TRILOGI ACCOUNTING AND BUSINESS RESEARCH
Vol. 05, No. 02, Desember 2024, Hal. 146-155

TANTANGAN KEAMANAN DATA DALAM IMPLEMENTASI TEKNOLOGI AI DI AKUNTANSI

Dian Indah Hayati[1], Ahmad Rahbani Sulaiman S.[2*], Afriosa Syawitri[3], Nadya Fritanita Julyazti[4]

[1,2] Prodi Akuntasi Fakultas Ekonomi dan Bisnis Universitas Negeri Padang
[3] Prodi Bisnis Digital Fakultas Ekonomi dan Bisnis Universitas Negeri Padang
[4] Prodi Manajemen Perdagangan Fakultas Ekonomi dan Bisnis Universitas Negeri Padang
bani@unp.ac.id[2*]

ABSTRAK

Artificial Intelligence (AI) telah memberikan dampak besar dalam mentransformasi industri akuntansi dengan mengotomatiskan berbagai proses, meningkatkan efisiensi operasional, dan memberikan analisis data yang lebih akurat untuk pengambilan keputusan. Terlepas dari manfaatnya yang signifikan, penerapan AI dalam akuntansi juga membawa tantangan besar, terutama dalam hal keamanan data. Ancaman serangan siber dapat merusak integritas laporan keuangan dan proses audit. Kerentanan algoritma AI yang digunakan dalam akuntansi dapat memungkinkan manipulasi yang memengaruhi hasil analisis dan keputusan bisnis. Penelitian ini bertujuan untuk mengidentifikasi tantangan utama ini dan mengusulkan solusi mitigasi yang relevan. Solusi yang dibahas adalah penerapan *blockchain* untuk meningkatkan transparansi dan keamanan data, audit rutin untuk memantau integritas sistem AI, dan pelatihan karyawan untuk meningkatkan kesadaran akan potensi ancaman dunia maya. Dengan pendekatan deskriptif dan analisis literatur, penelitian ini memberikan panduan praktis bagi perusahaan untuk mengintegrasikan AI dalam praktik akuntansi.

Kata Kunci: Kecerdasan Buatan (AI), Keamanan Data, Blockchain

ABSTRACT

Artificial Intelligence (AI) has made a huge impact in transforming the accounting industry by automating various processes, improving operational efficiency, and providing more accurate data analysis for decision-making. However, despite its significant benefits, the application of AI in accounting also brings great challenges, especially in terms of data security. The threat of cyberattacks can undermine the integrity of financial statements and the audit process. In addition, vulnerabilities in AI algorithms used in accounting can enable manipulations that affect analysis results and business decisions. This research aims to identify these key challenges and propose relevant mitigation solutions. Among the solutions discussed are the implementation of blockchain to improve data transparency and security, regular audits to monitor the integrity of AI systems, and employee training to raise awareness of potential cyber threats. With a descriptive approach and literature analysis, this study provides practical guidance for companies to securely integrate AI in their accounting practices.

Keywords: *Artificial Intelligence (AI), Data Security, Blockchain*

Histori artikel:
Diunggah: 20-12-2024
Direvieu: 24-12-2024
Diterima: 30-12-2024
Dipublikasikan: 30-12-2024

* Penulis korespondensi ✉

PENDAHULUAN

Artificial Intelligence (AI) telah menjadi elemen penting dalam transformasi digital di berbagai sektor, termasuk bidang akuntansi. Teknologi ini memungkinkan otomatisasi berbagai tugas, mulai dari pengolahan data keuangan hingga analisis prediktif, yang tidak hanya meningkatkan efisiensi operasional tetapi juga memperkaya wawasan untuk pengambilan keputusan strategis. Selain itu, AI memberikan akuntan kemampuan untuk beralih dari peran administratif ke fungsi yang lebih strategis dengan memanfaatkan data secara efektif (Rich & Knight, 1991; Yusuf et al., 2023). Perusahaan global seperti PwC dan Deloitte telah memanfaatkan teknologi ini untuk meningkatkan efisiensi, memberikan layanan inovatif, dan memperkuat daya saing mereka di pasar (Alghafiqi & Munajat, 2022).

