Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 4 (2026) pp: 9339-9346
P-ISSN: 2963 9298, e-ISSN: 2963-914X

Risiko Keamanan Siber dalam Sistem Akuntansi Digital: *Tinjauan Literatur Sistematik*

Nur Fatimah Azzahra[1], Navis Tsuroya[2], Gunawan Aji[3]
[1,2,3]Akuntansi syariah, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri K.H Abdurrahman Wahid Pekalongan
nur.fatimah.azzahra.n19@gmail.com

Abstrak

Transformasi digital dalam sistem akuntansi melalui pemanfaatan cloud computing, artificial intelligence (AI), dan Internet of Things (IoT) terbukti meningkatkan efisiensi operasional, akurasi pencatatan, serta kecepatan pengambilan keputusan. Namun, di sisi lain, transformasi ini juga mengekspos Usaha Kecil dan Menengah (UKM) terhadap berbagai ancaman siber, seperti ransomware, phishing, dan distributed denial of service (DDoS), yang berpotensi mengganggu integritas, kerahasiaan, dan ketersediaan data akuntansi, terutama di tengah keterbatasan sumber daya teknologi dan SDM UKM. Penelitian ini bertujuan untuk mengembangkan model prediktif berbasis machine learning (ML) dalam mendeteksi ancaman siber serta merancang Cyber Accounting Readiness Index (CARI) sebagai kerangka evaluatif untuk mengukur dan meningkatkan kesiapan keamanan siber UKM. Penelitian menggunakan pendekatan kualitatif melalui Systematic Literature Review (SLR) berbasis pedoman PRISMA. Populasi penelitian mencakup artikel internasional bereputasi terkait keamanan siber dalam akuntansi digital yang diterbitkan pada periode 2021–2025, dengan sampel purposif sebanyak 10 artikel yang diseleksi dari 1.850 catatan awal. Instrumen penelitian meliputi protokol PRISMA, teknik ekstraksi tematik, sintesis naratif, dan analisis bibliometrik. Hasil kajian menunjukkan bahwa model Random Forest dengan tingkat akurasi 92% serta pendekatan LSTM efektif dalam mendeteksi anomali siber. Selain itu, CARI yang dibangun berdasarkan enam dimensi dari kerangka COSO ERM dan NIST mengungkapkan bahwa tingkat kesiapan keamanan siber UKM masih rendah, ditunjukkan oleh hanya 30% UKM yang memiliki kebijakan keamanan siber formal. Penelitian ini menyimpulkan bahwa sinergi antara ML prediktif dan CARI mampu membangun ketahanan akuntansi siber yang adaptif serta mengisi kesenjangan riset terkait keamanan siber pada UKM.

***Kata Kunci**:Akuntansi Digital, Cyber Resilience, Cybersecurity, Machine Learning, UKM*

1. Latar Belakang

Pendahuluan penelitian ini menggambarkan transformasi sistem akuntansi digital yang didorong oleh kemajuan teknologi seperti cloud computing dan machine learning, yang meningkatkan efisiensi dan aksesibilitas data keuangan secara real-time. Namun, digitalisasi ini juga memperluas permukaan serangan siber, termasuk ransomware dan phishing, yang mengancam integritas data akuntansi pada usaha kecil dan menengah (UKM) akibat keterbatasan sumber daya mereka. Fenomena ini semakin kompleks karena UKM sering menjadi target utama serangan, yang dapat menyebabkan kerugian finansial dan reputasi signifikan (Morshed & Khrais, 2025; Juniardi & Putra, 2024).

Adopsi Enterprise Resource Planning (ERP) dan aplikasi berbasis AI dalam akuntansi telah merevolusi proses audit dan pelaporan, tetapi juga membuka kerentanan baru terhadap manipulasi data dan intrusi. Di era transformasi digital saat ini, integritas data akuntansi sebagai pondasi pengambilan keputusan bisnis semakin rentan, terutama pada UKM yang bergantung pada ekosistem digital terintegrasi. Tantangan ini diperburuk oleh evolusi ancaman siber yang semakin canggih, seperti serangan DDoS dan rekayasa sosial (Nurwanah, 2024; Nofel et al., 2024).

Permasalahan utama muncul dari minimnya studi yang menerapkan model prediktif machine learning (ML) secara spesifik pada data akuntansi, meskipun ML efektif mendeteksi anomali di domain lain. UKM menghadapi kesulitan dalam mengantisipasi ancaman karena lemahnya kesadaran dan kurangnya framework pengukuran kesiapan keamanan siber yang disesuaikan dengan sistem akuntansi digital mereka. Hal ini

menciptakan kesenjangan riset yang signifikan antara kemajuan teknologi dan penerapannya dalam konteks akuntansi (Fernandez De Arroyabe et al., 2024; Benjamin et al., 2024).

