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: 8585-8596
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Tantangan Keamanan Siber dalam Penerapan Sistem Akuntansi Digital: Tinjauan Literatur Sistematik

Uswatun Khasanah[1], Najwa Savira Azzahra[2], Gunawan Aji[3]
[1,2,3]Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negri K.H. Abdurrahman Wahid Pekalongan
[1]uswatun.khasanah23071@mhs.uingusdur.ac.id , [2]najwa.savira.azzahra@mhs.uingusdur.ac.id , [3]gunawanaji@uingusdur.ac.id

Abstrak

Perkembangan transformasi digital telah mendorong perubahan signifikan dalam sistem akuntansi modern, terutama melalui adopsi teknologi berbasis internet, komputasi awan, dan otomatisasi proses. Perubahan ini meningkatkan kecepatan, akurasi, serta efisiensi pengelolaan data keuangan, namun pada saat yang sama memunculkan risiko keamanan siber yang semakin beragam dan sulit dikendalikan. Penelitian ini bertujuan untuk mengidentifikasi pola risiko keamanan siber serta pendekatan mitigasi yang dibahas dalam literatur ilmiah terkait sistem akuntansi digital. Metode yang digunakan adalah Systematic Literature Review dengan tahapan perencanaan, pelaksanaan, dan pelaporan yang terstruktur. Penelusuran artikel dilakukan melalui Google Scholar menggunakan kata kunci relevan dengan rentang publikasi tahun 2020 hingga 2025. Proses seleksi menghasilkan 25 artikel jurnal yang memenuhi kriteria inklusi dan eksklusi untuk dianalisis secara mendalam. Hasil kajian menunjukkan dominasi penelitian yang berfokus pada wilayah Indonesia dengan metode kualitatif sebagai pendekatan utama. Analisis tematik mengelompokkan temuan ke dalam empat area utama, meliputi pemanfaatan blockchain dan kecerdasan buatan, perlindungan data dan privasi informasi, peran kebijakan dan regulasi pemerintah, serta bentuk ancaman cybercrime beserta upaya penanggulangannya. Studi ini juga mengidentifikasi keterbatasan penelitian empiris yang mengevaluasi penerapan keamanan siber secara langsung pada organisasi. Berdasarkan penelitian yang telah dilakukan menunjukkan bahwa penguatan sistem akuntansi digital memerlukan integrasi teknologi yang adaptif, kerangka regulasi yang konsisten, serta peningkatan literasi keamanan siber bagi pelaku organisasi. Pendekatan terpadu tersebut diharapkan mampu mendukung keberlanjutan dan keandalan sistem akuntansi digital di masa depan.

***Kata Kunci**: Keamanan Siber, Sistem Akuntansi Digital, Transformasi Digital, Cybercrime, Regulasi, Systematic Literature Review*

1. Latar Belakang

Perkembangan teknologi digital telah mendorong transformasi signifikan dalam berbagai bidang, termasuk dalam sistem akuntansi. Salah satu bidang yang terdampak langsung oleh transformasi teknologi adalah sektor pelayanan keuangan, terutama sistem akuntansi perbankan (A. N. W. Nugroho, 2025). Perkembangan teknologi juga berdampak pada perubahan yang membawa alternatif dan kemudahan dalam bertransaksi, dimana transaksi dapat dilakukan secara *cashless* yang dapat dilakukan dengan platform *e-wallet* (Putra et al., 2024). Perkembangan teknologi kini semakin bergantung pada perangkat lunak berbasis *cloud computing*, *artificial intelligence* (AI), *big* data, serta teknologi *blockchain* (Novida, 2025). Sistem akuntansi digital kini menjadi tulang punggung utama dalam pengelolaan keuangan perusahaan karena efisiensinya dalam sistem operasional, menekan biaya layanan, serta mempermudah nasabah dalam mengakses rekening mereka melalui platform digital (Harahap, 2025). Selain itu, pemanfaatan AI memungkinkan otomatisasi proses rutin, seperti pencocokan transaksi dan penyusunan laporan keuangan, sehingga memungkinkan akuntan untuk fokus pada tugas-tugas yang membutuhkan keahlian manusia, seperti analisis interpretatif dan pengambilan keputusan (Jayanti, 2024). Dampak yang paling terasa adalah pergeseran pemrosesan data dari pendekatan manual ke sistem berbasis komputer atau digital (Salsabila & Rahman, 2023). Namun, pertumbuhan layanan digital yang pesat juga diiringi oleh dampak negatif berupa meningkatnya ancaman siber. Serangan dunia maya yang berpotensi merusak sistem perbankan, mencuri informasi pribadi, serta menimbulkan kerugian finansial yang signifikan kini semakin sering terjadi secara global (Rahman Najwa, 2024).

Dalam era digital, berbagai bentuk ancaman siber seperti *malware*, *phishing*, *ransomware*, dan serangan *Distributed Denial of Service* (DDoS) terus berkembang dengan tingkat kompleksitas yang semakin

tinggi (Faliha, 2025). *Phishing* adalah metode penipuan dengan memancing korban agar menyerahkan informasi pribadi melalui taktik manipulatif. Sedangkan serangan *malware* dapat mengakibatkan pencurian informasi sensitif, kerugian finansial, dan merusak reputasi. Tujuan utama dari *Cybercrime* adalah mendapatkan keuntungan pribadi secara ilegal, terutama dalam sektor keuangan (Azzahra et al., 2024).

Keamanan dalam sistem informasi akuntansi menjadi aspek krusial yang harus diperhatikan oleh perusahaan di era digital. Ancaman keamanan sistem informasi dapat berasal dari berbagai sumber, baik eksternal maupun internal (Simanjuntak et al., 2025). Sayangnya, banyak organisasi kecil seperti UMKM yang belum menyadari pentingnya sistem pengendalian digital secara menyeluruh (M. A. Nugroho et al., 2024). Bahkan lembaga besar seperti kantor pajak, telah mengalami terjadinya kasus pelanggaran keamanan data pada tahun 2021 lalu, yang menunjukan telah terjadi peretasan data di salah satu kantor pajak (Septian et al., 2024).

OJK (2022) menyatakan bahwa penilaian tingkat kematangan digital bank di Indonesia baik konvensional dan syariah pada aspek manajemen risiko masih cukup rendah yaitu bernilai 43% dimana hal ini menunjukkan strategi perbankan syariah dalam melakukan digitalisasi saat ini masih belum didukung oleh manajemen risiko yang memadai (Fajri & Violita, 2023). Manajemen risiko menjadi kunci untuk menghadapi tantangan ini dengan mengidentifikasi, menganalisis, dan mengendalikan risiko yang mungkin terjadi dalam operasi ekonomi digital (Susanto, 2025).