Namun, di balik manfaat besar yang ditawarkan, implementasi AI dalam akuntansi juga memunculkan tantangan signifikan, terutama dalam hal privasi dan keamanan data. Sistem berbasis AI sering kali mengelola informasi yang sangat sensitif, seperti data finansial perusahaan dan data pribadi pelanggan. Kebocoran atau penyalahgunaan data ini dapat berdampak buruk pada reputasi perusahaan, bahkan mengancam stabilitas operasionalnya (Ardi, 2023). Selain itu, keterbatasan transparansi algoritma AI menimbulkan tantangan etis dan teknis, terutama dalam hal mengatasi bias dan memastikan akurasi pengambilan keputusan berbasis data (Juniardi, 2024).

Risiko privasi dan keamanan data pribadi semakin meningkat seiring kemampuan AI untuk mengakses, mengelola, dan menganalisis data dalam skala besar. Penelitian menunjukkan bahwa penggunaan data pribadi dalam sistem AI memerlukan perhatian ekstra karena risiko manipulasi, pencurian, dan penyalahgunaan yang tinggi (Ardi & Bintari, 2024). Dalam konteks akuntansi, data finansial yang sensitif menjadi target utama bagi aktor jahat, sehingga membutuhkan perlindungan ketat terhadap pelanggaran etika privasi dan pengawasan berlebihan (Krishna, 2024). Oleh karena itu, penerapan enkripsi, kebijakan perlindungan data, dan pengawasan sistem menjadi langkah penting untuk menjaga integritas dan kerahasiaan data. Salah satu pelanggaran di dunia maya terjadi akibat tindakan karyawan TikTok yang menggunakan platform cashback sebagai konsumen, sehingga mengganggu hak-hak konsumen yang seharusnya diterima. Hal ini juga disebabkan oleh kurangnya pengawasan terhadap sistem cashback, serta tidak adanya pembaruan yang memadai terkait status produk yang terjual dan transaksi pembayaran yang terjadi (Putri et al., 2024).

Selain risiko privasi, ancaman serangan siber berbasis AI juga semakin kompleks. Teknologi seperti botnet berbasis AI, phishing cerdas, dan deepfake menciptakan celah yang dapat merusak sistem dan reputasi perusahaan. Misalnya, phishing cerdas mampu mencuri kredensial pengguna dengan memanfaatkan manipulasi digital yang presisi, sedangkan deepfake dapat digunakan untuk memalsukan dokumentasi keuangan atau bukti audit, merusak kepercayaan publik terhadap perusahaan (Hermawan et al., 2023; Ballantine et al., 2024). Ancaman-ancaman ini menunjukkan pentingnya langkah mitigasi yang proaktif, seperti audit keamanan rutin dan penggunaan teknologi pemantauan berbasis AI.

Tantangan lainnya berkaitan dengan etika dalam penerapan AI. Kebijakan seperti ethics-by-design, human-in-the-loop, dan pembatasan pengumpulan data menjadi kunci untuk memastikan AI yang dapat dipercaya (Kleizen et al., 2023). Namun, efektivitas langkah-langkah ini masih terbatas dalam membangun kepercayaan masyarakat terhadap AI, terutama jika sistem tidak transparan atau gagal memenuhi standar etika yang diharapkan (Krishna, 2024). Untuk itu, kolaborasi antara pengembang, regulator, dan pengguna menjadi sangat penting dalam menciptakan teknologi AI yang lebih aman dan bertanggung jawab.

METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif-kualitatif berbasis analisis literatur untuk mengidentifikasi tantangan keamanan data dalam penerapan AI di bidang akuntansi. Sumber data yang digunakan meliputi jurnal, buku, dan laporan yang relevan, dengan fokus pada publikasi terkini (2021–2024) untuk memastikan keaktualan informasi. Penelitian ini mengacu pada karya Alghafiqi & Munajat (2022), Das (2021), Juniardi (2024), Sanjiwani et al. (2024), Ardi & Bintari (2024), Krishna (2024), Hermawan et al. (2023), Ballantine et al. (2024), dan Kleizen et al. (2023), yang membahas tantangan keamanan data serta strategi mitigasi yang relevan. Kriteria pemilihan literatur mencakup pembahasan tentang tantangan keamanan data, solusi mitigasi, dan implikasi praktis penerapan AI. Analisis dilakukan secara komparatif untuk membandingkan berbagai strategi mitigasi, seperti penggunaan blockchain, audit keamanan reguler, serta pelatihan karyawan terkait kesadaran keamanan data. Pendekatan ini juga mencakup kontekstualisasi temuan dari berbagai penelitian untuk memberikan wawasan yang terintegrasi dan mendalam. Hasilnya, penelitian ini menawarkan panduan strategis bagi perusahaan dalam mengintegrasikan AI secara aman dan efektif di bidang akuntansi dengan mempertimbangkan aspek teknis, regulasi, dan etika.