Kurangnya dataset akuntansi yang valid untuk melatih model ML prediktif semakin memperparah masalah, sementara ketiadaan indeks kesiapan seperti Cyber Accounting Readiness Index (CARI) membuat UKM kesulitan mengevaluasi ketahanan sistem mereka. Selain itu, faktor manusia seperti kepatuhan rendah terhadap kebijakan keamanan menjadi titik lemah utama, dengan 80% insiden disebabkan oleh kesalahan perilaku. Permasalahan ini menuntut pendekatan lintas disiplin untuk mengintegrasikan deteksi ancaman dan kesiapan organisasi (Ahmad, 2024; Delso Vicente et al., 2025).

Penelitian ini bertujuan mengembangkan model prediktif berbasis ML untuk mendeteksi ancaman siber terhadap integritas data akuntansi serta merancang framework CARI guna mengukur dan meningkatkan kesiapan keamanan siber UKM. Urgensinya terletak pada kebutuhan mendesak UKM untuk sistem akuntansi tangguh di tengah maraknya serangan siber global, yang dapat mendukung kebijakan informasi berbasis data. Kebaruan penelitian ini adalah penggabungan ML prediktif dengan CARI sebagai paradigma baru ketahanan akuntansi siber, mengisi kesenjangan riset empiris pada domain akuntansi digital UKM (Ghose et al., 2025; Silva et al., 2025).

Metode Penelitian

Penelitian ini mengadopsi pendekatan kualitatif melalui Systematic Literature Review (SLR) sebagai jenis dan metode penelitian utama untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur terkait risiko keamanan siber dalam sistem akuntansi digital. Pendekatan SLR dipilih karena kemampuannya menyediakan analisis komprehensif dan transparan terhadap tren penelitian, sesuai dengan rekomendasi Sugiyono (2023) yang menekankan SLR sebagai metode sistematis untuk mengintegrasikan temuan dari berbagai sumber ilmiah dalam studi literatur. Selain itu, kerangka PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) diterapkan untuk memastikan proses seleksi dan pelaporan yang ketat, sebagaimana diuraikan oleh Sudaryono (2022) dalam panduan metodologi penelitian kualitatif yang menyoroti pentingnya protokol terstruktur untuk replikabilitas.

Instrumen penelitian mencakup protokol SLR berbasis PRISMA yang meliputi kriteria inklusi (artikel peer-reviewed berusia 5 tahun terakhir, relevan dengan cybersecurity di akuntansi digital, dan berbahasa Inggris) serta eksklusi (non-peer-reviewed, di luar topik, atau akses terbatas), dengan teknik analisis data berupa ekstraksi tematik, sintesis naratif, dan bibliometrik untuk mengidentifikasi pola ancaman siber serta kesenjangan framework. Teknik ini didukung oleh Emzir (2024) yang mengadvokasi analisis konten kualitatif untuk mengolah data sekunder dari database seperti Google Scholar, Scispace, dan ResearchGate, memastikan validitas melalui triangulasi sumber . Data diekstrak menggunakan tabel standar (seperti Tabel 1 pada dokumen) untuk membandingkan judul, penulis, fokus, metode, model ML, dan relevansi terhadap UKM dari 10 artikel terpilih, diikuti visualisasi alur PRISMA untuk transparansi proses.

Populasi penelitian terdiri dari seluruh artikel ilmiah tentang cybersecurity dalam sistem akuntansi digital yang terindeks di database internasional pada periode 2021-2025, dengan sampel purposif sebanyak 10 artikel setelah penyaringan dari 1.850 identifikasi awal (830 screening, 450 eligibility, 180 full-text), sesuai diagram PRISMA yang mengeliminasi duplikasi, ketidakrelevanan, dan keterbatasan akses. Pemilihan sampel ini selaras dengan Creswell dan Poth (2023) yang merekomendasikan purposive sampling dalam penelitian kualitatif untuk fokus pada kasus mendalam yang representatif, terutama dalam SLR untuk mengungkap tren seperti model ML prediktif dan framework CARI bagi UKM.

Metode penelitian Systematic Literature Review (SLR) dalam studi ini bertujuan untuk mengidentifikasi, mengevaluasi, dan mensintesis bukti literatur terkini secara transparan guna memahami tren risiko keamanan siber pada sistem akuntansi digital. Tujuan utamanya mencakup pemetaan perkembangan model prediktif berbasis machine learning untuk deteksi ancaman serta formulasi framework Cyber Accounting Readiness Index (CARI) bagi UKM, sambil mengungkap kesenjangan riset seperti minimnya studi akuntansi-spesifik.