Penerapan teknologi *blockchain* pada sistem keamana identifikasi pengguna merupakan salah satu inovasi yang sangat menjanjikan dalam dunia teknologi. Teknologi *blockchain* memiliki potensi untuk meningkatkan tingkat keamanan informasi terkait pengidentifikasian pengguna dengan memanfaatkan prinsip desentralisasi dan transparansi yang melekat pada teknologi ini (Afdilah et al., 2024).

Beberapa penelitian sebelumnya telah membahas pentingnya keamanan siber dalam berbagai konteks digital, seperti perbankan syariah, *e-wallet*, dan aplikasi keuangan mobile. Namun demikian, kajian yang secara khusus mengulas risiko keamanan siber dalam sistem akuntansi digital masih terbatas, baik dari segi ruang lingkup maupun pendekatan pemetaan risikonya. Hal ini menunjukkan adanya gap penelitian yang perlu dijembatani agar sistem akuntansi digital dapat berkembang secara aman dan berkelanjutan.

Oleh karena itu, studi ini bertujuan untuk melakukan Tinjauan Literatur Sistematik (*Systematic Literature Review*/SLR) guna mengidentifikasi, menganalisis, dan mensintesis berbagai risiko keamanan siber yang muncul dalam implementasi sistem akuntansi digital. Penelitian ini juga akan mengeksplorasi strategi mitigasi yang telah diusulkan dalam literatur. Selain itu, studi ini akan mengevaluasi sejauh mana pendekatan tersebut dapat diterapkan dalam konteks akuntansi digital.

Adapun struktur artikel ini disusun sebagai berikut: Bagian pertama adalah abstrak yang terdiri atas latar belakang singkat tujuan SLR, metode kajian (*database*, tahun, dan kriteria seleksi), temuan utama, serta kontribusi dan implikasi. Bagian kedua yaitu pendahuluan yang memuat latar belakang dan urgensi topik, masalah atau gap penelitian, tujuan SLR secara eksplisit, dan struktur artikel. Bagian ketiga yaitu metodologi SLR, sebagai bagian wajib dan jantung dari artikel SLR, pada artikel ini kerangka PRISMA digunakan dalam menyusun metodologi SLR. Bagian keempat yaitu hasil dan pembahasan yang menjelaskan mengenai profil studi, kategori tematik, gap penelitian, dan diskusi kritis. Bagian kelima yaitu kesimpulan yang memuat ringkasan hasil utama, kontribusi terhadap ilmu pengetahuan, implikasi praktis, keterbatasan studi, dan arah penelitian masa depan. Bagian keenam yaitu daftar Pustaka dengan format APA berdasarkan referens artikel yang di *review*.

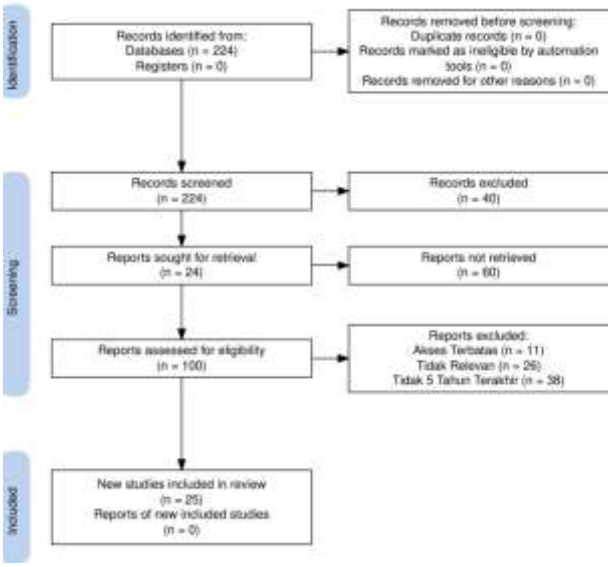
2. Metode Penelitian

Sumber database pada artikel slr dengan judul “Risiko Keamanan Siber dalam Sistem Akuntansi Digital: Tinjauan Literatur Sistematik” adalah Google Scholar dengan kriteria tahun publikasi 5 tahun terakhir, yaitu 2020 – 2025. Jenis dokumen sumber yang digunakan berupa artikel jurnal denga mnggunakan Bahasa Indonesia sesuai dengan topik keamanan siber dalam sistem akuntansi digital.

Strategi pencarian yang digunakan sebagai kata kunci dengan *Boolean operator* yaitu ("keamanan siber" OR "keamanan informasi") AND ("akuntansi digital" OR "sistem akuntansi") AND ("tinjauan pustaka" OR "kajian literatur sistematik" OR "literature review").

DOI: https://doi.org/10.31004/riggs.v4i4.5008

Proses seleksi artikel menggunakan diagram PRISMA mulai dari Identifikasi, kemudian *screening*, *eligibility*, dan *included* sehingga mendapatkan jumlah artikel awal 224 dan jumlah artikel akhir 25. Untuk lebih jelasnya dapat dilihat pada **Gambar 1** berikut :



Gambar 1 Diagram PRISMA

Untuk menjamin validitas dan reliabilitas studi yang disertakan dalam tinjauan literatur sistematik ini, dilakukan penilaian kualitas (*Quality Assessment*) terhadap setiap artikel terpilih. Proses ini menggunakan beberapa kriteria utama, yaitu :

Relevansi terhadap topik

Artikel harus secara eksplisit membahas isu keamanan siber dalam konteks sistem akuntansi digital. Dengan demikian, artikel tersebut memiliki kontribusi yang relevan dan mendalam dalam konteks perlindungan sistem akuntansi digital dari risiko keamanan siber.

Artikel terbit dalam jangka waktu lima tahun terakhir

Artikel yang dipilih yaitu artikel yang terbit dari tahun 2020-2025, karena mengandung informasu yang lebih relevan dengan perkembangan terbaru.

Artikel yang berbahasa Indonesia

Pemilihan artikel yang berbahasa Indonesia bertujuan agar materi yang digunakan lebih mudah dipahami dan diakses oleh peneliti maupun pembaca lokal. Selain itu, penggunaan sumber berbahasa Indonesia juga memastikan konteks budaya, regulasi, dan praktik yang dibahas lebih relevan dengan kondisi di Indonesia.