Alghafiqi & Munajat (2022) mengidentifikasi bahwa penerapan teknologi AI dalam profesi akuntansi membawa berbagai tantangan, terutama dalam hal keamanan data dan kerentanannya terhadap serangan siber. Mereka menyoroti pentingnya perlindungan data yang lebih baik dalam pengelolaan informasi keuangan dan menekankan bahwa tanpa kontrol yang tepat, penggunaan AI dalam akuntansi dapat membuka celah bagi ancaman seperti manipulasi data atau akses tidak sah. Penelitian ini juga merujuk pada karya Das (2021), yang memaparkan bahwa meskipun AI menawarkan keuntungan efisiensi, risiko terkait integritas data tetap menjadi perhatian besar. Das berpendapat bahwa algoritma AI yang tidak terkontrol bisa rentan terhadap manipulasi data yang dapat mengubah hasil analisis akuntansi dan memengaruhi keputusan strategis perusahaan.

Juniardi (2024) juga berfokus pada aspek keamanan dalam penerapan AI di bidang akuntansi, dengan menunjukkan bahwa AI berisiko mengalami kesalahan dalam proses pengambilan keputusan jika data yang digunakan terkontaminasi atau tidak valid. Menurut Juniardi, tantangan utama dalam mengimplementasikan AI di akuntansi adalah bagaimana melindungi sistem dari serangan seperti data poisoning yang bisa merusak keputusan-keputusan yang dihasilkan oleh AI. Senada dengan itu, Goyal et al. (2023) mengingatkan bahwa pengamanan yang lemah terhadap algoritma yang digunakan dalam AI dapat berisiko pada manipulasi data yang bisa mengarah pada pengambilan keputusan yang tidak akurat dalam laporan keuangan.

Ardi & Bintari (2024) menambahkan bahwa risiko privasi dalam implementasi AI semakin tinggi karena teknologi ini mampu mengakses dan memanfaatkan data pribadi dalam skala besar. Penanganan data finansial yang sensitif memerlukan perlindungan yang ketat untuk mencegah pelanggaran privasi dan penyalahgunaan data. Krishna (2024) menyoroti bahwa tantangan transparansi dalam algoritma AI juga menciptakan celah untuk terjadinya bias dan kesalahan dalam pengambilan keputusan, sehingga langkah mitigasi berbasis etika menjadi sangat penting.

Hermawan et al. (2023) menyebutkan bahwa serangan siber berbasis AI, seperti phishing cerdas dan deepfake, dapat menciptakan risiko signifikan terhadap integritas sistem akuntansi. Serangan ini sering kali dirancang untuk mencuri informasi atau memalsukan data yang memengaruhi kredibilitas perusahaan. Ballantine et al. (2024) memperkuat argumen ini

dengan menunjukkan bahwa phishing cerdas berbasis AI mampu mencuri data dengan tingkat akurasi tinggi melalui manipulasi digital.

Ancaman siber yang dimaksud meliputi serangan seperti data poisoning dan manipulasi algoritma, yang dapat merusak hasil analisis yang dihasilkan oleh AI. Selain itu, kerentanan algoritma yang mengacu pada kemungkinan perubahan atau manipulasi pada algoritma AI dapat mengubah keputusan yang diambil oleh sistem dan memengaruhi proses pengambilan keputusan akuntansi (Goyal et al., 2023). Penelitian ini juga menganalisis tantangan regulasi, dengan merujuk pada Nehemia & Hendrayana (2024), yang menjelaskan bahwa regulasi yang ketat terhadap data pribadi dan pelaporan akuntansi memperberat beban perusahaan dalam menjaga keamanan data mereka, terutama ketika menggunakan teknologi canggih seperti AI dan blockchain.

Solusi mitigasi yang dianalisis mencakup penggunaan blockchain untuk memastikan transparansi dan verifikasi data, pengawasan keamanan melalui sistem deteksi intrusi dan pengawasan aktif terhadap sistem AI, serta pelatihan karyawan untuk meningkatkan kesadaran mengenai potensi ancaman dan cara-cara untuk melindungi data sensitif. Sanjiwani et al. (2024) menyarankan penggunaan blockchain sebagai solusi untuk memastikan integritas data yang diolah oleh AI, sehingga mengurangi kemungkinan manipulasi atau kebocoran data yang dapat merusak kredibilitas laporan akuntansi. Selain itu, Yusuf et al. (2023) merekomendasikan pentingnya pelatihan berkelanjutan bagi staf akuntansi untuk meningkatkan kesadaran mereka terhadap potensi ancaman yang bisa terjadi ketika menggunakan teknologi AI dalam pengelolaan data sensitif.

