Land Journal
e –ISSN: 2715-9590 | p–ISSN: 2716-263X
Volume 7 Nomor 1, Januari 2026
https://ejurnal.ulbi.ac.id/index.php/jurnalland

STRATEGI CYBERSECURITY UNTUK PERLINDUNGAN DATA AKUNTANSI: KAJIAN LITERATUR SISTEMATIS 2021-2025

Iman Suyakin Daeli[1], Ririn Setia Ningsih[2], Karina Lolo Limbong[3], Jufri Darma[4]
Universitas Negeri Medan[1,2,3,4]
imandaeli.7223142032@mhs.unimed.ac.id, ririinsetiaa@gmail.com, lololimbongg@gmail.com, jufridarma@unimed.ac.id

ABSTRACT

The rapid digitalization of business processes has positioned accounting data as a strategic asset that is highly vulnerable to cyber threats such as ransomware, malware, and social engineering. Protecting this data is crucial not only to ensure operational continuity but also to maintain public trust and organizational accountability. This study aims to provide an in-depth review of relevant cybersecurity strategies for safeguarding accounting data, focusing on recent practices and technologies from 2021 to 2025. The research employed a Systematic Literature Review (SLR) approach by examining academic databases such as Scopus, Google Scholar, and SINTA, followed by content analysis and synthesized through a narrative synthesis method. The findings reveal that effective protection strategies emphasize a holistic and multilayered approach, including data encryption, role-based access control, multi-factor authentication, real-time system monitoring, and security audits. Beyond technical measures, employee training and awareness play a critical role in minimizing internal risks. In conclusion, the integration of advanced technologies with human factors and organizational policies significantly enhances the security of accounting data, ensuring data integrity while strengthening business resilience and sustainability in the digital era.

Keywords: *Cybersecurity, Accounting Data, Data Protection, Cyber Threats, Information Security*

ABSTRAK

Perkembangan digitalisasi dalam dunia bisnis menjadikan data akuntansi sebagai aset strategis yang sangat rentan terhadap ancaman siber, mulai dari ransomware, malware, hingga social engineering. Perlindungan terhadap data ini menjadi krusial, tidak hanya untuk menjaga keberlangsungan operasional, tetapi juga untuk mempertahankan kepercayaan publik dan akuntabilitas organisasi. Penelitian ini bertujuan untuk mengkaji secara mendalam strategi cybersecurity yang relevan dalam melindungi data akuntansi, dengan fokus pada praktik dan teknologi terkini dalam periode 2021–2025. Metode yang digunakan adalah Systematic Literature Review (SLR) dengan menelusuri basis data akademik seperti Scopus, Google Scholar, dan SINTA, kemudian dianalisis menggunakan content analysis dan disintesis melalui pendekatan narrative synthesis. Hasil kajian menunjukkan bahwa strategi perlindungan data akuntansi yang efektif menekankan pendekatan holistik dan berlapis, meliputi penerapan enkripsi, kontrol akses berbasis peran,

autentikasi multi-faktor, pemantauan sistem real-time, serta audit keamanan. Selain aspek teknis, pelatihan dan peningkatan kesadaran karyawan terbukti berperan penting dalam meminimalkan risiko internal. Kesimpulannya, integrasi teknologi mutakhir dengan penguatan faktor manusia dan kebijakan organisasi mampu meningkatkan keamanan data akuntansi secara signifikan, mendukung integritas informasi, serta memperkuat resiliensi dan keberlanjutan bisnis di era digital.

Kata Kunci: Keamanan Siber, Data Akuntansi, Perlindungan Data, Ancaman Siber, Keamanan Informasi

PENDAHULUAN

Dalam dunia bisnis yang semakin terdigitalisasi, data akuntansi telah menjadi komponen vital yang tidak hanya mendukung pengambilan keputusan strategis, tetapi juga menjadi aset yang sangat rentan terhadap berbagai ancaman siber. Keamanan data, khususnya data akuntansi, kini menjadi isu utama bagi setiap organisasi, mengingat betapa krusialnya informasi keuangan dalam menjaga keberlanjutan dan transparansi operasional perusahaan. Ancaman terhadap data akuntansi yang semakin kompleks mulai dari serangan peretasan, malware, hingga pencurian data oleh pihak yang tidak bertanggung jawab semakin meningkat seiring dengan semakin canggihnya teknologi. Jika data akuntansi tidak terlindungi dengan baik, maka kerugian yang ditimbulkan bukan hanya bersifat finansial, tetapi juga dapat merusak reputasi perusahaan, merusak kepercayaan publik, dan bahkan menimbulkan permasalahan hukum terkait akuntabilitas keuangan.

