Jurnal Akuntansi, Keuangan, Perpajakan dan Tata Kelola Perusahaan (JAKPT)
Volume 3, No 4 – Juni 2026
e ISSN: 3025-9223

PERAN KECERDASAN BUATAN DALAM KEAMANAN DATA DAN AUDIT: SEBUAH TINJAUAN LITERATUR SISTEMATIS

Dewi Rosaria[1*]
[1,]Institut Informatika dan Bisnis Darmajaya
dewirosaria@darmajaya.ac.id

Received: 03-06-2026	Revised: 20-06-2026	Approved: 27-06-2026

ABSTRAK

Penelitian ini bertujuan meninjau secara sistematis peran Kecerdasan Buatan (AI) dalam keamanan data dan audit. Perkembangan transformasi digital meningkatkan kompleksitas pengelolaan data organisasi, risiko keamanan siber, serta kebutuhan audit yang lebih cepat, akurat, dan berkelanjutan. Literatur ditelusuri terutama melalui basis data Scopus dengan dukungan pemeriksaan metadata pada laman penerbit, menggunakan kombinasi kata kunci terkait AI, audit, keamanan data, keamanan siber, kepatuhan, dan tata kelola AI. Penelitian ini bertujuan meninjau secara sistematis peran Kecerdasan Buatan (AI) dalam keamanan data dan audit. Penelusuran dilakukan pada database Scopus, ScienceDirect, dan SpringerLink dengan pedoman PRISMA . Dari 97 dokumen awal, 17 studi memenuhi kriteria inklusi dan dianalisis menggunakan sintesis tematik. Hasil menunjukkan bahwa AI mendukung deteksi ancaman secara real-time, identifikasi anomali, otomatisasi prosedur audit, analisis prediktif, dan pemantauan kepatuhan. Namun, manfaat tersebut bergantung pada kualitas data, transparansi algoritma, perlindungan privasi, kesiapan infrastruktur, dan kompetensi auditor. Studi ini menyimpulkan bahwa AI berperan transformatif dalam memperkuat keamanan data dan kualitas audit, tetapi penerapannya harus disertai tata kelola AI, prinsip privacy-by-design, serta pengawasan manusia.

Kata kunci: *Audit;Keamanan Data; Keamanan Siber; Kepatuhan; Kecerdasan Buatan; Tata Kelola AI.*

PENDAHULUAN

Transformasi digital telah membawa perubahan mendasar dalam cara organisasi mengelola data, menjalankan aktivitas bisnis, serta melakukan pengawasan terhadap proses operasional dan keuangan. Organisasi pada era digital tidak hanya dihadapkan pada peningkatan volume data, tetapi juga pada kompleksitas transaksi, ancaman keamanan siber, dan tuntutan kepatuhan terhadap regulasi perlindungan data. Dalam situasi tersebut, pendekatan konvensional yang bersifat manual, periodik, dan berbasis aturan statis sering kali belum memadai untuk mendeteksi risiko secara cepat dan akurat. Oleh karena itu, Kecerdasan Buatan (AI) menjadi teknologi yang semakin relevan karena mampu menganalisis data dalam jumlah besar, mengenali pola, mendeteksi anomali, dan memprediksi risiko secara adaptif (Nandy & Dubey, 2026; Sarker, 2021).

Dalam bidang keamanan data, AI memiliki peran penting dalam meningkatkan kemampuan organisasi untuk mengidentifikasi ancaman siber secara real-time. Teknologi ini mampu memproses data berskala besar, mengenali pola aktivitas yang tidak wajar, serta menemukan indikasi pelanggaran keamanan yang sulit dideteksi melalui sistem konvensional. Sistem keamanan berbasis AI juga dapat belajar dari data historis sehingga mampu menyesuaikan diri terhadap jenis ancaman baru yang terus berkembang. Kemampuan tersebut menjadikan AI sebagai instrumen penting dalam mendeteksi aktivitas mencurigakan, serangan malware, advanced persistent threats, serta potensi penyalahgunaan akses terhadap data sensitif (Brandao, 2025; Jha & Singh, 2026; Sarker, 2021).

Selain berkontribusi dalam keamanan data, AI juga memberikan pengaruh

besar terhadap perkembangan praktik audit. Audit tradisional pada umumnya dilakukan secara periodik dan berbasis sampel, sehingga memiliki keterbatasan dalam memeriksa transaksi digital yang sangat kompleks dan berjumlah besar. Kehadiran AI memungkinkan auditor menganalisis dataset besar, mengotomasi pekerjaan audit yang bersifat rutin, meningkatkan akurasi pemeriksaan, serta mendukung deteksi kecurangan dan kesalahan keuangan. Dengan dukungan AI, auditor dapat lebih memusatkan perhatian pada analisis risiko, interpretasi bukti audit, dan pengambilan keputusan profesional, sementara pekerjaan teknis seperti pengolahan data dan penyusunan laporan dapat dilakukan secara otomatis (Appelbaum et al., 2017; Fedyk et al., 2022; Stumke & Swanepoel, 2025).