Dengan menganalisis solusi-solusi ini, penelitian ini bertujuan memberikan wawasan tentang bagaimana perusahaan dapat melindungi data mereka dan memastikan bahwa penerapan AI dalam akuntansi berjalan dengan aman dan efektif.

HASIL DAN PEMBAHASAN

Ancaman Keamanan Data dalam Implementasi AI

Ancaman Serangan Siber

Sistem berbasis AI menjadi target utama serangan siber karena kompleksitas dan peran kritisnya dalam operasional bisnis. Serangan ransomware, misalnya, dapat mengunci akses ke data penting hingga tebusan dibayar, menyebabkan kerugian finansial yang signifikan dan merusak reputasi perusahaan (Das, 2021). Selain itu, serangan phishing yang didukung AI semakin canggih, menggunakan algoritma untuk meniru komunikasi resmi dan mencuri kredensial pengguna (Ballantine et al., 2024). Malware juga menjadi ancaman serius dalam lingkungan yang mengandalkan perangkat terhubung, karena dapat menyebar dengan cepat di seluruh jaringan (Nehemia & Hendrayana, 2024). Akibatnya, perusahaan harus terus berinvestasi dalam teknologi keamanan terbaru untuk melindungi data dan sistem mereka.

Keterbatasan sumber daya membuat perusahaan kecil dan menengah (UKM) lebih rentan terhadap serangan siber. Banyak UKM tidak memiliki dana atau staf TI yang cukup untuk mengimplementasikan sistem keamanan canggih. Keterhubungan perangkat dalam ekosistem AI menciptakan lebih banyak celah yang dapat dimanfaatkan oleh peretas untuk menyusup ke sistem (Yusuf et al., 2023). Serangan yang berhasil dapat menyebabkan gangguan operasional seperti hilangnya data pelanggan atau penundaan proyek penting. Oleh karena itu, UKM harus

mempertimbangkan kolaborasi dengan pihak ketiga yang menyediakan layanan keamanan siber sebagai solusi yang lebih ekonomis.

Audit keamanan rutin merupakan salah satu langkah mitigasi paling efektif dalam menghadapi ancaman serangan siber. Proses audit melibatkan analisis menyeluruh terhadap sistem untuk mendeteksi dan memperbaiki potensi kerentanan. Selain itu, teknologi pemantauan berbasis AI dapat mendeteksi aktivitas anomali dalam jaringan yang menunjukkan upaya serangan (Nehemia & Hendrayana, 2024). Perusahaan yang secara proaktif melakukan audit dan pemantauan sistem dapat memperkuat perlindungan data mereka. Hal ini juga membantu dalam meningkatkan kepercayaan pelanggan terhadap keamanan platform yang mereka gunakan.

Kerentanan Algoritma dan Model Data

Kerentanan algoritma AI sering kali muncul akibat ketergantungan pada data historis yang rentan terhadap manipulasi. Salah satu bentuk serangan adalah data poisoning, di mana data palsu dimasukkan ke dalam model untuk mengubah hasil prediksi atau analisis (Sanjiwani et al., 2024). Ini dapat menyebabkan perusahaan membuat keputusan yang salah, seperti investasi yang tidak menguntungkan atau kebijakan operasional yang tidak efektif. Dampak jangka panjang dari manipulasi data ini mencakup penurunan kepercayaan stakeholder dan potensi kerugian finansial yang besar. Oleh karena itu, langkah-langkah validasi data yang ketat sangat penting untuk memastikan integritas model AI.

Selain manipulasi data, kurangnya transparansi dalam algoritma AI merupakan tantangan besar dalam memastikan keandalan sistem. Banyak algoritma AI berfungsi sebagai black box, di mana proses pengambilan keputusan tidak dapat dilihat atau dipahami oleh pengguna (Juniardi, 2024). Hal ini menyulitkan perusahaan dalam mengidentifikasi kesalahan atau bias yang mungkin terjadi dalam sistem. Ketiadaan transparansi ini juga menurunkan tingkat kepercayaan pengguna terhadap hasil yang dihasilkan oleh AI. Untuk mengatasi masalah ini, diperlukan pengembangan algoritma yang lebih transparan dan dapat diaudit secara independen.