Laporan IBM Cost of a Data Breach 2024 mencatat bahwa rata-rata kerugian global akibat pelanggaran data mencapai USD 4,88 juta, dengan sektor keuangan menjadi yang paling terdampak, yakni mencapai USD 6,08 juta per insiden. Fakta ini menunjukkan betapa besar risiko ekonomi yang dihadapi oleh organisasi ketika sistem akuntansinya tidak memiliki perlindungan siber yang memadai. Dengan meningkatnya frekuensi dan kompleksitas serangan siber, sektor akuntansi dan keuangan kini menjadi salah satu target utama karena menyimpan informasi finansial sensitif dan strategis. Oleh karena itu, urgensi untuk mengimplementasikan strategi cybersecurity yang kuat tidak dapat diabaikan. Ashraf & Puccia (2023) menjelaskan bahwa permintaan klien terhadap auditor yang memiliki keahlian cybersecurity meningkat karena mereka membantu memperbaiki proteksi keamanan klien, mengurangi risiko, dan menjadi sinyal bahwa organisasi serius terhadap keamanan *"clients value auditors with cybersecurity expertise"*

Selain itu, data akuntansi yang bersifat sensitif juga menghadapi tantangan unik terkait pengelolaannya. Data ini bukan hanya menjadi bagian dari laporan internal organisasi, namun juga harus dipertanggungjawabkan kepada berbagai pihak eksternal seperti regulator dan pemangku kepentingan lainnya. Oleh karena itu, menjaga integritas data akuntansi menjadi prioritas utama, yang tidak hanya melibatkan perlindungan terhadap data itu sendiri, tetapi juga terhadap sistem yang mengolahnya. Namun, meskipun ancaman terhadap data akuntansi semakin besar, banyak organisasi yang masih menghadapi kesulitan dalam mengimplementasikan strategi cybersecurity yang efektif. Terbatasnya anggaran untuk investasi dalam sistem keamanan canggih, serta kurangnya kesadaran di kalangan karyawan terkait ancaman siber, menjadi beberapa tantangan utama yang perlu diatasi.

Amos Nyombi et al. (2024) menekankan pentingnya protokol yang ditingkatkan dalam

cybersecurity akuntansi pajak untuk melindungi data wajib pajak. Ditemukan bahwa meskipun enkripsi, MFA, firewall, IDS, audit keamanan, dan pelatihan efektif, implementasi yang tidak konsisten masih menjadi tantangan besar. Keamanan data akuntansi ini memerlukan pendekatan yang lebih komprehensif, yang mengintegrasikan berbagai strategi cybersecurity secara efektif. Berbagai metode telah diusulkan dan diterapkan, mulai dari penggunaan enkripsi data, kontrol akses yang ketat, hingga pemantauan sistem secara real-time untuk mendeteksi ancaman secara dini. Meskipun demikian, implementasi strategi-strategi ini sering kali terbentur pada tantangan dalam hal sumber daya, baik dalam bentuk teknologi maupun pengelolaan manusia. Oleh karena itu, penting bagi setiap organisasi untuk terus memperbarui kebijakan dan prosedur mereka, seiring dengan perkembangan ancaman yang ada. Sementara itu, akuntan dan firma besar telah mengintegrasikan teknologi mutakhir seperti AI, blockchain, dan enkripsi dalam strategi cybersecurity mereka (Hasan et al. 2024). Pendekatan multilayered security terbukti meningkatkan proteksi data, integritas, dan deteksi penipuan — meski tantangan seperti biaya tinggi dan evolusi cepat ancaman tetap ada. Penelitian ini bertujuan untuk melakukan kajian yang mendalam mengenai berbagai strategi cybersecurity yang dapat diimplementasikan untuk melindungi data akuntansi, dengan fokus pada praktik-praktik terbaru dan penerapan teknologi dalam konteks perlindungan data yang relevan untuk periode 2021 hingga 2025. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi dan mengevaluasi seberapa efektif berbagai strategi cybersecurity dalam menangani ancaman terhadap data akuntansi di era digital saat ini. Melalui pendekatan ini, penelitian diharapkan dapat memberikan pemahaman yang lebih komprehensif mengenai tantangan yang dihadapi oleh organisasi dalam mengelola dan melindungi data akuntansi serta mengoptimalkan strategi yang ada.

Dalam rangka mencapai tujuan tersebut, penelitian ini akan menjawab beberapa pertanyaan penting yang menjadi fokus kajian, yaitu: (1) Apa saja ancaman siber utama yang sering dihadapi oleh sistem akuntansi digital saat ini? (2) Apa strategi cybersecurity yang paling efektif dan relevan dalam melindungi data akuntansi? (3) Bagaimana implementasi dari strategi-strategi tersebut dapat memberikan dampak positif dalam meningkatkan tingkat keamanan data akuntansi di organisasi? Dengan menjawab pertanyaan-pertanyaan ini, diharapkan dapat diperoleh gambaran yang lebih jelas mengenai langkah-langkah yang perlu diambil oleh organisasi untuk mengatasi ancaman siber yang ada dan menjaga integritas data akuntansi mereka.