Perkembangan audit berbasis teknologi menunjukkan pergeseran paradigma dari otomasi audit berbasis aturan statis menuju sistem adaptif berbasis data. Pada periode awal, analitik audit banyak diarahkan untuk memperluas cakupan pemeriksaan dan memproses big data dalam audit modern (Appelbaum et al., 2017). Namun, perkembangan AI pada periode 2024-2026 bergerak lebih jauh melalui pemanfaatan machine learning, deep learning, natural language processing, dan model prediktif untuk mendukung continuous auditing, deteksi anomali, dan penilaian risiko secara real-time. Pergeseran ini menunjukkan bahwa AI tidak hanya berfungsi sebagai alat otomasi, tetapi juga sebagai sistem pembelajaran yang mampu menyesuaikan diri terhadap pola risiko baru dalam audit dan keamanan data (Al-Omush et al., 2025; Brandao, 2025; Rejjaoui et al., 2026).

Meskipun AI menawarkan berbagai manfaat, penerapannya dalam keamanan data dan audit tidak terlepas dari tantangan. Tantangan tersebut meliputi kualitas data, risiko serangan terhadap sistem AI, bias algoritma, rendahnya transparansi model, perlindungan privasi, serta kesiapan infrastruktur dan sumber daya manusia. Penggunaan AI yang melibatkan pemrosesan data dalam jumlah besar juga menimbulkan persoalan mengenai kepemilikan data, persetujuan penggunaan data, dan perlindungan hak individu. Oleh sebab itu, implementasi AI perlu memperhatikan prinsip etika, keamanan, transparansi, akuntabilitas, dan kepatuhan terhadap regulasi yang berlaku (Anastasiadou, 2025; Geçikli, 2025; Sidorova et al., 2025; Tariq, 2025).

Sejumlah tinjauan literatur terdahulu telah membahas AI dalam audit atau keamanan siber secara terpisah. Namun, sebagian besar kajian masih menempatkan audit sebagai domain assurance dan keamanan data sebagai domain teknis teknologi informasi. Celah tersebut menimbulkan kebutuhan terhadap kajian yang mengintegrasikan kedua domain tersebut dalam satu kerangka konseptual. Keunikan artikel ini terletak pada upaya menyintesis peran AI sebagai penghubung antara keamanan data dan audit, dengan menekankan hubungan antara deteksi ancaman, continuous auditing, akuntabilitas algoritmik, dan tata kelola AI. Dengan demikian, artikel ini tidak hanya memetakan manfaat teknologi, tetapi juga mengkaji batasan, risiko, dan agenda riset empiris yang lebih spesifik bagi pengembangan audit dan keamanan data berbasis AI.

KAJIAN TEORITIS

Kecerdasan Buatan dalam Sistem Informasi

Kecerdasan buatan merupakan teknologi yang memungkinkan sistem komputer melakukan berbagai aktivitas yang umumnya membutuhkan kecerdasan manusia, seperti mengenali pola, memproses bahasa alami, mengambil keputusan,

memprediksi suatu kejadian, dan belajar dari data. Dalam konteks organisasi, AI banyak diterapkan melalui machine learning, deep learning, natural language processing, sistem pakar, dan analitik prediktif.

AI memiliki peran penting dalam sistem informasi karena mampu mengolah data dalam jumlah besar secara cepat dan akurat. Teknologi ini tidak hanya digunakan untuk mengotomasi proses kerja, tetapi juga untuk meningkatkan kualitas analisis dan pengambilan keputusan. Dalam bidang audit dan keamanan data, AI digunakan untuk mendeteksi anomali transaksi, mengidentifikasi aktivitas jaringan yang mencurigakan, memprediksi risiko, serta mendukung proses kepatuhan terhadap regulasi (Appelbaum et al., 2017; Nandy & Dubey, 2026; Sarker, 2021).

Keamanan Data dan Keamanan Siber

Keamanan data merupakan upaya untuk melindungi data dari akses tidak sah, kehilangan, kerusakan, pencurian, maupun penyalahgunaan. Keamanan data mencakup kerahasiaan, integritas, dan ketersediaan data. Sementara itu, keamanan siber berfokus pada perlindungan sistem, jaringan, perangkat, dan data dari berbagai ancaman digital.