Bias dalam model AI dapat muncul akibat data pelatihan yang tidak representatif atau berkualitas rendah. Misalnya, jika data yang digunakan hanya mencerminkan satu kelompok populasi, hasil prediksi AI akan cenderung bias dan tidak akurat (Ballantine et al., 2024). Dalam konteks bisnis, bias ini dapat mengarah pada pengambilan keputusan yang merugikan, seperti salah sasaran dalam strategi pemasaran atau ketidakadilan dalam evaluasi kinerja karyawan. Audit berkala terhadap model AI membantu mengidentifikasi dan mengurangi bias, sehingga hasil yang dihasilkan lebih objektif dan dapat diandalkan. Validasi data yang berkelanjutan juga penting untuk memastikan model AI bekerja sesuai dengan ekspektasi.

Kepatuhan terhadap Regulasi Data

Kepatuhan terhadap regulasi data seperti GDPR di Eropa dan UU Perlindungan Data Pribadi di Indonesia menjadi prioritas utama bagi perusahaan yang mengadopsi AI. Regulasi ini mengharuskan perusahaan untuk melindungi data pelanggan dengan langkah-langkah keamanan yang ketat, seperti enkripsi dan kontrol akses yang ketat (Goyal et al., 2023). Pelanggaran terhadap regulasi ini dapat mengakibatkan denda besar, yang tidak hanya merugikan secara finansial tetapi juga merusak reputasi perusahaan. Selain itu, perusahaan

harus transparan dalam cara mereka mengelola data pelanggan untuk memenuhi persyaratan hukum. Dengan mematuhi regulasi, perusahaan dapat meningkatkan kepercayaan publik dan membangun hubungan yang lebih baik dengan pelanggan.

Kebijakan privasi yang kuat adalah elemen penting dalam memastikan kepatuhan terhadap regulasi data. Kebijakan ini harus mencakup prosedur yang jelas mengenai pengumpulan, penyimpanan, dan penggunaan data, serta langkah-langkah untuk mencegah penyalahgunaan (Ardi, 2023). Perusahaan juga harus mengedukasi karyawan mereka mengenai pentingnya perlindungan data dan kepatuhan terhadap kebijakan privasi. Kebijakan yang lemah atau tidak konsisten dapat meningkatkan risiko kebocoran data, yang dapat berdampak negatif pada bisnis. Dengan menerapkan kebijakan yang solid, perusahaan dapat melindungi data pelanggan dan menjaga integritas operasional mereka.

Audit reguler terhadap sistem AI dan kebijakan privasi sangat penting untuk memastikan bahwa perusahaan tetap mematuhi regulasi yang berlaku. Audit ini membantu mengidentifikasi potensi pelanggaran dan memperbarui protokol keamanan sesuai dengan perkembangan ancaman baru (Nehemia & Hendrayana, 2024). Disamping itu, Auditor internal memiliki peran yang signifikan dalam memperbaiki tata kelola perusahaan, terutama di sektor layanan kesehatan. Mereka dapat mendukung peningkatan efisiensi operasional dengan mengidentifikasi serta mengatasi kelemahan yang ada dalam sistem pengendalian internal(Hia et al., 2024). Perusahaan harus siap untuk beradaptasi dengan perubahan regulasi, yang sering kali diperbarui untuk mengatasi tantangan baru dalam keamanan data. Dengan pendekatan proaktif ini, perusahaan dapat meminimalkan risiko pelanggaran regulasi dan menjaga keberlanjutan operasional mereka.

Solusi untuk Mengatasi Tantangan Keamanan Data

Penggunaan Blockchain untuk Keamanan Data

Blockchain merupakan teknologi yang menawarkan solusi inovatif untuk menjaga keamanan data dalam sistem berbasis AI. Dengan menggunakan blockchain, setiap transaksi atau perubahan data dicatat dalam ledger yang terdesentralisasi dan terenkripsi, sehingga sulit untuk dimanipulasi (Sanjiwani et al., 2024). Teknologi ini memungkinkan pencatatan yang transparan dan akurat, yang dapat digunakan sebagai jejak audit yang tidak dapat diubah. Dalam konteks AI, blockchain dapat memastikan bahwa data yang digunakan untuk melatih model tetap utuh dan otentik. Integritas data yang terjamin ini membantu perusahaan dalam membuat keputusan yang lebih akurat dan dapat dipercaya.