Land Journal
e –ISSN: 2715-9590 | p–ISSN: 2716-263X
Volume 7 Nomor 1, Januari 2026
https://ejurnal.ulbi.ac.id/index.php/jurnalland

STUDI LITERATUR

1. Cybersecurity dalam Perlindungan Data Akuntansi

Cybersecurity memiliki peran yang sangat penting dalam menjaga keamanan data, terutama pada data akuntansi, yang menyimpan informasi sensitif terkait dengan transaksi dan keuangan perusahaan. Hasan et al. (2024) mendefinisikan cybersecurity sebagai praktik, teknologi, dan kebijakan yang diterapkan untuk melindungi sistem komputer, jaringan, dan data dari akses yang tidak sah, manipulasi, atau pencurian. Pendekatan ini menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data, sehingga informasi sensitif organisasi tetap aman. Dalam konteks data akuntansi, cybersecurity memiliki peran yang sangat penting karena data tersebut menyimpan informasi finansial yang kritikal. Tanpa perlindungan yang baik, data akuntansi dapat terpapar ancaman seperti ransomware dan phishing, yang dapat menyebabkan kerugian finansial dan gangguan operasional. Hasan et al. (2024) menegaskan bahwa serangan siber terhadap sistem informasi akuntansi dapat mengakibatkan hilangnya akses ke data, kerusakan informasi, dan biaya pemulihan yang tinggi. Ransomware, yang mengenkripsi data penting dan meminta tebusan untuk mengembalikannya, telah menjadi salah satu ancaman utama. Oleh karena itu, perlindungan data akuntansi mengharuskan perusahaan untuk mengadopsi teknologi seperti enkripsi data, pemantauan sistem real-time, dan pengelolaan akses berbasis peran (RBAC) yang efektif.

Selain itu, Morshed & Khrais (2025) juga menggarisbawahi pentingnya pelatihan berkelanjutan bagi karyawan. Tanpa kesadaran yang memadai terhadap ancaman siber, potensi kebocoran data akuntansi sangat besar. Oleh karena itu, pengintegrasian kebijakan keamanan yang baik dengan teknologi yang tepat dan keterlibatan aktif dari seluruh anggota organisasi adalah langkah penting dalam menjaga data akuntansi.

2. Data Akuntansi

Keamanan data dalam konteks data akuntansi tidak hanya berkaitan dengan pengamanan fisik, tetapi juga meliputi perlindungan terhadap data yang diproses dan disimpan secara digital. Data akuntansi mencakup informasi yang digunakan dalam pencatatan, pengolahan, dan pelaporan transaksi keuangan perusahaan, termasuk laporan laba rugi, neraca, dan arus kas. Nurwanah (2024) menyatakan bahwa data akuntansi yang aman merupakan fondasi bagi kredibilitas laporan keuangan dan pengambilan keputusan strategis. Setiap kebocoran atau manipulasi data berpotensi merusak integritas organisasi serta menurunkan kepercayaan pemangku kepentingan. Dalam praktiknya, keamanan data akuntansi sangat penting karena kebocoran atau manipulasi dapat merusak reputasi dan kredibilitas perusahaan. Mauliza et al. (2022) menekankan bahwa data akuntansi yang aman meningkatkan keyakinan publik terhadap akurasi laporan keuangan. Temuan ini menegaskan pentingnya langkah- langkah perlindungan yang memadai untuk menjaga integritas data akuntansi dalam sistem digital.

Untuk itu, perusahaan perlu menggunakan enkripsi data dan kontrol akses berbasis peran (RBAC) untuk membatasi siapa yang memiliki akses ke data sensitif tersebut.

Pengelolaan keamanan data ini juga melibatkan sistem pemantauan untuk mendeteksi aktivitas mencurigakan yang bisa menunjukkan adanya potensi ancaman atau pelanggaran.

3. Perlindungan Data

Untuk memastikan data akuntansi tetap aman dari ancaman siber, perlu diterapkan langkah- langkah perlindungan yang melibatkan pengelolaan data yang cermat dan penggunaan teknologi yang tepat. Nurwanah (2024) sebagai kombinasi langkah teknis, administratif, dan kebijakan untuk menjaga agar data akuntansi tetap aman dari ancaman internal maupun eksternal. Fokusnya adalah pada kerahasiaan, integritas, dan ketersediaan data yang kritis bagi organisasi. Untuk itu, organisasi perlu menerapkan enkripsi, kontrol akses berbasis peran (RBAC), audit keamanan rutin, dan pemantauan sistem real-time. Enkripsi merupakan salah satu langkah paling efektif untuk melindungi informasi yang sensitif dalam data akuntansi. Enkripsi membuat data tidak dapat dibaca oleh pihak yang tidak berwenang, meskipun data tersebut jatuh ke tangan yang salah.

Nurwanah (2024) mengungkapkan bahwa tantangan utama dalam mengamankan Sistem Informasi Akuntansi (SIA) adalah integrasi faktor teknologi, manusia, dan organisasi. Oleh karena itu, perusahaan perlu mengadopsi pendekatan holistik yang mencakup pelatihan bagi karyawan, penerapan teknologi yang tepat, dan kebijakan organisasi yang mendukung keamanan data. Selain itu, penting bagi perusahaan untuk melakukan pemantauan sistem secara berkelanjutan untuk mendeteksi ancaman dan merespons dengan cepat. Dengan sistem deteksi intrusi (IDS) dan penggunaan audit keamanan secara rutin, perusahaan dapat mengidentifikasi titik-titik lemah dalam sistem dan melakukan perbaikan dengan segera.