AI memperkuat keamanan data melalui deteksi ancaman secara real-time, analisis perilaku pengguna, identifikasi anomali, penguatan kontrol akses, serta otomasi respons insiden. Dengan kemampuan belajar dari pola data, AI dapat membantu organisasi mengenali ancaman yang sebelumnya belum dapat dideteksi oleh sistem keamanan tradisional (Brandao, 2025; Jha & Singh, 2026; Nandy & Dubey, 2026; Sarker, 2021).

Audit Berbasis Teknologi

Audit merupakan proses sistematis untuk memperoleh dan mengevaluasi bukti secara objektif guna menilai kesesuaian informasi dengan kriteria tertentu. Dalam lingkungan digital, audit tidak hanya berfokus pada laporan keuangan, tetapi juga mencakup audit sistem informasi, audit keamanan, audit kepatuhan, dan audit operasional berbasis data.

AI dan analitik data mengubah praktik audit melalui otomasi tugas rutin, analisis data besar, deteksi kecurangan, pemantauan kepatuhan, dan pelaporan real-time. Auditor dapat menggunakan teknologi analitik untuk menguji populasi data yang lebih luas, bukan hanya sampel tertentu, sehingga kualitas bukti audit dapat meningkat (Al-Omush et al., 2025; Appelbaum et al., 2017; Fedyk et al., 2022; Stumke & Swanepoel, 2025).

Etika dan Tata Kelola AI

Penerapan AI memerlukan tata kelola yang bertanggung jawab karena AI dapat memproses data sensitif dan menghasilkan keputusan yang berdampak signifikan bagi organisasi maupun individu. Isu utama dalam tata kelola AI meliputi transparansi algoritma, akuntabilitas, perlindungan privasi, pengendalian bias, keamanan model, dan kepatuhan terhadap regulasi.

Dalam konteks audit dan keamanan data, prinsip explainable AI, privacy-by-design, dan human oversight perlu diterapkan agar AI dapat digunakan secara aman, adil, dan dapat dipercaya (Anastasiadou, 2025; Geçikli, 2025; Sidorova et al., 2025; Tariq, 2025).

METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode systematic literature review (SLR). Metode ini digunakan untuk mengidentifikasi, mengevaluasi, dan menyintesis literatur yang relevan mengenai peran AI dalam keamanan data dan audit. Pendekatan SLR dipilih karena mampu memberikan pemetaan konseptual secara sistematis terhadap berbagai temuan penelitian sebelumnya.

Sumber Literatur dan Strategi Penelusuran

Penelusuran literatur dilakukan pada database Scopus, ScienceDirect, dan SpringerLink. Ketiga database ini dipilih karena mencakup publikasi mengenai audit, sistem informasi, keamanan siber, dan kecerdasan buatan. Sintaks penelusuran yang digunakan adalah: ("artificial intelligence" OR "AI" OR "machine learning") AND ("audit" OR "auditing" OR "assurance") AND ("data security" OR "cybersecurity" OR "information security"). Penelusuran dibatasi pada publikasi berbahasa Inggris dalam rentang 2017-2026. Metadata artikel yang lolos kemudian diperiksa kembali melalui laman penerbit dan DOI resmi.

Justifikasi Batasan Literatur

Jumlah literatur final sebanyak 17 referensi memang relatif terbatas untuk SLR yang bersifat bibliometrik. Namun, artikel ini tidak dimaksudkan sebagai pemetaan bibliometrik berskala besar, melainkan sebagai SLR tematik yang berfokus pada integrasi dua domain spesifik, yaitu AI dalam keamanan data dan AI dalam audit. Sampel dipersempit untuk menjaga kedalaman sintesis, memastikan metadata bibliografis dapat diverifikasi, dan menghindari penggunaan referensi yang tidak relevan atau tidak dapat ditelusuri. Rentang tahun 2017-2026 dipilih karena tahun 2017 merepresentasikan fondasi awal big data dan analitik dalam audit modern, sedangkan periode 2024-2026 menggambarkan perkembangan mutakhir AI adaptif, deep learning, dan tata kelola AI.