Salah satu keunggulan utama blockchain adalah mekanisme konsensus yang digunakan untuk validasi data. Dalam jaringan blockchain, setiap perubahan data memerlukan persetujuan dari mayoritas node, sehingga mengurangi risiko manipulasi atau serangan siber (Goyal et al., 2023). Selain itu, teknologi ini menawarkan sistem yang tamper-proof, di mana setiap entri memiliki hash unik yang menghubungkannya dengan entri sebelumnya. Hal ini membuat manipulasi data menjadi hampir mustahil, bahkan jika seorang peretas berhasil mengakses salah satu node. Dengan transparansi yang terjamin, blockchain tidak hanya melindungi data, tetapi juga meningkatkan kepercayaan pelanggan terhadap pengelolaan data yang dilakukan oleh perusahaan.

Kepercayaan pelanggan terhadap pengelolaan data adalah aspek penting dalam membangun hubungan yang kuat dan berkelanjutan. Blockchain memungkinkan pelanggan

untuk memverifikasi secara langsung bagaimana data mereka dikelola, menciptakan tingkat transparansi yang belum pernah ada sebelumnya (Kleizen et al., 2023). Dengan demikian, perusahaan dapat menunjukkan komitmen mereka terhadap keamanan dan privasi data. Selain itu, implementasi blockchain juga membantu perusahaan memenuhi persyaratan regulasi data, seperti GDPR, yang semakin ketat dalam hal pelaporan dan perlindungan data pelanggan. Dalam jangka panjang, penggunaan blockchain dapat menjadi investasi strategis yang meningkatkan reputasi dan daya saing perusahaan di pasar global.

Pemantauan dan Audit Rutin

Pemantauan sistem AI secara real-time merupakan langkah penting dalam mendeteksi ancaman keamanan dengan cepat dan akurat. Teknologi pemantauan berbasis AI mampu mengenali pola anomali dalam aktivitas jaringan, seperti akses tidak sah atau upaya manipulasi data (Das, 2021). Deteksi dini ini memungkinkan tim keamanan untuk merespons ancaman sebelum menyebabkan kerugian yang signifikan. Selain itu, pemantauan yang berkelanjutan membantu perusahaan memahami pola serangan siber yang mungkin berulang, sehingga langkah pencegahan dapat ditingkatkan. Dengan pendekatan ini, risiko kerugian operasional akibat serangan siber dapat diminimalkan.

Audit rutin berperan sebagai elemen kunci dalam menjaga keamanan sistem AI. Proses audit mencakup pemeriksaan menyeluruh terhadap algoritma, validasi data, dan evaluasi celah keamanan dalam sistem (Nehemia & Hendrayana, 2024). Audit ini penting untuk memastikan bahwa sistem tetap sesuai dengan standar keamanan yang berlaku dan dapat menyesuaikan diri dengan ancaman baru. Selain itu, audit juga memberikan pandangan yang objektif tentang efektivitas protokol keamanan yang ada. Dengan melibatkan pihak ketiga untuk melakukan audit independen, perusahaan dapat memastikan bahwa penilaian keamanan mereka bebas dari bias internal.

Audit dan pemantauan rutin tidak hanya bermanfaat dalam mengidentifikasi kerentanan, tetapi juga dalam memperkuat kepercayaan pelanggan dan mitra bisnis. Transparansi dalam pelaksanaan audit menunjukkan bahwa perusahaan memiliki komitmen untuk melindungi data dan menjaga integritas operasional mereka. Laporan hasil audit juga dapat digunakan sebagai bukti kepatuhan terhadap regulasi, yang semakin penting dalam lingkungan bisnis yang diatur secara ketat. Dengan memperbarui sistem secara berkala berdasarkan temuan audit, perusahaan dapat terus meningkatkan pertahanan mereka terhadap ancaman siber dan memastikan keberlanjutan operasional.

Pendidikan dan Pelatihan Keamanan Data

Kesadaran karyawan tentang pentingnya keamanan data adalah komponen vital dalam menjaga integritas sistem AI. Pelatihan keamanan data harus mencakup pemahaman mendalam tentang praktik terbaik dalam pengelolaan data, termasuk bagaimana melindungi data sensitif dari akses yang tidak sah (Alghafiqi & Munajat, 2022). Pelatihan ini juga harus mencakup cara merespons insiden keamanan, sehingga karyawan dapat bertindak cepat dan tepat saat ancaman terdeteksi. Selain itu, pelatihan harus diperbarui secara berkala untuk mencerminkan perkembangan terbaru dalam ancaman siber dan teknologi keamanan. Dengan demikian, perusahaan dapat memastikan bahwa seluruh staf mereka memiliki keterampilan dan pengetahuan yang diperlukan untuk menjaga keamanan sistem.

