antarmuka mesin manusia (HMI), mengganggu operasi, membahayakan integritas data, dan berpotensi mendapatkan kendali yang tidak sah atas infrastruktur penting.

Serangan Distribute Denial-of-Service (DDoS) , seperti serangan DoS, menggunakan botnet perangkat terinfeksi yang didistribusikan ke seluruh dunia. Serangan DDoS lebih sulit untuk dimitigasi karena sifatnya yang tersebar.

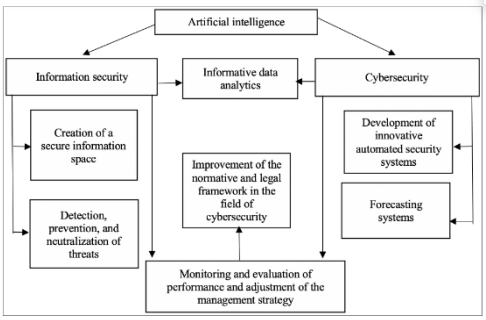
3.3. Dampak Kecerdasan Buatan (AI)

Kecerdasan buatan (AI) telah memainkan peran penting dalam berbagai bidang kehidupan. AI telah menghasilkan solusi pembelajaran dan pengajaran baru yang telah diuji di berbagai lingkungan. Melihat kepada teknologi AI yang dapat melakukan tindakan dan perbuatan layaknya manusia, tentunya hal tersebut yang melandasi suatu pengaturanhukum di sebuah negara untuk memiliki pengaturan secara khusus terkait dengan AI.

Keamanan data merupakan salah satu risiko yang paling serius. Teknologi kecerdasan buatan dapat memperoleh informasi sensitif yang dapat digunakan secara tidak etis. Hal ini akan memungkinkan penyerang siber untuk mencuri atau mengambil data pribadi, seperti identifikasi atau informasi keuangan, yang dihasilkan saat menggunakan model tersebut [18].

Penggunaan platform media sosial seperti Facebook, Twitter, WhatsApp, dan Instagram telah dikaitkan dengan peningkatan pencurian data. Pihak-pihak tertentu telah menggunakan teknologi AI untuk mengubah keamanan data pribadi. Sebagai contoh, teknologi AI telah dieksploitasi untuk memanipulasi dan menyalahgunakan informasi pribadi pengguna media sosial.

Semakin pentingnya kecerdasan buatan dalam strategi keamanan siber menunjukkan potensinya dalam meningkatkan deteksi ancaman, waktu reaksi, dan ketahanan secara keseluruhan terhadap serangan yang tidak bersahabat. Saat ini, solusi bertenaga AI secara rutin digunakan untuk mendeteksi, memantau, dan berhasil merespons gangguan.



Gambar 2. Potensi teknologi AI dalam pertahanan siber

3.4 Dampak Keamanan Cyber

Menekankan pentingnya risiko siber sambil menguraikan prosedur penilaian risiko yang tepat. Studi ini dimulai dengan survei literatur yang relevan untuk menilai metodologi evaluasi risiko siber yang ada. Studi ini, sebagai studi dasar dalam subjek ini, memberikan terminologi kunci dalam konteks keamanan siber.

Indonesia merupakan salah satu dari lima negara teratas dalam hal penggunaan media sosial, yang memiliki implikasi positif dan negatif terhadap perang siber. Penggunaan media sosial yang meluas dapat menimbulkan bahaya bagi kedaulatan negara[19].

Indonesia berada di peringkat atas dalam hal penggunaan media sosial, yang berdampak baik pada pemahaman masyarakat terhadap dunia digital. Namun, hal ini membuat pemerintah terekspos pada serangan siber, yang dapat membahayakan kedaulatan dan keamanan informasi yang disediakan melalui jaringan digital.

Berikut ini adalah beberapa potensi ancaman kejahatan siber di Indonesia :

Hacker: Salah satu alasan serangan siber, mulai dari keinginan untuk menguji keamanan hingga penolakan terhadap pemerintah. Salah satu insiden dari pemilihan presiden 2014 adalah penyebaran berita bahwa situs web KPU telah diretas oleh peretas. Situs web KPU mengalami masalah akses, yang menyebabkan situs web tersebut tidak dapat diakses untuk sementara waktu.