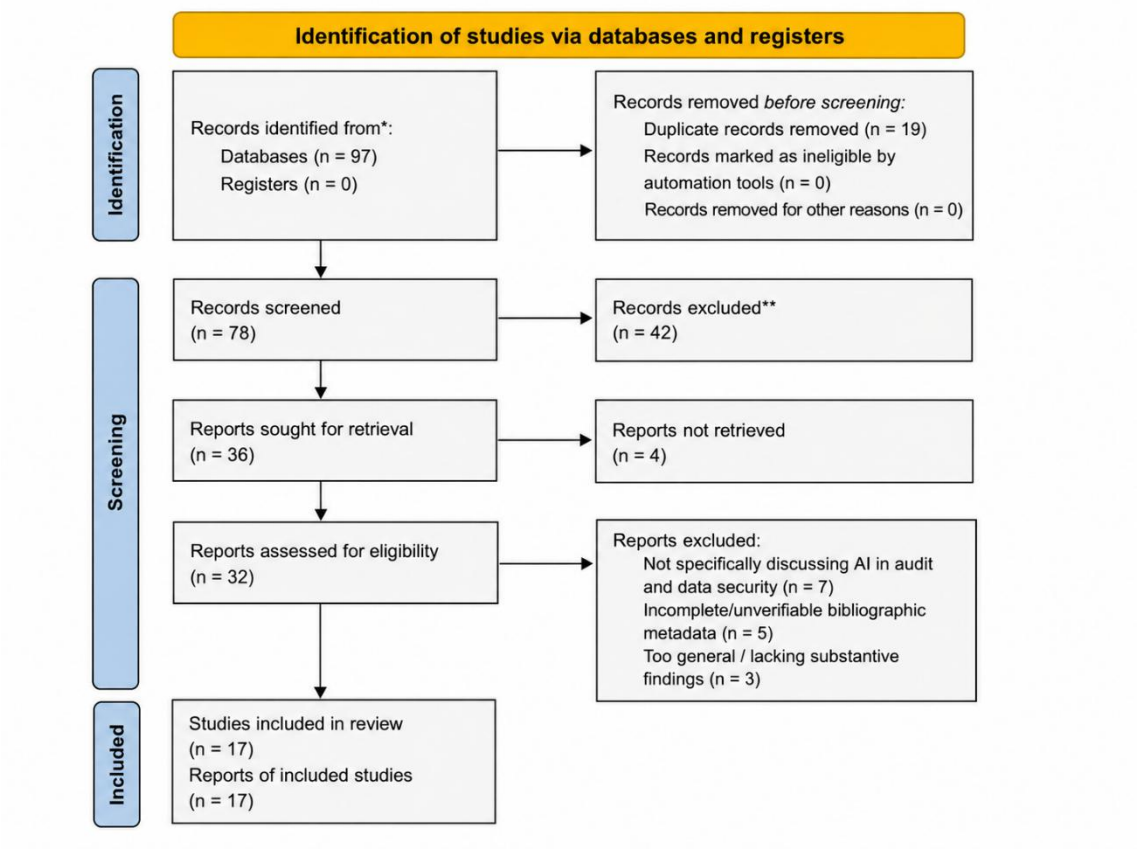
Kriteria Inklusi dan Eksklusi

Kriteria inklusi meliputi: (1) literatur membahas AI, audit, keamanan data, keamanan siber, kepatuhan, atau tata kelola AI; (2) diterbitkan dalam jurnal, prosiding, atau penerbit akademik bereputasi; (3) relevan dengan proses audit, deteksi ancaman, respons insiden, perlindungan data, atau akuntabilitas algoritmik; dan (4) memiliki metadata bibliografis yang dapat ditelusuri. Kriteria eksklusi meliputi literatur yang tidak relevan dengan topik, hanya membahas AI secara umum tanpa kaitan dengan audit atau keamanan data, serta referensi yang metadata publikasinya tidak dapat diverifikasi.

Proses Seleksi Literatur

Proses seleksi literatur mengikuti diagram alir PRISMA 2020 pada Gambar 1. Sebanyak 97 dokumen teridentifikasi dari database. Setelah 19 dokumen duplikat dihapus, 78 dokumen disaring berdasarkan judul dan abstrak. Sebanyak 42 dokumen dikeluarkan pada tahap ini karena tidak relevan. Dari 36 laporan yang dicari full text-nya, empat laporan tidak berhasil diperoleh. Selanjutnya, 32 laporan

dinilai kelayakannya dan 15 laporan dikeluarkan karena tidak membahas keterkaitan AI, audit, dan keamanan data secara spesifik, metadata tidak dapat diverifikasi, atau temuan terlalu umum. Sebanyak 17 studi akhirnya digunakan sebagai unit analisis.



Gambar 1. Diagram alir seleksi literatur berdasarkan PRISMA 2020

Teknik Analisis Data

Analisis data dilakukan dengan analisis tematik. Temuan dari literatur dikodekan dan dikelompokkan ke dalam tema: peran AI dalam keamanan data, peran AI dalam audit, sinergi audit-keamanan data, tantangan etika dan regulasi, serta rekomendasi penguatan tata kelola AI.

HASIL DAN PEMBAHASAN

Matriks Sintesis Literatur

Untuk memperkuat analisis, Tabel 1 merangkum fokus domain, pendekatan, dan temuan utama dari 17 referensi yang digunakan. Matriks ini digunakan untuk membandingkan perbedaan tujuan, pendekatan, dan implikasi setiap studi dalam keamanan data dan audit.