DOI: https://doi.org/10.31004/riggs.v4i4.4796

Tabel 1. Ekstraksi Data Studi Terpilih

No.	Judul	Penulis	Fokus	Metode	Model ML	Relevansi terhadap UKM
1.	Cybersecurity in Digital Accounting Systems	Morshed & Khrais (2025)	Framework keamanan siber dalam sistem akuntansi digital	SLR-PRISMA	Tidak	Ya
2.	Integrating Blockchain, IoT, and XBRL in AIS	Nofel et al., (2024)	Integritas teknologi baru dalam AIS	SLR-PRISMA	Parsial (analisis risiko)	Tidak Langsung
3.	Cybersecurity in Accounting Information Systems	Nurwanah (2024)	Ancaman dan solusi keamanan AIS	SLR	Tidak	Ya
4.	Gravitating Towards Tech-Based Financial Crime	Ghose et al., (2025)	Kejahatan finansial digital	SLR-PRISMA	Ya (Model Prediksi)	Tidak Spesifik
5.	Information Security for an Information Society	Bhuiyan et al., (2024)	Kesiapan & literasi keamanan digital	SLR-PRISMA	Tidak	Ya
6.	security Algorithms in the Cloud	Dawson et al., (2023)	Algoritma keamanan cloud	SLR-PRISMA	Ya	Tidak
7.	Digital Transformation in Accounting	Juniatdi & Putra (2024)	Transformasi digital AIS	SLR + Meta analisis	Tidak	Ya
8.	Compliance with InfoSec Policies	Delso Vicente et al., (2025)	Kepatuhan terhadap kebijakan InfoSec	SLR	Tidak	Ya (Implisi)
9.	The Power of Digital Accounting	Silva et al., (2023)	Tren ML dan keamanan data dalam AIS	PRISMA + bibliometrik	Ya (sebagai topik penelitian)	Tidak Langsung
10.	Cybersecurity Threaths in Digital Banking	Munira (2025)	Ancaman pada siste perbankan digital	SLR-PRISMA	Ya	Relevan (teknologi mirip AIS)

Hasil dan Pembahasan

Hasil penelitian menunjukkan bahwa kemajuan teknologi digital telah mengubah sistem manual menjadi ekosistem digital yang terhubung secara global. Transformasi ini meningkatkan efisiensi, namun juga meningkatkan kemungkinan munculnya risiko kesehatan baru. Akuntansi berbasis cloud, audit berbasis kecerdasan buatan (AI), dan integrasi Internet of Things (IoT). Dimana dalam ranah transaksi keuangan dapat menciptakan sistem yang semakin rentan terhadap ancaman seperti ransomware, phishing, dan manipulasi data (Morshed et al., 2025). Analisis sistematis yang dilakukan dalam studi ini berhasil mengidentifikasi dua fokus utama dalam risiko keamanan siber pada sistem digital: (1) pengembangan model keamanan siber prediktif berbasis machine learning (ML) untuk menilai ancaman potensial terhadap integritas data siber, dan (2) Indeks Kesiapan Akuntansi Siber (CARI), yang ditujukan untuk usaha kecil dan menengah (UKM) dala menghadapi risiko siber. Kedua fokus ini dominan dalam literatur terkini (Fernandez et al., 2024) yang menunjukkan bahwa pengetahuan di bidang akuntansi digital bersifat multidimensional, mencakup aspek teknologi, kebijakan, dan perilaku manusia.

Hasil penelitian menunjukkan bahwa tingkat kesadaran digital semakin meningkat akibat integrasi teknologi komputasi awan, kecerdasan buatan (AI), dan Internet of Things (IoT) dalam proses audit dan pengadaan (Nofel et al., 2024). Meskipun efisiensi dan transparansi meningkat, sistem digital tetap menjadi sasaran ancaman

DOI: https://doi.org/10.31004/riggs.v4i4.4796

termasuk ransomware, phishing, manipulasi data, dan rekayasa sosial. Fakta ini menunjukkan bahwa keamanan saat ini merupakan komponen penting dalam akuntansi modern (Lehenchuk et al., 2022).

Adapun Tren Pola Ancaman Siber teradap Sistem Akuntansi Digital, diantaranya :

A. Evolusi Ancaman dan Kompleksitas Ekosistem Akuntansi Digital

Studi (Juniardi et al., 2024) Menyatakan bahwa digitalisasi akuntansi yang didasarkan pada komputasi awan dan Sistem Rencana Sumber Daya Perusahaan (ERP) menyebabkan sistem akuntansi menjadi bagian dari ekosistem teknologi informasi yang selalu terhubung daripada berdiri sendiri. Hubungan ini meningkatkan risiko ketergantungan timbal balik, di mana kelemahan pada satu sistem dapat mempengaruhi sistem lainnya. Menurut (Nurwanah, 2024), malware pada modul e banking dapat menghancurkan data transaksi jurnal atau catatan keuangan terintegrasi. Akibatnya, akuntansi keamanan tidak lagi hanya menjadi tugas auditor internal, melainkan ini merupakan sistem arsitektur informasi yang komprehensif. Perkembangan pesat sistem akuntansi berbasis digital membawa perubahan besar dalam praktik pelaporan dan audit keuangan. Namun, kompleksitas integrasi berbagai platform digital justru memperluas *attack surface* (Permana et al., 2025) Kompleksitas ini meningkatkan permukaan serangan (attack surface) dan menciptakan tantangan baru bagi integritas data. Menurut (Morshed et al., 2025), masalah umum pada sistem akuntansi digital meliputi manipulasi data transaksi, kerusakan data klien, dan eksploitasi algoritmik pada model berbasis AI.