Selain pelatihan teknis, perusahaan perlu mengembangkan kampanye kesadaran yang berfokus pada pentingnya keamanan data dalam operasional sehari-hari. Kampanye ini dapat mencakup simulasi serangan siber, seperti phishing, untuk menguji kesiapan karyawan dalam mengenali dan mencegah ancaman (Juniardi, 2024). Kegiatan semacam ini membantu membangun budaya keamanan yang kuat di seluruh organisasi. Karyawan yang menyadari potensi ancaman cenderung lebih waspada dan proaktif dalam melaporkan aktivitas mencurigakan. Dengan meningkatkan kesadaran di seluruh tingkat organisasi, risiko kebocoran data atau pelanggaran keamanan internal dapat diminimalkan.

Pentingnya pendidikan dan pelatihan keamanan data juga tercermin dalam penguatan kebijakan internal perusahaan. Kebijakan ini harus mencakup panduan yang jelas tentang penggunaan data, perangkat lunak, dan jaringan perusahaan. Selain itu, perusahaan harus menyediakan saluran pelaporan yang aman bagi karyawan untuk melaporkan potensi pelanggaran atau ancaman. Dengan mendukung karyawan untuk terlibat secara aktif dalam menjaga keamanan data, perusahaan dapat menciptakan lingkungan kerja yang lebih aman dan mendukung implementasi AI yang bertanggung jawab dan efektif.

SIMPULAN

Penerapan Artificial Intelligence (AI) di bidang akuntansi menawarkan manfaat signifikan dalam meningkatkan efisiensi operasional, akurasi pengolahan data, dan kemampuan untuk melakukan analisis prediktif. AI memungkinkan otomatisasi tugas-tugas manual yang memakan waktu, seperti pengolahan laporan keuangan, analisis data transaksi, dan peramalan tren keuangan. Namun, meskipun manfaatnya besar, tantangan keamanan data menjadi perhatian utama, karena data yang digunakan oleh algoritma AI sering kali bersifat sensitif dan sangat berharga bagi perusahaan. Ketergantungan pada data historis dan algoritma yang dilatih untuk menghasilkan keputusan akuntansi membuat sistem ini rentan terhadap serangan siber dan manipulasi.

Ancaman serangan siber, seperti data poisoning dan pencurian data, merupakan salah satu risiko terbesar dalam penerapan AI di akuntansi. Data poisoning terjadi ketika data yang digunakan untuk melatih algoritma AI sengaja dimanipulasi untuk menghasilkan analisis yang salah atau merugikan perusahaan. Serangan ini dapat memengaruhi keputusan akuntansi, seperti laporan keuangan yang tidak akurat atau analisis risiko yang salah. Selain itu, manipulasi algoritma juga menjadi masalah serius, di mana pihak yang tidak bertanggung jawab dapat mengubah atau memodifikasi kode algoritma untuk merubah hasil analisis yang dihasilkan. Hal ini bisa berakibat fatal, terutama dalam sistem audit atau penilaian keuangan yang berkaitan dengan transparansi dan akuntabilitas.

Di samping ancaman tersebut, tantangan regulasi juga harus dipertimbangkan. Banyak negara kini memiliki peraturan ketat mengenai pengelolaan dan pelaporan data sensitif, termasuk data keuangan yang dikelola oleh sistem akuntansi berbasis AI. Ketidakpatuhan terhadap regulasi ini dapat menyebabkan denda besar dan merusak reputasi perusahaan. Oleh karena itu, perusahaan perlu mengintegrasikan strategi mitigasi yang komprehensif untuk menghadapi tantangan keamanan ini. Salah satu langkah penting adalah penggunaan blockchain, yang dapat memberikan transparansi dalam verifikasi data dan menciptakan jejak audit yang aman dan tidak dapat diubah, mengurangi risiko manipulasi data dan meningkatkan keamanan data yang diproses oleh AI.

Untuk memitigasi ancaman ini lebih lanjut, perusahaan harus mengadopsi audit rutin terhadap sistem AI yang digunakan dalam akuntansi. Audit ini memastikan bahwa algoritma bekerja sesuai dengan yang diharapkan, tanpa perubahan yang tidak sah. Selain itu, pelatihan karyawan tentang potensi ancaman siber dan cara melindungi data sensitif juga sangat penting. Dengan meningkatkan kesadaran mengenai keamanan data, perusahaan dapat mengurangi risiko kebocoran atau manipulasi data. Integrasi AI dengan teknologi seperti blockchain, ditambah dengan langkah-langkah pengawasan dan pelatihan yang berkelanjutan, memungkinkan perusahaan untuk memanfaatkan potensi AI sambil melindungi data mereka dari ancaman yang terus berkembang.