4. Ancaman Siber terhadap Data Akuntansi

Ancaman siber terhadap data akuntansi mencakup berbagai bentuk serangan yang dapat merusak atau mengakses informasi sensitif tanpa izin. Surya Guritno et al. (2024) menjelaskan ancaman siber adalah segala bentuk serangan atau upaya yang dilakukan pihak internal maupun eksternal untuk mendapatkan akses tidak sah, merusak, atau mencuri data. Dalam konteks data akuntansi, ancaman siber mencakup ransomware, phishing, malware, dan social engineering. Ransomware dapat mengenkripsi data penting sehingga perusahaan tidak dapat mengaksesnya, sedangkan phishing menipu karyawan untuk memperoleh kredensial login atau informasi sensitif. Slapničar et al. (2022) mengatakan audit keamanan siber dapat membantu organisasi dalam menilai efektivitas langkah- langkah keamanan yang diterapkan dan mengidentifikasi area yang perlu diperbaiki. Audit ini mencakup evaluasi terhadap kebijakan dan prosedur keamanan, serta pengujian terhadap sistem untuk mengidentifikasi potensi kerentanannya. Dengan melakukan audit secara rutin, organisasi dapat memastikan bahwa sistem akuntansi mereka tetap terlindungi dari ancaman yang berkembang.

Salah satu ancaman paling serius terhadap data akuntansi adalah ransomware, terutama varian double-extortion di mana pelaku tidak hanya mengenkripsi data tetapi juga mengekstraksi informasi dan mengancam menyebarkannya apabila tebusan tidak dibayar. Meurs et al. (2024) mengungkap bahwa strategi ini meningkatkan daya tawar penyerang

karena korban menghadapi risiko kehilangan kerahasiaan data sensitif seperti catatan transaksi, data karyawan, dan informasi pelanggan. Ancaman semacam ini berimplikasi langsung pada perlakuan akuntansi, termasuk pencatatan biaya pemulihan, penilaian kerugian, serta kemungkinan pengungkapan dalam laporan keuangan.

Serangan Distributed Denial of Service (DDoS) juga menjadi ancaman yang signifikan terhadap ketersediaan data akuntansi. Serangan ini tidak selalu bertujuan mencuri data, tetapi melumpuhkan sistem informasi akuntansi dengan membanjiri server menggunakan lalu lintas palsu, sehingga proses pencatatan transaksi, konsolidasi laporan, atau akses auditor eksternal terganggu. Songa & Karri (2024) mengusulkan kerangka kerja berbasis Software-Defined Networking (SDN) untuk mendeteksi dini serangan Distributed Denial of Service (DDoS) di lingkungan komputasi awan. Mereka menekankan bahwa sistem berbasis cloud, termasuk aplikasi akuntansi modern, sangat rentan terhadap serangan DDoS karena bergantung pada ketersediaan jaringan untuk menjalankan pencatatan, konsolidasi, dan pelaporan data keuangan secara real-time. Dengan pendekatan integratif SDN, serangan dapat diidentifikasi lebih cepat melalui analisis lalu lintas dan pemisahan jalur komunikasi yang mencurigakan, sehingga mengurangi dampak gangguan layanan. Dampak bagi organisasi sangat nyata, yakni penundaan proses akuntansi, keterlambatan pelaporan keuangan, serta biaya tambahan untuk pemulihan dan peningkatan kapasitas infrastruktur.

Secara keseluruhan, literatur menunjukkan bahwa ancaman siber terhadap data akuntansi bersifat beragam, mulai dari ransomware dengan model double-extortion, serangan phishing dan social engineering, hingga serangan DDoS yang melumpuhkan sistem. Ancaman-ancaman ini tidak hanya mengganggu kerahasiaan, integritas, dan ketersediaan data, tetapi juga menimbulkan implikasi langsung bagi perlakuan akuntansi, pengungkapan laporan keuangan, serta reputasi organisasi. Oleh karena itu, penerapan audit keamanan siber dan penguatan pengendalian internal menjadi langkah penting untuk menjaga keamanan data akuntansi di tengah meningkatnya risiko serangan digital.

5. Keamanan Informasi

Keamanan sistem informasi akuntansi menghadapi tantangan signifikan, termasuk kerentanan teknis, ancaman berupa serangan siber, serta kelemahan dalam kebijakan dan budaya organisasi. Nurwanah (2024) dalam Cybersecurity in Accounting Information Systems: Challenges and Solutions menegaskan bahwa pendekatan holistik sangat diperlukan, yang mencakup integrasi teknologi seperti enkripsi, autentikasi multi-faktor (MFA), dan kecerdasan buatan (AI) untuk deteksi ancaman secara real time, serta penguatan faktor manusia melalui budaya keamanan dan kebijakan yang jelas. Selain itu, Juanda (2025) dalam A Comprehensive Literature Review on the Impact of Cyberattacks on Accounting Practices and Security Measures menunjukkan bahwa kombinasi teknologi (AI, blockchain, enkripsi) dan pelatihan karyawan serta tata kelola regulasi merupakan mitigasi kritikal terhadap dampak serangan siber terhadap sistem akuntansi.