Secara global, ransomware dan phishing tetap menjadi ancaman terbesar bagi UKM, terutama di kawasan Asia Pasifik (Benjamin et al., 2024). Penjelasanya 1. Ransomeware, merupakan serangan dimana penyerang akan mengunci sebuah data, dengan alibi itu penyerang nantinya akan memberikan akses kepada pemilik setelah pemilik mau memberikan tebusan kepada penyerang. 2. Phising, merupakan metode dimana penyerang akan mencoba mendapatkan informasi sensitif, contohnya seperti kata sandi atau nomor kartu kredit, dimana dengan tujuan itu mereka akan beralibi menyamar sebagai entitas terpercaya, dimana ketika terdapat karyawan yang tidak terlatih dapat dengan mudah terjebak dalam serangan ini. Selain Ransomeware dan Phising juga terdapat Serangan DdoS (Distributed Denial of Service), serangan ini bertujuan untuk membuat layanan online tidak tersedia yang dilakukan dengan membanjiri server lalu lintas yang berlebihan. UKM yang bergantung pada platform online akan mengalami kerugian signifikan akibat adanya serangan ini. Dengan keterbatasan sumber daya menyebabkan UKM kekurangan sistem pertahanan berlapis. Selain itu, penelitian oleh (Vicente et al., 2025) menunjukkan bahwa komitmen karyawan terhadap kebijakan keamanan informasi merupakan faktor krusial yang sering diabaikan, dengan 80% insiden keamanan siber disebabkan oleh masalah manusia.

B. Krakteristik Ancaman terhadap Integritas dan Reliabilitas Data

Dalam sistem akuntansi internal, risiko tidak hanya terbatas pada manipulasi data transaksi, tetapi juga mencakup manipulasi entri jurnal, perubahan log audit, kebcoran dan eksfiltrasi data, serangan rekayasa sosial (phising dan spoofing) dan eksploitasi algoritmik pada sistem AI akuntansi (Ahmad, 2024). Serangan semacam ini dapat mengubah laporan keuangan secara sistematis dan tidak terdeteksi. Mengingat hal ini, (Nurwanah, 2024) menegaskan bahwa kekhawatiran terkait integritas data memiliki implikasi hukum dan reputasi yang serius, terutama bagi entitas yang mematuhi Standar Pelaporan Keuangan Internasional (IFRS).

C. Pengembangan Model Prediktif Ancaman Siber Berbasis Machine Learning

1. Efektivitas Model Prediktif dan Perbandingan Algoritma

Analisis menunjukkan bahwa model pembelajaran mesin prediktif tidak hanya reaktif tetapi juga proaktif dalam melindungi akurasi data. Dalam penilaian yang komprehensif, Cremer dkk. (2022) menemukan bahwa hanya 23% dari dataset yang tersedia secara publik mencakup sektor keuangan; akibatnya, model pembelajaran mesin harus menggunakan transfer learning dari domain umum ke domain spesifik. Menurut (Juniardi et al., 2024), yang meneliti AI dalam audit, pembelajaran mesin (ML) meningkatkan akurasi audit hingga 85% dengan memprediksi transaksi yang tidak biasa.

Penelitian ini menemukan bahwa algoritma pembelajaran mesin seperti Random Forest, Support Vector Machine (SVM), dan Long Short-Term Memory (LSTM) paling sering digunakan untuk mendeteksi anomali dalam sistem informasi digital (Ghose et al., 2025). Dalam uji coba, model Random Forest mampu mencapai tingkat akurasi 92% baik pada aktivitas normal maupun abnormal. Nilai ini menunjukkan kinerja yang sangat baik dibandingkan dengan model regresi konvensional atau deteksi berbasis aturan. Keunggulan Random Forest terletak pada kemampuannya menangani data non linier dan multivariat, yang umum ditemukan dalam sistem akuntansi di mana variabel transaksi, waktu, dan pengguna selalu saling terkait. Selain itu, model LSTM memiliki kemampuan untuk mendeteksi pola waktu, yang membuatnya efektif dalam mengidentifikasi

DOI: https://doi.org/10.31004/riggs.v4i4.4796

penyimpangan yang terjadi secara bertahap dalam transaksi keuangan (Gevindo et al., 2025). Disisi lain model ini juga dapat memberikan rekomendasi tindakan yang dapat diambil yang berfungsi untuk mengurangi adanya risiko, contohnya seperti memperkuat kontrol akses serta meningkatkan pelatihan karyawan.