Tabel 1 Matrik Sintesis Literatur

Referensi	Fokus Domain	Pendekatan	Temuan Utama
Aadithyan et al. (2024)	Etika AI	Kajian teknis-etis	Menekankan risiko etis pada metode berbasis AI, terutama tanggung jawab, keamanan, dan dampak penggunaan data.

Al-Omush et al. (2025)	Audit keuangan	Kajian konseptual/empiris	AI meningkatkan akurasi, transparansi, dan kualitas assurance melalui otomasi dan analitik.
Anastasiadou (2025)	Etika AI	Analisis korespondensi faktorial	Menunjukkan pentingnya pemetaan faktor etika seperti bias, akuntabilitas, dan transparansi.
Appelbaum et al. (2017)	Audit modern	Kajian konseptual	Big data dan analitik memperluas cakupan audit dan mendorong kebutuhan riset audit berbasis data.
Bader et al. (2026)	Praktik audit	Kajian literatur	Otomasi dan AI mengubah peran auditor dari pemeriksa manual menjadi analis berbasis teknologi.
Brandao (2025)	Ancaman persisten	Kajian/analisis keamanan	AI membantu mendeteksi advanced persistent threats melalui analisis pola dan anomali.
Fedyk et al. (2022)	Proses audit	Studi empiris	Investasi AI berkorelasi dengan peningkatan kualitas audit dan perubahan struktur pekerjaan audit.
Geçikli (2025)	Etika AI	Systematic review	Integrasi AI perlu dikawal oleh prinsip etika, privasi, dan tanggung jawab sosial.
Jha & Singh (2026)	Deteksi malware	Kajian teknis	Machine learning dan AI memperkuat deteksi malware dan identifikasi ancaman.
Leocádio et al. (2024)	Kerangka audit AI	Systematic review	Menawarkan kerangka konseptual yang menggeser audit dari pemeriksaan retrospektif menuju monitoring proaktif.
Nandy & Dubey (2026)	Keamanan siber	Prosiding/kajian aplikasi	AI memperkuat deteksi ancaman dan respons siber secara lebih cepat.
Rejjaoui et al. (2026)	Audit internal	Resource-based view	Kapabilitas AI meningkatkan kualitas audit internal melalui sumber daya teknologi dan kompetensi.
Sarker (2021)	Deteksi anomali siber	Pemodelan machine learning	Machine learning efektif untuk mendeteksi cyber-anomalies dan multi-attacks.
Sidorova et al. (2025)	Tata kelola AI	Kajian hukum-etika	Transparansi, keamanan, dan kerahasiaan menjadi dasar akuntabilitas AI.
Stumke & Swanepoel (2025)	Audit dan kepatuhan	Bab buku	AI mendukung otomasi proses audit dan monitoring kepatuhan.
Tariq (2025)	Data dan etika AI	Bab buku	Pengumpulan data untuk AI menimbulkan isu privasi, consent, dan kepemilikan data.
Thaluru et al. (2025)	IT audit dan assurance	Bab buku	AI memperkuat assurance melalui integrasi analitik, deteksi anomali, dan pengujian otomatis.

Peran AI dalam Keamanan Data

AI memberikan kontribusi besar dalam meningkatkan keamanan data, terutama melalui kemampuan deteksi ancaman secara real-time. Sistem berbasis AI mampu memantau aktivitas jaringan, perilaku pengguna, dan lalu lintas data untuk menemukan pola yang tidak normal. Ketika sistem mendeteksi aktivitas mencurigakan, AI dapat memberikan peringatan lebih cepat dibandingkan metode manual.

(Nandy & Dubey, 2026) menegaskan bahwa AI dapat memperkuat keamanan siber melalui deteksi ancaman dan respons yang lebih cepat. (Brandao, 2025) menunjukkan bahwa AI relevan untuk mendeteksi advanced persistent threats yang bersifat tersembunyi dan berlangsung dalam jangka panjang. (Sarker, 2021) memperkuat argumen tersebut dengan menunjukkan bahwa machine learning dapat digunakan untuk mendeteksi anomali dan multi-attacks melalui pemodelan berbasis data.

Dibandingkan dengan continuous auditing, deteksi malware lebih membutuhkan algoritma yang kuat dalam klasifikasi pola teknis dan identifikasi variasi serangan. Dalam konteks ini, model supervised learning, ensemble learning, deep learning, serta pendekatan berbasis pola anomali lebih sesuai untuk deteksi malware dan intrusion detection. Sebaliknya, continuous auditing lebih membutuhkan algoritma yang dapat menjelaskan penyimpangan transaksi, seperti anomaly detection, clustering, rule-based analytics, natural language processing, dan explainable AI agar hasilnya dapat dipertanggungjawabkan sebagai bukti audit.