Blockchain muncul sebagai salah satu teknologi yang menjanjikan dalam memperkuat keamanan dan integritas data akuntansi. Putritama et al. (2024) dalam The

Impact of Blockchain Technology on Accounting: A Literature Review menyimpulkan bahwa blockchain meningkatkan transparansi, efisiensi, dan keamanan dalam praktik akuntansi, sekaligus menyoroti tantangan seperti interoperabilitas dan regulasi. Almadadha (2024) dalam jurnal Blockchains menambahkan bahwa blockchain tidak hanya meningkatkan keamanan tetapi juga mendukung pelaporan ESG dan audit berbasis transparansi tinggi.

Dari beberapa kajian tersebut menunjukkan bahwa keamanan sistem informasi akuntansi membutuhkan pendekatan menyeluruh yang tidak hanya berfokus pada aspek teknis, tetapi juga memperhatikan faktor manusia, kebijakan organisasi, serta kepatuhan regulasi. Integrasi teknologi seperti enkripsi, autentikasi multi-faktor, dan kecerdasan buatan dapat memperkuat deteksi dan pencegahan ancaman siber, sementara pelatihan karyawan serta penerapan tata kelola yang baik menjadi elemen penting dalam meminimalkan risiko dari sisi pengguna. Di sisi lain, blockchain hadir sebagai teknologi pendukung yang mampu meningkatkan transparansi, integritas, dan akuntabilitas data akuntansi, meskipun masih menghadapi tantangan terkait interoperabilitas dan regulasi. Dengan demikian, kombinasi strategi berbasis teknologi mutakhir dan penguatan faktor non-teknis diyakini mampu memberikan perlindungan yang lebih efektif terhadap data akuntansi di tengah ancaman siber yang semakin kompleks

6. Penelitian Terdahulu

Penelitian	Hasil Pembahasan
Hossain, M. Z. (2024)	Emphasizes the importance of integrating advanced technologies like AI and blockchain in accounting practices to enhance data integrity and client trust. The study also highlights the need for continuous training and interdisciplinary knowledge in facing cyber threats (HOSSAIN et al. 2024b)
Morshed, A. (2025)	Identifies key challenges in digital accounting systems, including ransomware attacks, data breaches, and insider threats. The research stresses the importance of aligning cybersecurity strategies with international compliance standards like GDPR and ISO 27001 (Morshed & Khrais, 2025)
Schreyer, M. (2022)	Proposes a Federated Learning framework to train Deep Learning models on accounting data from various clients while considering privacy and regulatory compliance. This study shows that auditors can leverage DL models without violating client data confidentiality (Schreyer et al, 2022).

Jin, X. (2025)	Examines the impact of cybersecurity regulation on corporate digital transformation, focusing on the implementation of China's Cyber Security Law. The research finds that strict regulation can encourage companies to improve their cybersecurity practices (Jin et al. 2025).
Chotia, V. (2025)	Highlights the importance of cybersecurity in supporting digital transformation and sustainable business performance. This research suggests that companies should adopt an agile cybersecurity approach to ensure data integrity and business continuity (Chotia et al. 2025).
Dewi, A. K., et al. (2025)	Presents effective internal control strategies for maintaining the security of Accounting Information Systems in Indonesia, with a focus on protecting financial data. The study highlights the importance of internal audits and periodic evaluations in ensuring system security (Dewi et al. 2025).

METODE

Kajian ini menggunakan pendekatan Systematic Literature Review (SLR) sebagaimana dijelaskan oleh Boell & Cecez-Kecmanovic (2015) dan Snyder (2019). Proses penelitian dilakukan melalui empat tahap: (1) identifikasi literatur dari Scopus, Web of Science, Google Scholar, dan SINTA; (2) penyaringan berdasarkan relevansi judul dan abstrak; (3) analisis isi (content analysis) terhadap artikel yang lolos seleksi; dan (4) sintesis naratif (narrative synthesis) untuk merangkum hasil temuan.

Langkah pertama dalam penelitian ini adalah merumuskan pertanyaan penelitian, yang menjadi dasar seleksi literatur. Pertanyaan utama yang akan dijawab dalam kajian ini adalah: (1) Apa saja ancaman siber yang dihadapi oleh sistem akuntansi digital? (2) Apa strategi cybersecurity yang paling efektif untuk melindungi data akuntansi? dan (3) Bagaimana penerapan strategi-strategi tersebut dapat meningkatkan keamanan data akuntansi di organisasi? Sebagaimana dijelaskan oleh Jesson et al. (2011), pemilihan pertanyaan penelitian yang tepat sangat penting dalam SLR, karena hal ini memberikan arah yang jelas dalam pencarian literatur dan pembatasan studi.