Artikel yang dipilih memiliki metode penelitian yang valid

Artikel yang dipilih harus menggunakan metode penelitian yang jelas, sistematis, dan dapat dipertanggungjawabkan secara ilmiah. Metode penelitian yang valid memastikan data dan analisis yang diperoleh akurat serta hasilnya dapat dipercaya.

Setelah proses seleksi dan penilaian kualitas artikel, langkah selanjutnya adalah melakukan ekstraksi dan sintesis data secara sistematik. Setiap artikel yang lolos dibaca secara mendalam untuk mengambil informasi kunci yang relevan dengan topik penelitian. Informasi tersebut kemudian ditulis dalam tabel ringkasan kajian agar memudahkan analisis dan perbandingan antar studi. Untuk lebih jelasnya, data ekstrasi dapat dilihat pada **Tabel 1** berikut :

DOI: https://doi.org/10.31004/riggs.v4i4.5008

Tabel 1 Data Extraction

Penulis	Tahun	Tujuan Penelitian	Metode	Temuan Utama
Revira, Rayyan Firdaus	2024	Menganalisis pengaruh akuntansi syariah sebagai instrumen pengendalian risiko di perbankan syariah menghadapi disrupsi digital.	Pendekatan kualitatif, studi literatur, wawancara mendalam dengan praktisi perbankan syariah.	Penerapan akuntansi syariah meningkatkan efisiensi, transparansi, dan kepercayaan nasabah sehingga memitigasi risiko di era digital.
Edy Susanto, Denya Saputri, Deva Adika Prasetya	2023	Menganalisis pengamanan objek vital, keamanan file, dan keamanan siber di PT. Pos Indonesia	Studi literatur dan pengumpulan data primer melalui wawancara dengan pihak terkait di PT. Pos Indonesia.	PT. Pos Indonesia menerapkan pengamanan fisik dan sistem keamanan file yang baik, namun masih terdapat potensi kerentanan di aspek keamanan siber.
Herla Shabahal Khair, Ok Agam, Admar, Mar'atussoliha, Nurlaila	2024	Menganalisis implementasi teknologi *blockchain* dalam akuntansi internasional untuk meningkatkan transparansi dan keamanan	Pendekatan kualitatif, studi literatur, analisis komparatif studi kasus.	*Blockchain* meningkatkan transparansi dan keamanan laporan keuangan global melalui mekanisme kriptografi dan sistem audit yang mudah dilacak.
Wulan Wahyu Ningrum	2024	Mendeskripsikan dampak teknologi digital pada perubahan peran akuntan dan keterampilan baru di era digital	Kualitatif dengan studi literatur atau kajian Pustaka.	Peran akuntan bergeser menjadi analis dan penasihat bisnis strategis, sementara tugas administratif dapat diotomatisasi. Keterampilan analisis data dan manajemen risiko sangat penting.
Sonia Afdilah, Nova Sari Agustina, Ilfa Hani, Indra Gunawan	2024	Mengkaji tantangan adopsi teknologi blockchain dalam keamanan sistem identifikasi pengguna	Metode review jurnal dan analisis kuantitatif	*Blockchain* sangat cocok meningkatkan keamanan sistem identifikasi pengguna dan data, disarankan untuk penggunaan teknologi *blockchain* demi keamanan lebih baik.
Darin Putri Salsabila, Abdul Rahman	2023	Investigasi pengaruh teknologi digital terhadap efisiensi dan keamanan privasi data akuntansi di perusahaan swasta	Studi literatur dengan teknik pengumpulan data sekunder	Teknologi digital berkontribusi pada perubahan praktik akuntansi dan perusahaan perlu adaptasi untuk menjaga efisiensi dan keamanan data.
Shofie Azizah, Zava Nurruzuhrotil Ula, Dwi Mutiaram Michelle Prajna Prameswari	2024	Mengkaji pentingnya keamanan siber dalam aplikasi keuangan mobile menghadapi ancaman *cybercrime*	Deskriptif kualitatif melalui pendekatan SLR. Teknik analisis meta-sintesis diterapkan dalam penelitian ini guna mensintesis data penelitian yang bersumber dari 26 sumber artikel jurnal dalam kurun waktu 2019	Serangan *cybercrime* meningkat karena kelemahan sistem, kurangnya pembaruan, SDM kurang kompeten, dan faktor eksternal seperti malware dan regulasi yang belum jelas.

DOI: https://doi.org/10.31004/riggs.v4i4.5008

			sampai dengan 2024	
Yulianissa Alvina, Wiska Sridayanti, Nabila Azzahra	2024	Menganalisis teknologi *blockchain* dalam sistem akuntansi dan solusi keamanan siber	*Systematic Literature Review* (SLR) dengan total artikel yang digunakan sejumlah 16 dengan rentang tahun 2018-2022.	*Blockchain* dan IoT meningkatkan efisiensi dan akurasi pengelolaan data, namun rentan terhadap serangan *DDoS* dan *Sybil*, perlu solusi keamanan lebih kuat.
Yulisbet Hutapea, Achmad Fauzi, Amanda Dwiyanti, Fajrina Ajeng Alifah, Niyar Andina, Sania Murtafia Dara Jati	2024	Identifikasi teknologi pengendalian dan perlindungan kejahatan keuangan digital.	Kualitatif dengan melakukan pemeriksaan mendalam terhadap kebijakan sosial baru di masyarakat atau untuk memahami isu-isu rumit.	Manajemen keamanan penting dalam melindungi dana digital dengan deteksi risiko responsif dan kolaborasi multipihak menggunakan teknologi canggih.
Diah Rachmawatie Novida	2025	Mengkaji tren, tantangan, peluang digitalisasi sistem informasi akuntansi termasuk *cloud computing* dan AI	Tinjauan Pustaka dengan kualitatif, data dikumpulkan dari Google Scholar untuk periode 2008–2025, dengan seleksi dari 40 artikel menjadi 19 artikel yang relevan.	Digitalisasi sistem informasi akuntansi dengan *cloud* comput*ing*, big data, dan AI meningkatkan efisiensi dan transparansi keuangan.
Hana Elisabet Simanjuntak	2025	Penelitian ini bertujuan untuk menganalisis konsep keamanan dalam SIA serta implementasinya dalam dunia bisnis.	Studi literatur, analisis berbagai strategi keamanan termasuk enkripsi dan 2FA	Keamanan sistem informasi efektif melalui pelatihan karyawan, kebijakan ketat, dan teknologi seperti AI, enkripsi AES-256, Zero Trust, firewall, VPN, dan pemantauan cloud.
Jefri Okinaldi, Nurna Aziza	2024	Memahami perkembangan teknologi audit, hambatan, dan dampaknya pada praktik audit	Metode penelitian yang digunakan adalah kualitatif dengan kajian teoritis berupa teknik pengumpulan data. Penggunaan kajian teoretis ini bermaksud untuk menyelesaikan masalah yang ada di dalam penelitian sesuai sumber dan berpatokan pada penelitian sebelumnya.	Teknologi audit modern meningkatkan efisiensi, akurasi, dan keamanan data, tetapi isu keamanan siber masih menjadi tantangan utama.
Diny Widya Evriyanti Simatangkir, Eka Febriantika Nur Afifah,	2025	Mengkaji ancaman siber di sektor perbankan dan solusi penguatan pertahanan digital	Studi literatur kualitatif	Ancaman *malware*, *phishing*, *ransomware*, *DDoS* membutuhkan teknologi AI dan blockchain, regulasi kuat, serta edukasi bagi karyawan dan nasabah.