Cracking: Di Indonesia, orang-orang yang dikenal sebagai “carder” telah terlibat dalam peretasan. Mereka menggunakan metode ini untuk mencuri informasi kartu kredit dengan memata-matai data kartu kredit nasabah. Setelah mendapatkan akses ke informasi tersebut, para peretas berusaha mengakses data sensitif serta dana yang disimpan nasabah di bank untuk keuntungan mereka sendiri.

3.5 Peluang Menggunakan AI dan Keamanan Cyber

Proses transformasi ekonomi digital terjadi ketika bisnis dan ekonomi secara bertahap bertransisi dari teknik tradisional ke teknik digital, terutama di bidang teknologi informasi dan komunikasi [20].

Peluang Untuk Inovasi Bisnis: Proses transformasi ekonomi digital terjadi ketika bisnis dan ekonomi secara bertahap bertransisi dari teknik tradisional ke teknik digital, terutama di bidang teknologi informasi dan komunikasi. Perusahaan dapat menggunakan teknologi digital untuk menciptakan produk dan layanan yang baru, inventif, dan menarik. Contohnya termasuk produk digital, seperti aplikasi seluler.

Peluang Untuk Pertumbuhan Ekonomi: Teknologi digital memungkinkan bisnis untuk mengotomatisasi berbagai operasi, meningkatkan efisiensi dan produktivitas. Selain itu, teknologi digital memungkinkan bisnis untuk mengumpulkan dan

menganalisis data dengan lebih baik. Ekonomi digital memungkinkan bisnis untuk lebih mudah mengakses pasar global. Platform e-commerce memungkinkan bisnis untuk menjual produk mereka secara global. Ekspansi ekonomi digital memiliki potensi untuk menciptakan lapangan kerja baru di sektor teknologi digital.

Peluang Untuk Kemitraan: Platform e-commerce dan media sosial, misalnya, memungkinkan bisnis untuk menjangkau klien di seluruh dunia dan memperluas jangkauan pasar. Evolusi ekonomi digital memungkinkan bisnis untuk mengakses teknologi dan keterampilan yang diperlukan untuk bersaing di pasar global.

Hasil penelitian menunjukkan bahwa integrasi AI dalam SIA dapat meningkatkan efisiensi pengolahan data dan pengambilan keputusan secara signifikan. Temuan ini mengindikasikan bahwa penerapan AI dan keamanan siber dalam SIA tidak hanya meningkatkan efisiensi tetapi juga memberikan perlindungan yang diperlukan terhadap ancaman siber, menjadikan sistem lebih andal dan aman.

4. Kesimpulan

Penelitian ini secara efektif menyelidiki tingkat efisiensi sistem informasi akuntansi (SIA) berbasis kecerdasan buatan (AI) dengan fokus pada keamanan siber. Temuan mengungkapkan bahwa mengintegrasikan AI ke dalam SIA secara signifikan meningkatkan efisiensi dan akurasi pemrosesan data akuntansi dibandingkan dengan pendekatan konvensional sebelumnya. Karyawan memuji teknologi ini, meskipun ada kekhawatiran tentang keamanan dan privasi data. SIA dengan karakteristik AI efektif dalam mengotomatisasi proses yang biasa, mengidentifikasi anomali, dan memberikan analisis data secara real-time, yang semuanya membantu manajemen dalam mengambil keputusan. Teknologi AI memungkinkan otomatisasi proses-proses umum, yang mengurangi beban kerja manual dan meningkatkan produktivitas staf. Prosedur keamanan siber yang diterapkan menjaga integritas dan kerahasiaan data, menurunkan risiko kebocoran informasi dan ancaman siber. Penggunaan SIA ini dapat memberikan solusi bagi bisnis lain yang memiliki masalah serupa dengan sistem akuntansi manual. Manfaat dari penggunaan SIA ini antara lain adalah peningkatan efisiensi operasional, akurasi data keuangan, dan bahaya kebocoran data yang lebih rendah. Studi lebih lanjut dapat mempertimbangkan untuk mengintegrasikan SIA ini dengan sistem SDM dan penggajian, serta mengembangkan kemampuan baru seperti notifikasi keamanan siber dan analisis prediktif untuk mendeteksi potensi masalah keuangan. Dengan demikian, SIA berbasis AI dan keamanan siber ini tidak hanya memenuhi kebutuhan akan sistem akuntansi yang lebih efisien dan aman, tetapi juga memiliki potensi untuk menetapkan standar baru dalam pengelolaan keuangan di berbagai industri.