Proses pencarian literatur dilakukan melalui basis data akademik seperti Scopus, Google Scholar, Web of Science, dan portal jurnal nasional yang terindeks SINTA. Kata kunci yang digunakan dalam pencarian termasuk: Ancaman Siber; Data Akuntansi; Cybersecurity for Accounting Data; Data Protection in Accounting Systems; Digital Accounting and Cybersecurity; Data Integrity in Financial Systems; Cyber Threats in Accounting. Artikel yang digunakan dibatasi pada tahun 2021–2025 untuk memastikan kebaruan (recency) dan relevansi. Kriteria inklusi mencakup: artikel ilmiah berbahasa Inggris atau Indonesia, topik terkait cybersecurity dan data akuntansi, tersedia dalam teks lengkap, serta dipublikasikan di jurnal terindeks. Kriteria eksklusi meliputi: duplikasi artikel, studi non-akademik, serta artikel konseptual tanpa data pendukung.

Setelah proses seleksi, data disusun menggunakan pendekatan PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) untuk menggambarkan alur penyaringan literatur secara sistematis. Tahap pencarian awal menemukan 96 artikel; setelah penghapusan duplikasi tersisa 75 artikel; 45 artikel memenuhi kriteria relevansi dan kelengkapan; dan akhirnya 30 artikel dianalisis secara mendalam. Penjelasan ini menegaskan transparansi proses seleksi dan konsistensi metodologis kajian literatur.

HASIL DAN PEMBAHASAN

Kajian ini menunjukkan bahwa data akuntansi digital menghadapi ancaman siber yang semakin kompleks, baik dari sumber eksternal maupun internal organisasi. Ancaman eksternal termasuk ransomware, malware, dan phishing, sementara ancaman internal muncul akibat kesalahan karyawan, kelalaian, atau penyalahgunaan akses. Ransomware, misalnya, dapat mengenkripsi data penting sehingga akses ke sistem menjadi terhenti dan operasional organisasi terganggu. Phishing dan social engineering memanfaatkan kelemahan manusia untuk memperoleh kredensial dan informasi sensitif, yang menunjukkan bahwa risiko terhadap data akuntansi bersifat multidimensional. Fenomena ini menegaskan bahwa perlindungan data tidak hanya terkait aspek teknis, tetapi juga melibatkan pengelolaan perilaku pengguna dan penerapan prosedur internal yang konsisten.

Dari hasil analisis literatur, teridentifikasi lima strategi utama yang efektif diterapkan dalam perlindungan data akuntansi digital, yaitu:

Strategi Utama	Teknologi yang Digunakan	Tujuan Perlindungan
Enkripsi Data	AES-256, SSL/TLS	Menjaga kerahasiaan dan integritas data
Kontrol Akses Berbasis Peran (RBAC)	Role Management Tools	Membatasi hak akses pengguna terhadap data sensitif
Autentikasi Multi-Faktor (MFA)	Biometric, OTP	Mengurangi risiko akses tidak sah
Pemantauan Real-Time & IDS/SIEM	Splunk, Snort, IBM QRadar	Deteksi dini aktivitas mencurigakan
Audit & Pelatihan Keamanan	Internal Audit Tools, Workshop	Meningkatkan kesadaran dan kepatuhan karyawan

Temuan ini menunjukkan bahwa kombinasi teknologi dan pendekatan manusia menciptakan sistem pertahanan berlapis yang efektif. Negara-negara seperti Amerika Serikat, Tiongkok, dan Uni Eropa telah membuktikan bahwa organisasi yang menerapkan pelatihan keamanan reguler dan kepatuhan pada standar ISO 27001 mengalami tingkat kebocoran data hingga 30% lebih rendah dibanding organisasi yang hanya bergantung pada teknologi (Jin et al. 2025).

Selain pendekatan teknis, aspek perilaku dan budaya organisasi memiliki kontribusi penting. Pelatihan keamanan dan audit berkala membentuk kesadaran karyawan terhadap risiko siber, sekaligus memperkuat budaya tanggung jawab terhadap data. Pendekatan holistik ini menghasilkan sistem keamanan yang adaptif, meningkatkan keandalan informasi, serta memperkuat kepercayaan pemangku kepentingan. Dengan demikian, strategi cybersecurity yang efektif tidak hanya melindungi data akuntansi dari serangan eksternal, tetapi juga membangun ketahanan internal organisasi terhadap perubahan ancaman digital yang dinamis.