DOI: https://doi.org/10.31004/riggs.v4i4.5008

Nafiza Salsabila Faliha				
Fadhila Rahman Najwa	2024	Evaluasi efektivitas kerangka hukum keamanan siber di Indonesia dan kerjasama lintas sektor	Penelitian ini menggunakan metode kualitatif dengan pendekatan analisis data sekunder yang berasal dari sumber hukum, kebijakan pemerintah, dan studi kasus terpilih.	Regulasi sudah ada namun implementasi dan konsistensi kurang, perlu peningkatan kerjasama dan kapasitas penegakan hukum menghadapi kompleksitas keamanan siber.
O. Feriyanto, Zulfa Qur'anisa, Mira Herawati, Lisvi, Melinda Helmalia Putri	2024	Mengkaji perkembangan *FinTech* di Indonesia dan tantangan inklusi keuangan dan keamanan	Metode yang digunakan adalah analisis literatur, di mana berbagai sumber dan studi sebelumnya dikaji untuk memahami bagaimana *FinTech* telah mempengaruhi akses dan interaksi keuangan.	*FinTech* meningkatkan inklusi dan layanan keuangan digital, tetapi tantangan keamanan dan akses teknologi perlu regulasi adaptif dan kolaborasi.
Angelina Wijaya Tan, Nathalie Elshaday Betrix Ambouw, Irda Agustin Kustiwi	2024	Menyelidiki dampak digitalisasi terhadap ekonomi dan Sistem Informasi Akuntansi (SIA)	Menggunakan pendekatan kualitatif.	Digitalisasi membuka peluang besar perubahan positif dalam SIA, namun perusahaan perlu strategi matang untuk mengatasi tantangan transformasi.
Ahmad Septian, Teuku Alfiansyah, Aji Dewa Abdulla, Hedi Sutiawan, Dwi Ali Ega Fauzi, Dimas Hadi Saputram Tubagus Hedi Saepudin	2024	Mengkaji ancaman keamanan data di sistem keuangan kantor pajak dan solusi pencegahan	Metode yang digunakan dalam penelitian ini yaitu metode kualitatif dan melibatkan studi literatur yang berfokus pada sistem manajemen keuangan dan sistem manajemen keamanan pada perkantoran.	Hasil penelitian menunjukkan bahwa pencurian data merupakan ancaman serius dalam kejahatan siber yang berdampak luas. Untuk mengatasinya, diperlukan manajemen risiko yang kuat, dukungan hukum yang terpadu, serta langkah-langkah keamanan menyeluruh dalam sistem informasi, seperti kebijakan yang jelas, pelatihan rutin, dan pembaruan teknologi secara berkala.
Arya Nanda Mahardika Putra, Fayruz Rahma, Elyza Gustri Wahyuni	2024	Mengetahui kesadaran keamanan siber di kalangan pengguna e-wallet dan pengaruh budaya, sosial, psikologis	Penelitian ini menggunakan metode tinjauan pustaka (*literature review*).	Faktor non-teknis seperti budaya dan psikologi berpengaruh besar terhadap keamanan dan kepercayaan transaksi *e-wallet*, implikasi penting bagi penyedia layanan dan pemerintah.
Mahendra Adhi Nugroho, Agatha Yerika Septininditya,	2024	Penelitian ini bertujuan untuk membahas pentingnya	Penelitian ini menggunakan metode kualitatif deskriptif dengan	Hasil penelitian menunjukkan bahwa pengelolaan dan pengendalian sistem informasi

DOI: https://doi.org/10.31004/riggs.v4i4.5008

R. Andro Ziliyo Nugraha		pengelolaan dan pengendalian sistem informasi dalam mendukung pertumbuhan Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia. Tujuan utamanya adalah untuk menunjukkan urgensi penerapan sistem keamanan informasi yang memadai bagi UMKM agar dapat bertahan dan berkembang di tengah tantangan era digital.	pendekatan studi kepustakaan (*library research*). Peneliti mengumpulkan dan menganalisis berbagai sumber literatur terkait isu keamanan sistem informasi pada UMKM sebagai dasar untuk menarik kesimpulan dan memberikan rekomendasi.	sangat penting bagi UMKM, namun sebagian besar masih menerapkannya secara dasar. Banyak UMKM belum menerapkan langkah-langkah keamanan secara optimal, sehingga diperlukan peningkatan kesadaran dan penerapan sistem keamanan yang lebih komprehensif.
Amhar Maulana Harahap	2025	Mengidentifikasi risiko digitalisasi perbankan syariah dan merumuskan strategi mitigasi efektif.	Penelitian ini menerapkan metode kualitatif dengan pendekatan studi kepustakaan.	Hasil penelitian menunjukkan bahwa digitalisasi dalam perbankan syariah membawa manfaat besar seperti efisiensi dan kemudahan akses layanan, namun juga menghadirkan berbagai risiko signifikan seperti serangan siber, kebocoran data, dan rendahnya kesiapan SDM serta infrastruktur.
Muhazzah Alief Faizal, Zelyn Faizatul, Binti Nur Asiyah, Rokhmat Subagyo	2023	Memberikan pemahaman tentang ancaman siber dan solusi perlindungan sistem serta privasi nasabah.	Metode yang digunakan dalam penelitian ini adalah studi literatur dengan menganalisis sumber informasi terpercaya yang relevan terkait risiko keamanan di bank syariah.	Hasil penelitian menunjukkan bahwa bank syariah menghadapi ancaman serius dan semakin kompleks seperti kejahatan siber, malware, phishing, dan pelanggaran data yang dapat merusak sistem dan melanggar privasi nasabah.
Abdul Malik Fajri, Evony Silvino Violita	2023	Mengetahui efektivitas manajemen risiko dalam transformasi digital Bank AS.	Metode yang digunakan adalah pendekatan kualitatif dengan jenis penelitian studi kasus.	Penerapan Risk IT Framework baik, tapi ada kendala: kurang sosialisasi, pelaporan lambat, mitigasi lemah.
Nasywa Shafa Azzahra, Aron Michael Tambunan, Najwa Nayra Aulia, Arista Binarsih, Tubagus Hedi Saepudin	2024	Mengindentifikasi ancaman utama *cybercrime* yang mengincar sektor perbankan, mengevaluasi langkah-langkah keamanan siber yang telah diterapkan oleh bank, serta	Metode yang digunakan adalah tinjauan pustaka (*literature review*) terhadap lima jurnal terkait yang membahas ancaman *cybercrime* seperti *phishing*, *malware*, dan kebocoran data,	Penelitian menegaskan pentingnya peningkatan keamanan siber secara berkelanjutan dan kerjasama antar lembaga untuk menghadapi ancaman *cybercrime* yang semakin kompleks di sektor keuangan.