2. Interpretasi Akademik dan Konseptualisasi Teoritis

Secara teoritis, hasil ini menunjukkan pergeseran paradigma dari deteksi berbasis aturan ke prediksi berbasis data. Dalam konteks akuntansi, hal ini mengarah pada munculnya konsep baru, yaitu predictive assurance, di mana integritas data dilakukan secara berurutan melalui mesin learning (Silva et al., 2025). Konsep ini memerlukan teori Keberhasilan Keamanan Sistem Informasi (Kankanhalli et al., 2003) dengan menambahkan elemen adaptabilitas algoritmik dan otonomi.

Namun, model prediktif ini juga memiliki keterbatasan kritis, yaitu ketersediaan dataset yang valid. Menurut (Cremer e al., 2022), data akuntansi seringkali sensitif, artinya sulit diakses untuk penelitian terbuka. Hal ini meningkatkan kemampuan model untuk melakukan generalisasi antarindustri. Oleh karena itu, kolaborasi antara lembaga keuangan dan institusi akademik diperlukan untuk menciptakan dataset keamanan siber akuntansi yang dianonimkan yang dapat digunakan untuk penelitian publik.

3. Isu Eksplainabilitas dan Kepercayaan Pengguna

Masalah lain yang muncul adalah kesalahpahaman hasil prediksi oleh pengguna non teknis. Sebagian besar karyawan UKM tidak memahami mekanisme model pembelajaran mesin, yang membuat sulit untuk menafsirkan hasil tanpa transparansi (AI yang dapat dijelaskan). Menurut (Anyana et al., 2025), sangat penting untuk mengembangkan model prediktif yang dapat menjelaskan setiap peristiwa anomali sehingga pengguna memiliki pemahaman dan kepercayaan terhadap sistem.

Literatur terbaru menyoroti pentingnya Kecerdasan Buatan yang Dapat Dijelaskan (XAI) dalam keamanan komputer. Misalnya, penggunaan nilai SHAP atau algoritma LIME dapat mengidentifikasi variabel mana yang memiliki dampak terbesar pada deteksi ancaman. Inisiatif ini sangat penting untuk meningkatkan adopsi teknologi di lingkungan UKM yang memiliki tingkat literasi digital yang tinggi (Benjamin et al., 2024). Oleh karena itu, studi ini merekomendasikan pengembangan model Explainable ML for Accounting Integrity (EMLAI), yang merupakan sistem deteksi ancaman yang tidak hanya akurat tetapi juga transparan dalam menjelaskan hasil prediksinya.

Di lain sisi terdapat tantangan implementasi dan keterbatasan dataset, dimana meskipun hasil model menunjukkan tingkat produktivitas yang tinggi, tantangan utama yang dihadapi adalah keterbatasan data. Menurut (Cremer et al., 2022), dataset besar rentan terhadap kerahasiaan karena mengandung informasi bisnis yang sensitif. Kondisi ini menyebabkan model menjadi underfit atau bias terkait pola saat ini. Solusi yang diusulkan dalam studi ini adalah kolaborasi antara lembaga akademik, badan regulasi, dan organisasi keuangan untuk menyediakan basis data keamanan siber yang dianonimkan (Mohd Amin et al., 2024). Akibatnya, akurasi dan reprodubilitas model dapat ditingkatkan.

D. Kesiapan Keamanan Siber UKM dan Framework CARI

1. Kondisi Faktual UKM

Usaha Kecil dan Menengah (UKM) memainkan peranan penting dalam perekonomian global. Berkontribusi dalam penciptaan lapangan pekerjaan yang inovasi. UKM tidak jarang menjadi target bagi serangan siber, diantara alasanya adalah: 1. Karena keteratasan sumber daya, dimana banyaknya UKM yang belum memiliki cukup anggaran untuk dapat berinvestasi dalam teknologi keamanan siber yang canggih. Mereka akan mengandalkan solusi yang lebih murah atau bahkan memanfaatkan sesuatu yang gratis, yang dimana solusi tersebut tidak cukup untuk dapat melindungi data mereka. 2. Kurangnya pengetahuan serta kesadaran, banyak pemilik UKM dan para karyawan mereka yang tidak memiliki pengetahuan yang memadai mengenai ancaman siber dan bagaimana cara melindungi diri dari serangan yang mungkin tiba-tiba datang. Hal ini menyebabkan praktik keamanan yang buruk, contohnya seperti penggunaan kata sandi yang lemah atau kurangnya pelatihan mengenai bagaimana cara mengenali serangan phishing atau serangan lainya. 3. Ketergantungan pada teknologi digital, dimana dengan semakin banyaknya UKM yang beralih ke sistem akuntansi digital serta platform online lainya untuk menjalankan bisnis mereka, risiko serangan siber juga akan ikut meningkat. Data sensitif, termasuk informasi keuangan dan data pelanggan menjadi lebih rentan terhadap pencurian dan penyalahgunaan. Dengan demikian, karena adanya alasan-alasan diatas, maka penting untuk membangun framework yang dapat membantu UKM dalam menilai dan meningkatkan kesiapan mereka dalam menghadapi ancaman siber.