Kajian ini juga mengungkap bahwa strategi cybersecurity yang terintegrasi memberikan dampak positif yang signifikan terhadap organisasi. Pertama, integritas data akuntansi terjaga sehingga laporan keuangan dapat digunakan sebagai dasar pengambilan keputusan strategis. Kedua, keamanan yang terjamin meningkatkan kepercayaan internal maupun eksternal, termasuk pemangku kepentingan dan regulator, terhadap data dan informasi yang disajikan. Ketiga, integrasi teknologi, prosedur, dan perilaku pengguna memungkinkan organisasi menyesuaikan strategi keamanan dengan ancaman baru yang muncul, sehingga resiliensi operasional dan kontinuitas bisnis dapat dipertahankan. Kajian ini menunjukkan bahwa strategi yang menyatukan ketiga dimensi ini lebih efektif dibandingkan pendekatan yang hanya fokus pada teknologi semata.

Selain itu, penggabungan berbagai lapisan strategi memberikan fleksibilitas dalam

pengelolaan risiko. Penggunaan sistem pemantauan real-time memungkinkan organisasi mengidentifikasi perilaku abnormal dalam sistem akuntansi, sementara audit rutin memastikan bahwa prosedur dan kebijakan diterapkan dengan konsisten. Pelatihan karyawan secara berkala memperkuat kesadaran terhadap potensi ancaman internal, sehingga risiko kebocoran data dapat dikurangi. Temuan Morshed (2025) menegaskan bahwa organisasi yang menerapkan strategi keamanan berlapis dengan keseimbangan antara teknologi dan perilaku pengguna mampu meningkatkan efektivitas perlindungan data akuntansi serta meminimalkan dampak negatif dari serangan siber

Dampak penerapan strategi cybersecurity yang komprehensif ini tidak hanya terbatas pada proteksi data, tetapi juga meningkatkan efisiensi operasional dan akuntabilitas organisasi. Data yang aman memungkinkan pengambilan keputusan yang lebih cepat dan tepat, sedangkan pelaporan yang terjaga integritasnya mendukung kepatuhan terhadap regulasi dan standar akuntansi. Dengan pendekatan berlapis dan adaptif, organisasi dapat merespons ancaman secara proaktif, sehingga proses bisnis tetap berjalan tanpa terganggu. Kajian ini menunjukkan bahwa perlindungan data akuntansi harus dilihat sebagai bagian dari manajemen risiko strategis, bukan sekadar tindakan preventif.

Kajian ini memperkuat argumen bahwa strategi cybersecurity yang efektif untuk perlindungan data akuntansi harus memadukan enkripsi, kontrol akses, pemantauan real-time, audit keamanan, serta pelatihan karyawan. Integrasi elemen-elemen tersebut menciptakan sistem keamanan yang adaptif, mengurangi risiko kebocoran data, dan meningkatkan kepercayaan stakeholder. Dengan pendekatan holistik ini, organisasi tidak hanya menjaga keamanan data, tetapi juga membangun fondasi untuk pengambilan keputusan yang berbasis data akurat, efisiensi operasional yang optimal, dan kontinuitas bisnis yang berkelanjutan.

Secara keseluruhan, kajian ini menegaskan bahwa perlindungan data akuntansi di era digital memerlukan strategi cybersecurity yang komprehensif dan adaptif. Strategi yang menggabungkan teknologi, prosedur, dan perilaku manusia memberikan perlindungan optimal, menjaga integritas informasi, meningkatkan kepercayaan stakeholder, serta mendukung pencapaian tujuan strategis organisasi. Dengan demikian, hasil kajian ini selaras dengan tujuan penelitian, yakni memberikan pemahaman yang mendalam mengenai ancaman siber utama, strategi cybersecurity yang efektif, serta dampak implementasi strategi tersebut terhadap keamanan data akuntansi.

KESIMPULAN

Kajian ini menegaskan bahwa data akuntansi digital menghadapi berbagai ancaman siber, mulai dari ransomware, phishing, malware, hingga risiko internal akibat kesalahan atau kelalaian pengguna. Hal ini menekankan bahwa perlindungan data tidak cukup mengandalkan teknologi saja, tetapi harus dikombinasikan dengan prosedur internal dan budaya organisasi yang mendukung praktik keamanan siber secara menyeluruh.

Strategi cybersecurity yang efektif menuntut sinergi antara teknologi, kebijakan, dan kesadaran manusia. Implementasi enkripsi, kontrol akses berbasis peran, MFA, IDS/SIEM, serta pelatihan keamanan terbukti meningkatkan integritas data dan keandalan laporan akuntansi. Sebagai rekomendasi praktis:

1. Organisasi perlu memperkuat audit keamanan dan memperbarui kebijakan akses secara berkala.
2. Lembaga pendidikan akuntansi perlu memasukkan materi cybersecurity ke dalam

kurikulum digital agar calon profesional memiliki kompetensi keamanan data.

3. Regulator disarankan menyusun standar keamanan akuntansi digital berbasis risiko untuk menjaga akuntabilitas dan kepatuhan terhadap perlindungan data.

Dengan demikian, strategi cybersecurity yang adaptif dan berlapis menjadi fondasi penting bagi organisasi untuk menjaga kepercayaan publik, meningkatkan transparansi, serta menjamin keberlanjutan bisnis di era digital.