DOI: https://doi.org/10.31004/riggs.v4i4.5008

		memberikan rekomendasi strategi untuk meningkatkan keamanan siber di industri perbankan.	serta penerapan keamanan siber di sektor perbankan.	
Ari Susanto	2024	Mengeksplorasi berbagai strategi dan pendekatan dalam manajemen risiko di e-bisnis, dengan fokus pada penguatan keamanan data dan mitigasi risiko siber.	Metode deskriptif kualitatif untuk menganalisis strategi manajemen risiko dalam e-bisnis, khususnya terkait keamanan data dan mitigasi risiko siber.	E-bisnis rawan diretas. Solusi AI membantu, tapi pelatihan minim & biaya tinggi jadi hambatan
Afiah Nurrizky, Wahyu Nugroho	2025	Menganalisis kebijakan Otoritas Jasa Keuangan dalam memitigasi kejahatan siber di sektor perbankan, mulai dari landasan hukum, kerangka kebijakan, manajemen risiko, serta kebijakan praktis yang telah dijalankan OJK demi ketahanan siber perbakan Indonesia	Metode penelitian yang digunakann adalah kualitatif degan pendekatan hukum normatif dalam analisis kebijakan. Pengumpulan data dilakukan melalui studi pustaka yang mengumpulkan peraturan perundang-undangan, Peraturan OJK, dan Surat Edaran OJK.	OJK mengelola risiko keamanan siber dengan memberikan pedoman dan pelatihan kepada bank untuk melindungi data nasabah serta menjaga stabilitas dan kelangsungan industri perbankan di era digital.

Sementara sintesis data dilakukan melalui dua pendekatan, yaitu :

a. Sintesis Kualitatif (Deskriptif)
   Berdasarkan hasil kajian terhadap 25 artikel terkait risiko keamanan siber dalam sistem akuntansi digital, dapat disimpulkan beberapa fokus penelitian utama sebagai berikut:
   1. Fokus Penelitian
      Sebagian besar artikel membahas risiko keamanan siber pada sistem akuntansi digital, dengan penekanan pada aspek-aspek seperti:
      a. Teknologi *blockchain* dan AI = 6 Artikel
      b. Keamanan data dan privasi = 10 Artikel
      c. Peran regulasi dan kebijakan pemerintah = 4 Artikel
      d. Ancaman dan Mitigasi *Cybercrime* = 5 Artikel
   2. Tema Utama
      a. Ancaman Siber
         Termasuk *malware, phishing, DDoS*, dan kebocoran data yang banyak diidentifikasi dalam konteks perbankan, *e-wallet*, dan UMKM.
      b. Teknologi Perlindungan
         Penggunaan teknologi seperti *blockchain*, AI, enkripsi AES-256, VPN, *Zero Trust Architecture*, dan *cloud monitoring* sebagai solusi utama.
      c. Peran SDM
         Banyak artikel menekankan pentingnya peningkatan literasi digital dan pelatihan SDM dalam mengurangi risiko internal.
      d. Manajemen Risiko
         Diperlukan *framework* manajemen risiko yang adaptif, termasuk *Risk IT Framework* dan kebijakan keamanan informasi yang kuat.

DOI: https://doi.org/10.31004/riggs.v4i4.5008

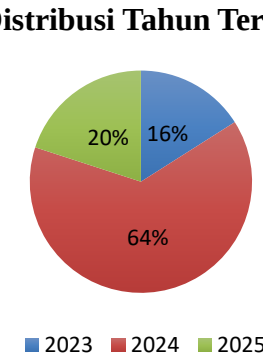
b. Sintesis Kuantitatif (Bibliometrik):
Untuk memahami tren publikasi, dilakukan analisis bibliometrik sederhana menggunakan distribusi frekuensi sebagai berikut :
1. Distribusi Tahun Publikasi
   a. 2023 = 4 Artikel
   b. 2024 = 16 Artikel
   c. 2025 = 5 Artikel
   Hal ini menunjukkan peningkatan minat riset secara signifikan sejak tahun 2023.
2. Metode Penelitian
   a. Kualitatif (Literatur/Wawancara/Studi Kasus) = 22 Artikel
   b. *Systematic Literatur Review* (SLR) = 2 Artikel
   c. Kuantitatif = 1 Artikel
   Pendekatan kualitatif menjadi metode dominan dalam penelitian ini, mengindikasikan sifat eksploratif dan deskriptif riset dalam bidang keamanan siber dan akuntansi digital.