DAFTAR PUSTAKA

Click or tap here to enter text.Alghafiqi, B., & Munajat, E. (2022). Impact of Artificial Intelligence Technology on Accounting Profession Dampak Teknologi Artificial Intelligence Pada Profesi Akuntansi. Berkala Akuntansi dan Keuangan Indonesia, 7(2), 140-159. http://dx.doi.org/10.20473/baki.v7i2.27934

Ardi, M., & Bintari, E. D. (2024). Systematic literature review: Risiko privasi dan keamanan data pribadi dalam penggunaan artificial intelligence (AI). Informasi Interaktif: Jurnal Informatika dan Teknologi Informasi, 9(1), 23-28. ISSN 2527-5240

Ballantine, J., Boyce, G., & Stoner, G. (2024). A critical review of AI in accounting education: Threat and opportunity. Critical Perspectives on Accounting, 99, 102711. https://doi.org/10.1016/j.cpa.2024.102711

Das, P. K. (2021). Impact of Artificial Intelligence on Accounting. Sumerianz Journal of Economics and Finance, 4(1), 17-24. DOI: 10.47752/sjef.41.17.24

Goyal, S. B., Rajawat, A. S., Solanki, R. K., Zaaba, M. A. M., & Long, Z. A. (2023). Integrating AI with Cyber Security for Smart Industry 4.0 Application. International Conference on Inventive Computation Technologies (ICICT), 1223-1232. IEEE. http://dx.doi.org/10.1109/ICICT57646.2023.10134374

Hermawan, A. Z., Anggoro, M. N., Lozera, D., & Faroqi, A. (2023, November). Studi Literatur: Ancaman Serangan Siber Artificial Intelligence (AI) Terhadap Keamanan Data di Indonesia. In Prosiding Seminar Nasional Teknologi dan Sistem Informasi (Vol. 3, No. 1, pp. 581-591). https://doi.org/10.33005/sitasi.v3i1.363

Hia, W. V., Miharja, K., Damayanti, N., & Angelina, F. J. (2024). Peran Auditor Internal Dalam Meningkatkan Efektifitas Tata Kelola Perusahaan: Studi Kasus Sektor Kesehatan. Trilogi Accounting & Business Research, 5(1), 48–60.

Juniardi, E. (2024). Peran dan Praktik Artificial Intelligence Akuntansi: Systematic Literature Review. Jurnal Revenue: Jurnal Ilmiah Akuntansi, 4(2), 885-898. https://doi.org/10.46306/rev.v4i2.385

Kleizen, B., Van Dooren, W., Verhoest, K., & Tan, E. (2023). Do citizens trust trustworthy artificial intelligence? Experimental evidence on the limits of ethical AI measures in government. Government Information Quarterly, 40(4), 101834. http://dx.doi.org/10.1016/j.giq.2023.101834

Krishna, V. V. (2024). AI and contemporary challenges: The good, bad, and the scary. Journal of Open Innovation: Technology, Market, and Complexity, 10(1), 100178. https://doi.org/10.1016/j.joitmc.2023.100178

Nehemia, J. P., & Hendrayana, M. R. (2024). Tantangan dan Manfaat AI dalam Perlindungan Data Kantor: Mengoptimalkan Keamanan Informasi. Jurnal Transformasi Bisnis Digital, 1(3), 13-27. https://doi.org/10.61132/jutrabidi.v1i2.108

Putri, D. A., Miharha, K., Azizah, A. N., & Putrie, M. (2024). Analisis Potensi Fraud Dalam Perolehan Cashback Pada Aplikasi Jual Beli Online Di Aplikasi Tiktok. Trilogi Accounting & Business Research, 5(1), 89–103.

Rich, E., & Knight, K. (1991). Artificial Intelligence. New York: McGraw-Hill.

Sanjiwani, P. D. A., Wulandari, A. A. I., Dewi, G. A., & Renta, M. P. P. (2024). The Impact of Artificial Intelligence on Accounting Information Systems. Jurnal Ekonomi, 13(2), 1220-1234. DOI 10.54209/ekonomi.v13i02

Yusuf, M. F. M., Sari, I. M., Hamid, A., & Garusu, I. A. (2023). Integrasi Teknologi Artificial Intelligence dalam Sistem Akuntansi Modern. Journal of Trends Economics and Accounting Research, 4(1), 230-234. https://doi.org/10.47065/jtear.v4i1.902