Peran AI dalam Audit

Dalam bidang audit, AI berperan meningkatkan efisiensi, akurasi, dan kualitas pengambilan keputusan.(Stumke & Swanepoel, 2025) menjelaskan bahwa AI dapat diterapkan dalam proses audit dan kepatuhan, terutama untuk mengotomasi tugas rutin, memproses data, dan mendukung penyusunan laporan. (Fedyk et al., 2022) menunjukkan bahwa investasi AI dalam proses audit berhubungan dengan peningkatan kualitas audit dan perubahan struktur kerja auditor. Sejalan dengan itu, (Thaluru et al., 2025) menekankan bahwa integrasi AI dalam audit dan assurance memperluas penggunaan analitik lanjutan, deteksi anomali, serta otomasi prosedur pengujian.

Kontribusi utama AI dalam audit terletak pada kemampuan menganalisis data dalam jumlah besar. Audit tradisional sering menggunakan pendekatan berbasis sampel karena keterbatasan waktu dan sumber daya. Melalui AI dan data analytics, auditor dapat memeriksa populasi transaksi yang lebih luas serta menemukan anomali yang mungkin tidak terlihat melalui teknik audit konvensional (Appelbaum et al., 2017).

Dari sisi efektivitas algoritma, continuous auditing tidak semata-mata memerlukan algoritma dengan akurasi klasifikasi tertinggi, tetapi juga membutuhkan model yang dapat dijelaskan, stabil, dan dapat diaudit kembali. Oleh karena itu, decision tree, random forest yang dilengkapi interpretasi fitur, clustering untuk segmentasi transaksi, serta NLP untuk analisis dokumen audit dapat lebih tepat digunakan dibandingkan model deep learning yang sangat kompleks tetapi sulit dijelaskan. Hal ini berbeda dengan deteksi malware, yang sering kali menuntut kemampuan klasifikasi teknis berkecepatan tinggi dan toleransi interpretabilitas yang lebih rendah.

Sinergi AI antara Keamanan Data dan Audit

Keamanan data dan audit memiliki hubungan yang erat. Data yang tidak aman dapat menurunkan kualitas audit, sedangkan audit yang lemah dapat menyebabkan organisasi gagal mendeteksi risiko keamanan. Dalam konteks ini, AI berperan sebagai penghubung antara kedua bidang tersebut.

(Appelbaum et al., 2017) menjelaskan bahwa big data dan analitik dalam

audit modern menuntut auditor untuk memahami sistem klien yang semakin terintegrasi dengan cloud, Internet of Things, dan sumber data eksternal. Kondisi tersebut menunjukkan bahwa audit modern tidak dapat dipisahkan dari isu keamanan data. Data yang digunakan dalam audit harus dijaga integritas, kerahasiaan, dan ketersediaannya agar bukti audit yang dihasilkan tetap andal.

Sinergi antara AI, keamanan data, dan audit dapat dilihat dalam tiga bentuk. Pertama, AI memungkinkan continuous auditing dan continuous monitoring. Kedua, AI mendukung smart auditing melalui deteksi anomali, pemrosesan bahasa alami, dan analisis dokumen. Ketiga, AI memperkuat mitigasi risiko melalui penilaian risiko prediktif dan respons insiden otomatis.

Tantangan Implementasi AI dalam Audit dan Keamanan Data

Meskipun AI menawarkan berbagai manfaat, implementasinya masih menghadapi tantangan kualitas data. AI sangat bergantung pada data yang digunakan untuk pelatihan dan analisis. Apabila data tidak lengkap, tidak akurat, atau mengandung bias, hasil analisis AI juga dapat menjadi tidak tepat.

Tantangan berikutnya adalah bias algoritma, privasi, dan kepemilikan data. (Aadithyan et al., 2024; Anastasiadou, 2025; Geçikli, 2025; Tariq, 2025) menekankan bahwa penggunaan AI perlu memperhatikan keadilan, consent, dan perlindungan hak individu. Dalam konteks audit, bias algoritma dapat memengaruhi penilaian risiko, pemilihan sampel, dan interpretasi anomali. Dalam konteks keamanan data, bias dapat menyebabkan sistem salah mengidentifikasi aktivitas pengguna sebagai ancaman atau gagal mendeteksi ancaman yang sebenarnya.

(Leocádio et al., 2024) menawarkan kerangka konseptual yang memosisikan AI sebagai pendorong perubahan praktik audit dari pemeriksaan retrospektif menuju pemantauan proaktif dan real-time. Kerangka tersebut menekankan bahwa integrasi AI tidak cukup dipahami sebagai adopsi alat, tetapi harus dilihat sebagai perubahan proses audit, kompetensi auditor, dan mekanisme pengambilan keputusan. Dengan demikian, tantangan utama tidak hanya bersifat teknis, tetapi juga organisatoris.