3. Hasil dan Diskusi

Berdasarkan referensi jurnal yang terpilih, dapat dilakukan analisis profil studi sesuai distribusi tahun terbit, metode penelitian yang digunakan, dan negara asal studi. Untuk lebih jelasnya sebagai berikut :

3.1 Distribusi Tahun Terbit

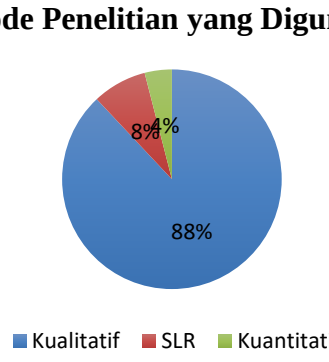
Studi yang dianalisis berkisar sejak tahun 2023 – 2025, dengan total 25 artikel jurnal. Sebagian besar artikel jurnal yang dianalisis terbit pada tahun 2024, yaitu sebanyak 16 artikel jurnal.Kemudian 4 artikel terbit pada tahun 2023 dan 5 artikel terbit pada tahun 2025. Tahun 2024 mendominasi dengan 16 publikasi (64%), menunjukkan lonjakan minat terhadap topik keamanan siber dan digitalisasi dalam sistem informasi akuntansi. Diagram distribusi tahun terbit dapat dilihat pada **Gambar 2** berikut :



Gambar 2 Distribusi Tahun Terbit

3.2 Metode Penelitian yang Digunakan

Sebagian besar studi menggunakan pendekatan kualitatif (88%), hanya sebagian kecil yang menggunakan analisis kuantitatif dan metode *systematic literature review* (SLR). Dengan jumlah metode dengan pendekatan kualitatif sebanyak 22 artikel, 2 artikel dengan metode SLR, dan 1 artikel dengan pendekatan kuantitatif. Diagram metode penelitian yang digunakan dapat dilihat pada **Gambar 3** berikut :

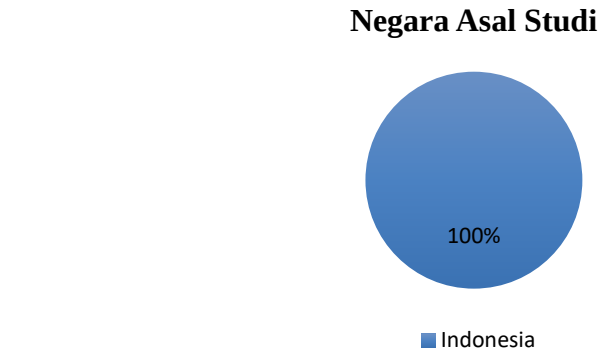


Gambar 3 Diagram Metode Penelitian yang Digunakan

DOI: https://doi.org/10.31004/riggs.v4i4.5008

3.3 Negara Asal Studi

Seluruh studi yang dianalisis (100%) berasal dari peneliti di Indonesia. Ini menunjukkan bahwa isu-isu terkait keamanan siber, digitalisasi sistem informasi akuntansi, serta penerapan teknologi baru seperti blockchain dan AI dalam sektor keuangan dan akuntansi menjadi topik yang relevan dan berkembang pesat di Indonesia. Diagram negara asal studi dapat dilihat pada **Gambar 4** berikut :



Gambar 4 Negara Asal Studi

Dari studi yang dianalisis, kategori tematik dapat dikelompokkan menjadi 4 kategori utama, yaitu :

A. Teknologi *blockchain* dan AI

Sebanyak 6 artikel membahas pemanfaatan teknologi terkini dalam memperkuat sistem informasi akuntansi dan keamanan digital, misalnya studi oleh (Nurlaila, 2024) yang menunjukkan bahwa implementasi *blockchain* dapat meningkatkan transparansi dan keamanan laporan keuangan global.

B. Keamanan data dan privasi sebanyak

Sebanyak 10 artikel membahas mengenai tema ini, misalnya studi oleh (Okinaldi & Aziza, 2024) yang menunjukann ahwa penggunaan teknologi audit dapat meningkatkan efisiensi, namun menimbulkan tantangan terkait keamanan data dan etika yang perlu diatasi.

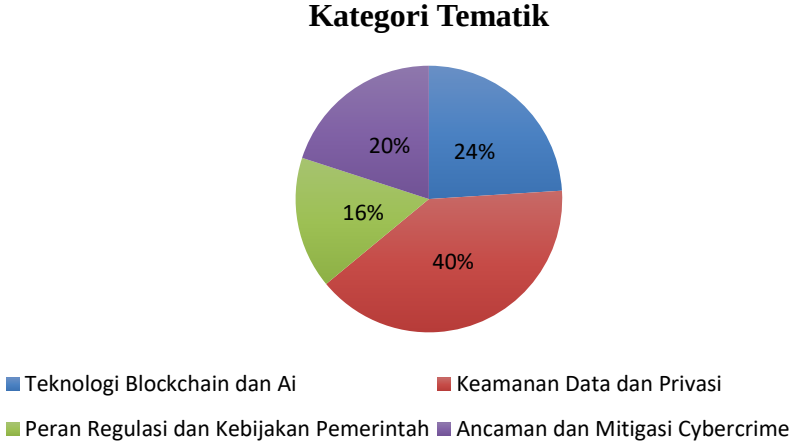
C. Peran regulasi dan kebijakan pemerintah

Sebanyak 4 artikel membahas mengenai peran regulasi dan kebijakan pemerintah, salah satunya ialah studi oleh (Jati, 2024) yang menjelaskan apabila terdapat dasar hukum yang melindungi informasi pribadi klien, yaitu pada UU No. 8 Tahun 2019 tentang Perlindungan Konsumen dan UU No. 2011 tentang Otoritas Jasa Keuangan.

D. Ancaman dan mitigasi *cybercrime*

Sebanyak 5 artikel membahas mengenai ancaman dan mitigasi *cybercrime*, salah satunya ialah studi oleh (Azizah et al., 2024) dan (Edy Susanto et al., 2023) yang membahas mengenai ancaman *cybercrime* dan mitigasinya yang dapat dilakukan dengan penerapan teknologi seperti *firewall* dan *blockchain*, manajemen risiko yang kuat, peningkatan infrastruktur jaringan, pembentukan tim keamanan siber, pengembangan regulasi yang jelas, serta edukasi pengguna untuk meningkatkan kesadaran keamanan siber.

Untuk lebih jelasnya, kategori tematik dapat dilihat pada diagram berikut :



Gambar 5 Kategori Tematik

DOI: https://doi.org/10.31004/riggs.v4i4.5008

Analisis terhadap studi-studi yang dikaji mengungkapkan sejumlah kesenjangan penelitian yang penting untuk diperhatikan oleh akademisi dan praktisi di bidang sistem informasi akuntansi, keamanan siber, serta penerapan teknologi digital dalam akuntansi dan keuangan. Sebagian besar studi yang ada masih bersifat konseptual atau deskriptif tanpa mengevaluasi secara menyeluruh efektivitas strategi keamanan yang digunakan di lapangan. Hal ini menyulitkan untuk menilai sejauh mana sistem tersebut mampu melindungi data akuntansi secara nyata di tengah meningkatnya ancaman keamanan siber. Belum adanya studi komparatif maupun pendekatan terukur terhadap efektivitas penerapan teknologi seperti cloud computing atau integrasi keamanan berbasis AI dan *blockchain* dalam konteks lokal juga menunjukkan ruang yang besar bagi penelitian ini untuk berkontribusi secara signifikan dalam pengembangan sistem akuntansi digital yang aman dan andal di Indonesia.