Daftar Rujukan

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

[2] S. Lysenko, N. Bobro, K. Korsunova, O. Vasylchyshyn, and Y. Tatarchenko, “The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats,” Feb. 01, 2024, *AESSRA*. doi: 10.46852/0424-2513.1.2024.6.

[3] T. Schiller, B. Caulkins, A. S. Wu, and S. Mondesire, “Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing,” *Information (Switzerland)*, vol. 14, no. 10, Oct. 2023, doi: 10.3390/info14100536.

[4] M. H. Behiry and M. Aly, “Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods,” *J Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-023-00870-w.

[5] S. A. Al-Somali, R. R. Saqr, A. M. Asiri, and N. A. Al-Somali, “Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture,” *Sustainability (Switzerland)* , vol. 16, no. 5, Mar. 2024, doi: 10.3390/su16051880.

[6] J. B. O’donnell, “Are Accounting Information Systems Programs Evolving to Meet the Needs of the Accounting Profession? An Analysis of Accounting Information Systems Programs in 2005 and 2019,” 2019.

[7] N. Sharma, “Maximizing the Benefits of Information Technology in Healthcare Finance and Accounting: A Quantitative Exploration of Organizational practices,” *J Commer Biotechnol*, vol. 29, no. 1, pp. 102–113, 2024, doi: 10.5912/jcb2217.

[8] O. J. Awosejo and Kekwaletswe, “The Effect of Accounting Information Systems in Accounting.”

[9] K. Phornlaphatrachakorn, “Accounting Control System, Accounting Information Quality, Value Creation, and Firm Success: An Empirical Investigation of Auto Parts Businesses in Thailand,” *INTERNATIONAL JOURNAL OF BUSINESS*, vol. 25, no. 2, p. 2020.

[10] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, “Cybersecurity Risk Analysis in the IoT: A Systematic Review,” Sep. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics12183958.

[11] A. A. Bouramdane, “Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, Dec. 2023, doi: 10.3390/jcp3040031.

[12] B. W. Aulia, M. Rizki, P. Prindiyana, and S. Surgana, “Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital,” *JUSTINFO| Jurnal Sistem Informasi dan Teknologi Informasi*, vol. 1, no. 1, pp. 9–20, 2023.

[13] N. H. Sinaga, D. Irmayani, and M. N. S. Hasibuan, “Mengoptimalkan Keamanan Jaringan Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman,” *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, vol. 7, no. 2, pp. 364–369, 2024.

[14] R. S. A. Faqir, “Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview,” *International Journal of Cyber Criminology*, vol. 17, no. 2, pp. 77–94, Jan. 2023, doi: 10.5281/zenodo.4766706.

[15] R. T. Apriadi and H. Sihotang, “Transformasi Mendalam Pendidikan Melalui Kecerdasan Buatan: Dampak Positif bagi Siswa dalam Era Digital,” *Jurnal Pendidikan Tambusai*, vol. 7, no. 3, pp. 31742–31748, 2023.

[16] A. S. Pratama, S. M. Sari, M. F. Hj, M. Badwi, and M. I. Anshori, “Pengaruh Artificial Intelligence, Big data dan

otomatisasi terhadap kinerja SDM di Era digital," *Jurnal Publikasi Ilmu Manajemen*, vol. 2, no. 4, pp. 108–123, 2023.

[17] Y. Samudra, A. Hidayat, and M. F. Wahyu, "Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital," *AMMA: Jurnal Pengabdian Masyarakat*, vol. 1, no. 12, pp. 1594–1601, 2023.

[18] N. F. Cahyono and S. Mukaromah, "Etika Penggunaan Kecerdasan Buatan Pada Teknologi Informasi," in *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, 2023, pp. 482–491.

[19] E. Soesanto, A. Romadhon, B. D. Mardika, and M. F. Setiawan, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File," *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen*, vol. 1, no. 2, pp. 172–191, 2023.

[20] D. Sudiantini, M. P. Ayu, M. C. A. S. Aswan, M. A. Prastuti, and M. Apriliya, "Transformasi Digital: Dampak, Tantangan, Dan Peluang Untuk Pertumbuhan Ekonomi Digital," *Trending: Jurnal Manajemen Dan Ekonomi*, vol. 1, no. 3, pp. 21–30, 2023.