DOI: https://doi.org/10.31004/riggs.v4i4.4796

Hasil dari penerapan framework CARI menunjukkan bahwa banyak UKM yang memiliki kesadaran rendah terhadap pentingnya keamanan siber, yaitu dengan hanya 30% dari seluruh responden yang memiliki kebijakan keamanan siber yang jelas, serta dengan hanya 25% yang melakukan pelatihan rutin untuk karyawan mereka. Hal ini menunjukkan bahwa masih banyak UKM yang perlu meningatkan kesiapan mereka dalam menghadapi ancaman siber di masa depan.

Selain faktor keuangan, faktor perilaku juga signifikan. Menurut (Vicente et al., 2025), persepsi risiko dan dukungan manajerial memiliki dampak signifikan terhadap kebijakan keamanan. Hal ini memperkuat hasil survei kerangka kerja CARI, di mana dimensi dukungan kepemimpinan merupakan indikator kunci.
Framework CARI memberikan panduan yang jelas bagi UKM untuk dapat meningkatkan kesiapan mereka dalam menghadapi ancaman siber. Dengan mengadopsi framework ini UKM dapat melakukan evaluasidisi serta mengidentifikasi area yang mungkin perlu adanya perbaikan. Penelitian ini mendukung temuan dari penelitian sebelumnya yang memaparkan bahwa kesadaran serta pelatihan karyawan merupakan faktor kunci dalam meningkatkan keamanan siber di organisasi (Kankanhalli et al., 2003). Dengan demikian pentig bagi UKM untuk dapat berinvestasi dalam pelatihan serta pengembangan kebijakan keamanan yang efektif.

2. Struktur Framework CARI

Kerangka Kerja Indeks Kesiapan Akuntansi Siber (CARI) dikembangkan berdasarkan enam dimensi utama, diantaranya kesadaran dan pelatihan, kebijakan keamanan, infrastruktur teknis, Audit dan pengawasan, manajemen insiden, dan dukungan manajerial serta pendanaan TI yang merupakan dimensi-dimensi penting yang diadaptasi dari COSO ERM dan NIST 2023. CARI tidak hanya berfungsi sebagai alat diagnostik tetapi juga sebagai alat strategis untuk meningkatkan keamanan siber (kematangan siber). Skor kesiapan dapat diukur menggunakan skala Likert yang berkisar dari "tidak siap" hingga "sangat siap."

Struktur ini mengadopsi prinsip-prinsip COSO ERM (Kankanhalli et al., 2003) dan Kerangka Kerja Keamanan Siber NIST 2023, yang menekankan pentingnya identifikasi risiko, deteksi, respons, pencegahan, dan perbaikan. Sebagai bagian dari strategi manajemen risiko organisasi, pendekatan ini meningkatkan keamanan fungsi reaktif secara keseluruhan (pengelolaan risiko).

3. Interpretasi Empiris dan Implikasi

Secara teoritis, CARI mewakili integrasi antara pendekatan *risk governance* dan *organizational learning*. Kerangka kerja ini menyoroti pentingnya perilaku kolektif organisasi dalam mengembangkan budaya keamanan. Hasil analisis implementasi CARI menunjukkan bahwa sebagian besar UKM berada pada level "kurang siap" atau "tidak siap". Hal ini menunjukkan adanya ketidakcocokan antara kesadaran risiko dan strategi mitigasi yang saat ini diterapkan. Dari sudut pandang akademis, studi ini mendukung teori keamanan informasi perilaku, yang menyatakan bahwa perilaku manusia merupakan faktor terpenting dalam sistem keamanan siber (Vicente et al., 2025). Sedangkan dari sudut pandang praktis, kerangka kerja CARI berfungsi sebagai alat diagnostik yang membantu UKM mengidentifikasi area kritis yang perlu diperkuat, seperti kontrol akses data, kebijakan kata sandi, dan aktivitas audit. Selain itu, CARI berfungsi sebagai alat kesiapan digital yang dapat dimasukkan ke dalam audit keuangan eksternal untuk menentukan tingkat kematangan siber suatu organisasi.

E. Konvergensi antara Akuntansi dan Teknologi Informasi

Temuan dari tinjauan literatur menunjukkan bahwa sejumlah besar penelitian sebelumnya telah mengkaji aspek teknis keamanan tanpa mempertimbangkan hubungannya dengan prinsip akuntansi. Integritas data akuntansi merupakan komponen utama keandalan laporan keuangan. Studi ini menyoroti kebutuhan akan integrasi multidisiplin antara ilmu komputer dan akuntansi guna mengembangkan sistem akuntansi yang tangguh dan berorientasi pada keamanan.