Hasil analisis menunjukkan adanya tren yang jelas terhadap peningkatan perhatian akademik dan praktis pada isu keamanan siber, inovasi teknologi informasi, serta regulasi digital di sektor keuangan dan bisnis. Transformasi digital yang terjadi secara masif dalam beberapa tahun terakhir telah mendorong lembaga keuangan, termasuk bank, koperasi, dan perusahaan swasta, untuk mengadopsi sistem informasi berbasis teknologi tinggi (Angelina Wijaya Tan et al., 2024). Penerapan teknologi seperti AI dan *blockchain* menawarkan peningkatan efisiensi dan keamanan, namun juga memperkenalkan tantangan baru.

Salah satu tantangan utama adalah meningkatnya kompleksitas ancaman siber. Studi oleh (Alvina et al., 2024) menjelaskan pentingnya sistem keamanan dalam menghadapi ancaman siber, salah satu yang dapat dilakukan ialah dengan menggunakan teknologi *blockchain*. *Blockchain* memiliki keunggulan dibandingkan langkah-langkah keamanan saat ini karena *blockchain* yang sebenarnya terdesentralisasi dan tidak memerlukan otoritas atau kepercayaan dari masing-masing anggota grup atau jaringan. Di sisi lain, pemerintah juga aktif merespons dinamika ini dengan kerangka hukum yang lebih kuat, salah satunya yaitu Otoritas Jasa Keuangan (OJK) yang mengeluarkan Peraturan OJK No.13/POJK.02/2018 tentang inovasi keuangan digital yang mengharuskan perusahaan *fintech* menjalani proses *regulatory sandbox*. Peraturan ini menekankan inovasi keuangan yang bertanggung jawab, keamanan sistem, tata kelola yang baik, perlindungan pelanggan, dan pencegahan pencucian uang (Putri, 2024). Namun demikian, berbagai tantangan masih menghambat optimalisasi sistem keamanan dan efektivitas teknologi digital yang diterapkan. Kepatuhan terhadap regulasi yang berlaku masih perlu ditindak lanjuti untuk keberhasilan penerapan dari regulasi yang tersedia (Firdaus, 2024).

Di balik tantangan tersebut, terdapat peluang besar yang bisa dimanfaatkan untuk memperkuat sektor ini. Pengembangan sistem informasi berbasis kecerdasan buatan (AI), *blockchain*, dan big data membuka jalan bagi peningkatan efisiensi sekaligus keamanan sistem. Pelatihan keamanan siber dan edukasi publik juga menjadi upaya yang krusial untuk meningkatkan kesadaran dan kemampuan adaptif Masyarakat. Kolaborasi antara sektor hukum, teknologi, dan dunia usaha dapat menciptakan ekosistem digital yang lebih tangguh dan responsif terhadap ancaman siber (Faizal et al., 2023). Dengan sinergi yang baik, peluang untuk mewujudkan sistem informasi yang aman, andal, dan berbasis regulasi yang kuat sangat terbuka lebar.

4. Kesimpulan

Transformasi digital dalam sistem akuntansi telah membawa perubahan signifikan dalam pengelolaan keuangan, khususnya dengan adopsi teknologi seperti *cloud computing*, *artificial intelligence* (AI), *big data*, dan *blockchain.* Studi ini melalui pendekatan Systematic Literature Review (SLR) terhadap 25 artikel jurnal yang dipilih dari rentang waktu 2020–2025, berhasil mengidentifikasi empat kategori utama risiko dan isu yang berkaitan dengan keamanan siber dalam sistem akuntansi digital, yakni: pemanfaatan teknologi *blockchain* dan AI, perlindungan data dan privasi, peran regulasi pemerintah, serta ancaman dan strategi mitigasi terhadap *cybercrime.* Kontribusi utama dari penelitian ini adalah memberikan pemetaan komprehensif atas literatur terkini di Indonesia yang berkaitan dengan keamanan siber dalam konteks sistem akuntansi digital. Temuan ini memperkaya wawasan ilmiah terkait integrasi teknologi digital dan pentingnya manajemen risiko dalam sistem informasi akuntansi. Selain itu, kajian ini juga mengisi kesenjangan riset yang selama ini belum banyak mengulas efektivitas strategi keamanan yang telah diterapkan secara nyata di lapangan. Dari sisi implementasi praktis, hasil kajian ini memberikan pemahaman mendalam bagi pelaku industri, khususnya lembaga keuangan mengenai pentingnya membangun sistem keamanan siber yang andal dan berkelanjutan. Pemanfaatan teknologi harus diiringi oleh kesadaran terhadap risiko serta strategi mitigasi yang tepat, termasuk perlunya regulasi yang kuat, tata kelola digital yang baik, dan edukasi publik untuk meningkatkan literasi keamanan siber. Namun demikian, studi ini memiliki keterbatasan pada ruang lingkup literatur yang hanya mengacu pada artikel berbahasa Indonesia dan bersumber dari satu *database* (Google Scholar). Selain itu, sebagian besar studi yang dianalisis bersifat konseptual atau deskriptif, belum banyak yang melakukan evaluasi kuantitatif atau uji implementasi teknologi secara mendalam.

DOI: https://doi.org/10.31004/riggs.v4i4.5008

Untuk penelitian di masa depan, disarankan agar dilakukan studi komparatif dan empiris guna mengukur efektivitas penerapan teknologi keamanan digital, khususnya AI dan *blockchain*, dalam konteks sistem akuntansi di berbagai jenis organisasi. Selain itu, integrasi pendekatan interdisipliner antara teknologi, hukum, dan manajemen risiko akan memperkuat kontribusi akademik dan relevansi praktis dari riset-riset selanjutnya.