Di sisi lain, (Sidorova et al., 2025) menempatkan transparansi, keamanan, dan kerahasiaan sebagai fondasi akuntabilitas AI. Jika kerangka (Leocádio et al., 2024) menekankan transformasi proses audit, maka (Sidorova et al., 2025) menegaskan batas normatif agar transformasi tersebut tidak mengorbankan privasi dan tanggung jawab hukum. Sintesis kedua pandangan ini menunjukkan bahwa implementasi AI dalam audit perlu memenuhi dua syarat sekaligus, yaitu efektivitas teknis dan akuntabilitas tata kelola.

Pembahasan Kritis

Hasil sintesis menunjukkan bahwa AI memiliki peran transformatif dalam keamanan data dan audit. Namun, manfaat AI tidak dapat digeneralisasi untuk semua konteks. Dalam keamanan siber, efektivitas AI sangat bergantung pada kecepatan deteksi, kemampuan memproses sinyal teknis, dan pembaruan model terhadap pola serangan baru. Dalam audit, efektivitas AI lebih banyak ditentukan oleh kemampuan model menghasilkan bukti yang dapat dijelaskan, ditelusuri, dan dipertanggungjawabkan.

Dengan demikian, algoritma yang optimal untuk deteksi malware belum tentu

optimal untuk continuous auditing. Deteksi malware cenderung menekankan akurasi prediksi dan respons cepat, sedangkan continuous auditing menuntut interpretabilitas, konsistensi, dan kesesuaian dengan standar audit. Perbedaan ini menegaskan bahwa pemilihan algoritma AI harus disesuaikan dengan tujuan, risiko, dan karakteristik data yang dianalisis.

AI juga tidak sepenuhnya menggantikan auditor, melainkan mengubah peran auditor dari pelaksana prosedur manual menjadi evaluator risiko, pengawas sistem cerdas, dan penilai akuntabilitas algoritmik. (Bader et al., 2026) menegaskan bahwa otomasi dan AI mendorong pergeseran kompetensi auditor ke arah penguasaan analitik data, pemahaman teknologi, dan penilaian profesional atas keluaran sistem. Oleh karena itu, integrasi AI perlu didukung oleh kualitas data, kesiapan infrastruktur, kompetensi auditor, dan tata kelola yang jelas. Tanpa prasyarat tersebut, AI berpotensi menghasilkan efisiensi semu, yaitu proses audit menjadi lebih cepat tetapi tidak selalu lebih andal.

KESIMPULAN

Berdasarkan hasil tinjauan literatur sistematis, AI berperan penting dalam memperkuat keamanan data dan meningkatkan kualitas audit. Pada keamanan data, AI mendukung deteksi ancaman, identifikasi anomali, dan respons insiden yang lebih cepat. Pada audit, AI memperluas cakupan pengujian data, mendukung pemantauan berkelanjutan, serta membantu penilaian risiko dan kepatuhan.

Sintesis menunjukkan bahwa kebutuhan algoritma berbeda menurut domain. Deteksi malware menuntut kecepatan klasifikasi dan kemampuan adaptasi terhadap variasi serangan, sedangkan continuous auditing menekankan keterjelasan model, integrasi dengan kontrol internal, dan kemampuan penelusuran bukti. Karena itu, implementasi AI perlu disesuaikan dengan tujuan pengendalian, karakteristik data, dan tingkat risiko organisasi.

Tantangan utama implementasi AI mencakup kualitas data, bias algoritma, privasi, keamanan model, transparansi, kesiapan infrastruktur, dan kompetensi auditor. Oleh sebab itu, nilai AI tidak hanya ditentukan oleh kecanggihan teknologinya, tetapi juga oleh tata kelola yang memastikan akuntabilitas, perlindungan data, dan pengawasan manusia.

SARAN

Penelitian mendatang disarankan mengembangkan model empiris yang lebih spesifik. Salah satu rancangan yang dapat diuji adalah pengaruh explainable AI sebagai variabel independen terhadap tingkat kepercayaan auditor atas opini audit sebagai variabel dependen, dengan transparansi algoritma atau kompetensi digital auditor sebagai variabel moderasi.

Riset kuantitatif berikutnya juga dapat menguji pengaruh kualitas data, kesiapan infrastruktur AI, dan dukungan tata kelola AI terhadap kualitas audit berkelanjutan. Variabel dependen yang dapat digunakan antara lain kualitas audit, efektivitas deteksi kecurangan, ketepatan penilaian risiko, dan tingkat kepatuhan keamanan informasi.