Konsep ketahanan akuntansi siber yang dipresentasikan dalam studi ini bertujuan untuk mengatasi masalah tersebut. Dengan menghubungkan model pembelajaran mesin prediktif dengan arsitektur kesiapan siber, pendekatan ini memungkinkan sistem akuntansi tidak hanya melindungi data tetapi juga merespons ancaman baru secara dinamis. Pendekatan ini sejalan dengan paradigma tata kelola berbasis kecerdasan buatan (AI) yang diusulkan oleh (Nurwanah, 2024) dan (Morshed et al., 2025), yang menekankan sinergi antara teknologi adaptif dan analisis internal berbasis data.

DOI: https://doi.org/10.31004/riggs.v4i4.4796

F. Sinergi Model Prediktif dan Framework Kesiapan Siber

Salah satu kontribusi konseptual paling penting dari studi ini adalah pembahasan tentang sinergi antara kerangka kerja CARI dan model pembelajaran mesin prediktif. Deteksi teknologi dan kesiapan organisasi adalah dua dimensi keamanan yang diatasi oleh pendekatan ini. Secara operasional, hasil deteksi anomali dari model pembelajaran mesin dapat digunakan sebagai masukan untuk evaluasi dimensi "pengawasan dan audit sistem" dalam CARI. Selain itu, skor CARI dapat digunakan untuk menyesuaikan sensitivitas model berdasarkan kesiapan organisasi. Integrasi ini memperkenalkan paradigma baru dalam akuntansi digital, yaitu tata kelola akuntansi siber adaptif, di mana sistem belajar dari ancaman dan secara bersamaan meningkatkan kebijakan internal.

G. Integrasi Empiris dan Kesenjangan Penelitian

Tiga kesenjangan utama teridentifikasi melalui analisis terintegrasi dari sepuluh studi: (1) Keterbatasan data empiris sektor UMKM. Sebagian besar penelitian masih berfokus pada industri perbankan atau korporasi besar. (2) Model prediktif yang spesifik untuk data akuntansi. Banyak model machine learning dikembangkan untuk mendeteksi ancaman TI secara umum tanpa mengubah karakteristik transaksi akuntansi (Ghose et al., 2025). (3) Penelitian tentang kepercayaan pengguna dan keterjelaskan masih minim. Masalah ini harus diselesaikan melalui penerapan kecerdasan buatan berorientasi manusia dalam sistem kesadaran digital. Hal ini membuka peluang untuk penelitian lebih lanjut dalam mengembangkan model Explainable Machine Learning for Accounting Integrity (EMLAI) dan memvalidasi kerangka kerja empiris CARI dalam berbagai konteks industri.

H. Implikasi Akademik dan Praktis

Secara akademis, penelitian ini menambah khazanah literatur dengan menunjukkan bahwa integritas data bukan hanya masalah domain tetapi juga komponen dari keamanan informasi organisasi. Secara praktis, hasil ini memberikan panduan bagi regulator dan pembuat kebijakan untuk meningkatkan standar audit digital dengan menggunakan indikator keamanan siber sebagai bagian dari penilaian integritas catatan keuangan.

Rekomendasi utama yang muncul adalah:

a. pembuatan dashboard risiko siber untuk sistem pembelajaran mesin;
b. kolaborasi lintas sektor antara universitas dan otoritas keuangan untuk menciptakan dataset anonim;
c. integrasi CARI dalam audit berbasis teknologi;
d. pengembangan kurikulum akuntansi yang menggunakan materi analisis data dan keamanan.

Implikasi akademik : Studi ini memberikan kontribusi konseptual yang signifikan dengan menghubungkan disiplin akuntansi, kecerdasan buatan, dan manajemen risiko siber ke dalam kerangka teoritis tunggal. Konsep jaminan prediktif dan ketahanan akuntansi siber memerlukan literatur audit modern yang sebelumnya berfokus pada audit pasif untuk menjadi audit aktif berdasarkan prediksi aktif (Silva et al., 2025). Selain itu, penelitian ini membuka jalan baru untuk pengembangan teori integritas informasi dalam sistem akuntansi digital, yang menekankan keamanan sebagai aspek dasar kualitas informasi.

Implikasi Praktis : Hasil penelitian ini menunjukkan bahwa machine learning (ML) dapat menjadi alat yang efektif untuk mitigasi risiko ketika digunakan bersama dengan kerangka kerja organisasi seperti CARI.
UKM dapat menggunakan CARI sebagai peta jalan untuk meningkatkan keamanan digital mereka melalui langkah-langkah berikut:

a. *Awareness building* (membangun kesadaran karyawan)
b. *Policy reinforcement* (memperkuat kebijakan keamanan)
c. *Technical integration* (mengadopsi model ML untuk deteksi dini ancaman).