Referensi

1. Afdilah, S., Agustina, N. S., Hani, I., & Gunawan, I. (2024). Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna. *Journal Software, Hardware and Information Technology*, *4*(2), 47–62. https://doi.org/10.24252/shift.v4i2.142
2. Alvina, Y., Sridayanti, W., & Azzahra, N. (2024). Analisis Teknologi Blockchain Pada Cybersecurity Di Bidang Akuntansi: Sistematik Literatur Review. *Jurnal Riset Akuntansi*, *16*(1), 42–57.
3. Angelina Wijaya Tan, Nathalie Elshaday Betrix Ambouw, & Irda Agustin Kustiwi. (2024). Digitalisasi Ekonomi SIA: Transformasi Sistem Informasi Akuntansi Dalam Meningkatkan Efisiensi Dan Inovasi Bisnis. *Jurnal Mutiara Ilmu Akuntansi*, *2*(2), 332–341. https://doi.org/10.55606/jumia.v2i2.2636
4. Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. *JATI:Jurnal Akuntansi Dan Teknologi Informasi*, *17*(2), 221–237.
5. Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan . *HUMANITIS: Jurnal Humaniora, Sosial Dan Bisnis*, *2*(7), 692–700.
6. Edy Susanto, DenyaSaputri, Devan Adika Prasetya, Ian Arbatona, Joshua Christian Marpaung5, & Syuhada Hikmatyar Rahadian. (2023). Pengamanan Objek Vital, Keamanan File, Dan Keamanan Cyber Pada Pt Pos Indonesia. *Jurnal Mutiara Ilmu Akuntansi*, *1*(3), 163–174. https://doi.org/10.55606/jumia.v1i3.1516
7. Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022
8. Fajri, A. M., & Violita, E. S. (2023). Analisis Manajemen Risiko Bank Syariah Dalam Melakukan Transformasi Digital (Studi Kasus Pada Bank AS). *Owner*, *7*(2), 1249–1258. https://doi.org/10.33395/owner.v7i2.1373
9. Faliha, D. W. E. S. E. F. N. A. N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 33–42.
10. Firdaus, R. R. (2024). Pengaruh Akuntansi Syariah Sebagai Instrumen Pengendalian Risiko Pada Perbankan Syariah Dalam Menghadapi Tantangan Di Era Digital. *JICN: Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(6), 9494–9498.
11. Harahap, A. M. (2025). Analisis Risiko Dalam Digitalisasi Perbankan Syariah: Tantangan Dan Solusi. *Jurnal Masharif Al-Syariah*, *10*(1), 687–705.
12. Jati, Y. H. A. F. A. D. F. A. A. N. A. S. M. D. (2024). Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital. *Jurnal Kewirausahaan Dan Multi Talenta*, *2*(2), 148–161.
13. Jayanti, W. W. N. S. O. F. (2024). Peran Akuntan Dalam Era Digital: Transformasi Profesi Dan Keterampilan Baru Dalam Menghadapi Teknologi Dan Tuntutan Pasar. *Studia Economica : Jurnal Ekonomi Islam*, *10*(2), 140–149.
14. Novida, D. R. (2025). Evolusi Sistem Informasi Akuntansi dalam Era Digital: Tinjauan Literatur tentang Tren, Tantangan, dan Peluang. *Jurnal Minfo Polgan*, *14*(1), 77–85.
15. Nugroho, A. N. W. (2025). Analisis Kebijakan Otoritas Jasa Keuangan dalam Upaya Menanggulangi Cyber Crime di Sektor Perbankan Afiah. *Recht Studiosum Law Review*, *02*(02), 84–93. https://talenta.usu.ac.id/rslr
16. Nugroho, M. A., Septininditya, A. Y., & Nugraha, R. A. Z. (2024). Urgensi Manajemen Keamanan dan Pengendalian Sistem Informasi bagi UMKM di Indonesia. *Indo-Fintech Intellectuals: Journal of Economics and Business*, *4*(3), 734–744. https://doi.org/10.54373/ifijeb.v4i3.1373
17. Nurlaila, H. S. K. O. A. A. M. (2024). *Implementasi Blockchain Dengan Meningkatkan Transparasi Dan Keamanan Laporan Keuangan Global Dalam Akuntansi Internasional Herla*. *18*(2), 228–239.
18. Okinaldi, J., & Aziza, N. (2024). Implementasi Teknologi Audit Dalam Era Digital. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, *8*(2), 146–159. https://doi.org/10.31955/mea.v8i2.4016
19. Putra, A. N. M., Rahma, F., & Wahyuni, E. G. (2024). Kajian Literatur: Kesadaran Keamanan Siber pada Pengguna E-Wallet. *SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, Dan Teknik Informatika*, 404–411. https://ejournal.itats.ac.id/snestik/article/view/5881%0Ahttps://ejournal.itats.ac.id/snestik/article/download/5881/3946
20. Putri, O. F. Z. Q. M. H. L. M. H. (2024). Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital. *GEMILANG: Jurnal Manajemen Dan Akuntansi*, *4*(3), 99–114. https://doi.org/10.56910/gemilang.v4i3.1573
21. Rahman Najwa, F. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dan Hukum*, *2*(1), 8–16. https://doi.org/10.32520/albahts.v2i1.3044
22. Salsabila, D. P., & Rahman, A. (2023). Pengaruh Teknologi Digital Terhadap Bidang Akuntansi Pada Perusahaan Swasta. *Konferensi Nasional*, 209–214.
23. Septian, A., Alfiansyah, T., Abdulla, A. D., Sutiawan, H., Ega, D. A., Fauzi, Saputra, D. H., & Saepudin, T. H. (2024). Analisis Tingkat Keamanan Data Pada Salah Satu Kantor Perpajakan Di Bekasi Yang Rentan Terhadap Serangan Cyber Dalam Sistem Keuangan. *Jurnal Humaniora, Sosial Dan Bisnis*, *2*(7), 711–718.
24. Simanjuntak, H. E., Purba, H. C., Trimanda, J., Ginting, B., Aruan, A., Joy, R., Panjaitan, N., & Darma, J. (2025). Keamanan Sistem Informasi Akuntansi Dalam Era Digital: Konsep Dan Implementasi. *Indo-MathEdu Intellectuals Journal*, *6*(2), 2695–2705.
25. Susanto, A. (2025). Manajemen Risiko dalam E-Bisnis : Pendekatan untuk Keamanan Data dan Mitigasi Risiko Siber. *Journal of Economics, Business, Management, Accounting and Social Sciences (JEBMASS)*, *3*(1), 41–45.

DOI: https://doi.org/10.31004/riggs.v4i4.5008