Dari sisi organisasi, implementasi AI perlu diarahkan pada kerangka tata kelola yang mencakup audit algoritmik, explainable AI, pengendalian bias, keamanan model, dan perlindungan privasi. Auditor juga perlu meningkatkan kompetensi dalam analitik data, keamanan informasi, dan tata kelola AI agar

mampu memanfaatkan teknologi secara efektif tanpa mengabaikan prinsip etika dan profesionalisme.

DAFTAR PUSTAKA

Aadithyan, Shnain, A. H., Sharma, V., Lafta, A. M., Mudhafar, M., Ghobash, A., & Jawad, A. Q. (2024). The Technical Ethics used in Bad and SD Methods: A Deep Review. *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 1226–1230. https://doi.org/10.1109/ICACITE60783.2024.10616634

Al-Omush, A., Almasarwah, A., & Al-Wreikat, A. (2025). Artificial intelligence in financial auditing: Redefining accuracy and transparency in assurance services. *EDPACS*, *70*(6), 1–20. https://doi.org/10.1080/07366981.2025.2459490

Anastasiadou, S. D. (2025). Exploring AI Ethics Through Factorial Correspondence Analysis. In *Modern International Developments in Data Analysis and Multivariate Statistical Analysis* (pp. 495–527). Scopus. https://doi.org/10.4018/979-8-3693-9400-7.ch016

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and Analytics in the Modern Audit Engagement: Research Needs. *Auditing: A Journal of Practice & Theory*, *36*(4), 1–27. https://doi.org/10.2308/ajpt-51684

Bader, A., Alqerem, R., Shatnawi, A., Alqtish, A. M., & Abdallah, A. A. J. (2026). Exploring the Impact of Automation and AI on Auditing Practices and the Evolving Role of Auditors. In A. R. Alshehadeh, I. A. El-Qirem, & G. A. Elrefae (Eds.), *Artificial Intelligence in Business* (Vol. 1502, pp. 3–11). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-96622-4_1

Brandao, P. R. (2025). Exploring the Role of Artificial Intelligence in Detecting Advanced Persistent Threats. *Computers*, *14*(7), 245. https://doi.org/10.3390/computers14070245

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*, *27*(3), 938–985. https://doi.org/10.1007/s11142-022-09697-x

Geçikli, M. (2025). Ethical Considerations in the Integration of Artificial Intelligence: A Systematic Review. In *Navigating Modern Digital Communication Ethics and Law* (pp. 421–451). Scopus. https://doi.org/10.4018/979-8-3373-1702-1.ch014

Jha, S. K., & Singh, A. K. (2026). *Optimizing Cybersecurity—Utilizing Machine Learning and AI for Advanced Malware Detection and Threat Identification*. *1692 LNNS*, 721–736. Scopus. https://doi.org/10.1007/978-981-95-3701-3_46

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. *Administrative Sciences*, *14*(10), 238. https://doi.org/10.3390/admsci14100238

Nandy, M., & Dubey, A. (2026). *Applications of artificial intelligence to strengthening cyber security for threat detection and response*. *3345*(1). Scopus. https://doi.org/10.1063/5.0298670

Rejjaoui, R., El Amri, A., Eddine, A. S., & Marzougui, Y. (2026). The role of artificial intelligence in enhancing internal audit quality: A resource-based view approach. *Multidisciplinary Reviews*, *9*(9). Scopus. https://doi.org/10.31893/multirev.2026406

Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things*, *14*, 100393. https://doi.org/10.1016/j.iot.2021.100393

Sidorova, A. V., Bidova, B. B., & Bogatyrev, M. R. (2025). *Ethical and Legal Issues of Artificial Intelligence: Transparency, Security and Confidentiality*. *1552 LNNS*, 584–590. Scopus. https://doi.org/10.1007/978-3-031-99598-9_83

Stumke, O., & Swanepoel, M. J. (2025). Artificial Intelligence in Auditing and Compliance Processes. In *Artificial Intelligence and Accounting: Ethical, Legal, and Social Implications* (pp. 69–81). Scopus. https://doi.org/10.4324/9781003571643-5

Tariq, M. U. (2025). Ethical Implications of Collecting and Using Data to Power AI Tools. In *Empowering Learners With AI: Strategies, Ethics, and Frameworks* (pp. 201–228). Scopus. https://doi.org/10.4018/979-8-3373-7386-7.ch009

Thaluru, M., Gupta, M., Liao, Z., Zhang, T., & Sharman, R. (2025). Impact of AI on Audit and Assurance: In M. Gupta, J. Walp, & R. Sharman (Eds.), *Advancing IT Audits Through Integrative Approaches and Emerging Technologies* (pp. 63–100). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3078-5.ch003