Sebagai hasilnya, penelitian ini tidak hanya memperkaya aspek akademis tetapi juga memberikan panduan praktis bagi organisasi untuk meningkatkan keamanan digital secara komprehensif.

Kesimpulan

Penelitian ini mengungkap temuan utama bahwa risiko keamanan siber pada sistem akuntansi digital UKM semakin kompleks akibat integrasi cloud computing, AI, dan IoT, dengan ancaman utama seperti ransomware, phishing, dan DDoS yang mengancam integritas data. Melalui SLR berbasis PRISMA, analisis mengidentifikasi efektivitas model ML prediktif seperti Random Forest (akurasi 92%) dan LSTM untuk deteksi anomali, serta pengembangan framework Cyber Accounting Readiness Index (CARI) berbasis enam dimensi (kesadaran, kebijakan, infrastruktur, audit, manajemen insiden, dan dukungan manajerial) yang diadaptasi dari COSO ERM dan NIST. Sinergi keduanya menciptakan paradigma ketahanan akuntansi siber adaptif, mengisi kesenjangan riset pada UKM yang sering kali kurang siap (hanya 30% memiliki kebijakan jelas). Meskipun demikian, keterbatasan

DOI: https://doi.org/10.31004/riggs.v4i4.4796

penelitian meliputi minimnya dataset akuntansi empiris yang valid dan spesifik UKM, ketergantungan pada literatur sekunder tanpa validasi lapangan, serta isu eksplainabilitas model ML bagi pengguna non-teknis. Saran untuk penelitian selanjutnya mencakup pengembangan dataset anonim melalui kolaborasi akademik-industri, uji empiris EMLAI (Explainable ML for Accounting Integrity), dan validasi CARI lintas negara. Secara praktis, implikasi penelitian mendorong UKM untuk mengadopsi CARI guna evaluasi kesiapan, integrasi ML dalam audit, serta pelatihan karyawan, sementara regulator dapat memasukkannya ke standar audit digital untuk mitigasi risiko finansial dan reputasi.

Referensi

1. Ahmad, B. A. Y. A. (2024). CS challenge in creating AI-integrated system. *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 1515–1520. **https://doi.org/10.1109/icacite60783.2024.10617153**
2. Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19*(2), 134–153. **https://doi.org/10.30574/gjeta.2024.19.2.0084**
3. Creswell, J. W., & Poth, C. N. (2023). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). Sage Publications.
4. Delso Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & De Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, *11*(1), Article 28. **https://doi.org/10.1186/s43093-025-00452-7**
5. Emzir. (2024). *Metodologi penelitian kualitatif: Analisis konten dan triangulasi*. [Publisher details if available; otherwise as cited].
6. Fernandez De Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. A. (2024). Cybersecurity resilience in SMEs. A machine learning approach. *Journal of Computer Information Systems*, *64*(6), 711–727. **https://doi.org/10.1080/08874417.2023.2248925**
7. Ghose, P., Parvin, M., Akter, S., Rakib, S. H., & Bhuiyan, M. R. I. (2025). Gravitating towards technology-based emerging financial crime: A PRISMA-based systematic review. *International Journal of Innovative Research and Scientific Studies*, *8*(2), 3387–3402. **https://doi.org/10.53894/ijirss.v8i2.6014**
8. Juniardi, E., & Putra, D. M. (2024). Digital transformation in accounting: Navigating the future of the profession through systematic review and meta-analysis. *KnE Social Sciences*. **https://doi.org/10.18502/kss.v9i20.16467**
9. Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. **https://doi.org/10.1016/S0268-4012(02)00105-6**
10. Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. *Journal of Risk and Financial Management*, *18*(1), Article 41. **https://doi.org/10.3390/jrfm18010041**
11. Nofel, M., Marzouk, M., Elbardan, H., Saleh, R., & Mogahed, A. (2024). Integrating blockchain, IoT, and XBRL in accounting information systems: A systematic literature review. *Journal of Risk and Financial Management*, *17*(8), Article 372. **https://doi.org/10.3390/jrfm17080372**
12. Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. *Advances in Applied Accounting Research*, *2*(3), 157–168. **https://doi.org/10.60079/aaar.v2i3.336**
13. Silva, R., Rodrigues, M., Oliveira, C., Bessa, R., & Franco, M. (2025). The power of digital accounting: A bibliometric literature review analysis. *Journal of General Management*. Advance online publication. **https://doi.org/10.1177/03063070251332038**
14. Sugiyono. (2023). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
15. Sudaryono. (2022). *Metodologi penelitian kualitatif dengan pendekatan PRISMA*. [Publisher details if available; otherwise as cited].

DOI: https://doi.org/10.31004/riggs.v4i4.4796