REFERENSI

Almadadha, R. (2024). Blockchain Technology in Financial Accounting: Enhancing Transparency, Security, and ESG Reporting. Blockchains, 2(3), 312–333. https://doi.org/10.3390/blockchains2030015

Amos Nyombi, Wycliff Nagalila, Babrah Happy, Mark Sekinobe, & Jimmy Ampe. (2024). Enhancing cybersecurity protocols in tax accounting practices: Strategies for protecting taxpayer information. World Journal of Advanced Research and Reviews, 23(3), 1788–1798. https://doi.org/10.30574/wjarr.2024.23.3.2838

Ashraf, M., & Puccia, J. (2023). Should Accountants Upskill? Evidence from Demand for Auditors with Cybersecurity Expertise. https://doi.org/https://acis.pamplin.vt.edu/content/dam/acis_pamplin_vt_edu/research/2023/Ashr af.pdf

Boell, Sebastian K, & Cecez-Kecmanovic, Dubravka. (2015). On being 'Systematic' in Literature Reviews in IS. Journal of Information Technology, 30(2), 161–173. https://doi.org/10.1057/jit.2014.26

Chotia, V., Khoualdi, K., Broccardo, L., & Yaqub, M. Z. (2025). The role of cyber security and digital transformation in gaining competitive advantage through Strategic Management Accounting. Technology in Society, 81, 102851. https://doi.org/https://doi.org/10.1016/j.techsoc.2025.102851

Dewi, A. K., Sibarani, B. K., Saputra, E., Norazlina, N., Susanti, S., Syafira, Y., & munakalla, Y. (2025). Strategi Efektif Pengendalian Internal dalam Keamanan Sistem Informasi Akuntansi untuk Perlindungan Data Keuangan. Jurnal Ilmiah Raflesia Akuntansi, 11(1), 138–148. https://doi.org/10.53494/jira.v11i1.838

Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024a). Cybersecurity in Accounting: Protecting Financial Data in the Digital Age. European Journal of Applied Science, Engineering and Technology, 2(6), 64–80. https://doi.org/10.59324/ejaset.2024.2(6).06

Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024b). Cybersecurity in Accounting: Protecting Financial Data in the Digital Age. European Journal of Applied Science, Engineering and Technology, 2(6), 64–80. https://doi.org/10.59324/ejaset.2024.2(6).06

IBM Security, & Ponemon Institute. (2025). *Cost of a Data Breach Report 2025: Executive Summary.* IBM Corporation. https://www.ibm.com/downloads/documents/id-id/137a3e32273ed1f5

Jesson, J., Matheson, L., & Lacey, F. M. (2011). Doing Your Literature Review: Traditional and Systematic Techniques. SAGE Publications. https://books.google.co.id/books?id=NAYrLb8qsd4C

Jin, X., Cui, H., Liu, F., Hu, Z., & Cai, Y. (2025). Does cybersecurity regulation promote digital transformation? Evidence from the Cyber Security Law in China. Finance Research Letters, 76, 107041. https://doi.org/https://doi.org/10.1016/j.frl.2025.107041

Juanda, J. (2025). A Comprehensive Literature Review on the Impact of Cyberattacks on Accounting Practices and Security Measures. Fairness, 01(1), 64–80. https://doi.org/https://doi.org/10.70764/gdpu-fr.2025.1(1)-05

Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). PENGARUH PERLINDUNGAN DATA DAN CYBER SECURITY TERHADAP TINGKAT KEPERCAYAAN MENGGUNAKAN FINTECH MASYARAKAT DI SURABAYA. SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial,

Ekonomi, Budaya, Teknologi, Dan Pendidikan, 1(11), 2497–2516. https://doi.org/10.54443/sibatik.v1i11.395

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. Computers & Security, 138, 103670. https://doi.org/https://doi.org/10.1016/j.cose.2023.103670

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). https://doi.org/10.3390/jrfm18010041

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

Putritama, A., Warsono, S., Ali, S., & Handayani, W. (2024). The Impact of Blockchain Technology on Accounting: A Literature Review. Complex Systems Informatics and Modeling Quarterly, 2024(41), 40–54. https://doi.org/10.7250/csimq.2024-41.03

Schreyer, M., Sattarov, T., & Borth, D. (2022). Federated and privacy-preserving learning of accounting data in financial statement audits. Proceedings of the Third ACM International Conference on AI in Finance, 105–113. https://doi.org/https://doi.org/10.48550/arXiv.2208.12708

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/https://doi.org/10.1016/j.accinf.2021.100548

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/https://doi.org/10.1016/j.jbusres.2019.07.039

Songa, A. V., & Karri, G. R. (2024). An integrated SDN framework for early detection of DDoS attacks in cloud computing. Journal of Cloud Computing, 13(1), 64. https://doi.org/10.1186/s13677-024- 00625-9

Surya Guritno, D., Setiawan, D., Anni Aryani, Y., & Arifin, T. (2024). CYBERATTACKS ON THE ACCOUNTING PROFESSION : A LITERATUR REVIEW. Media Riset Akuntansi, Auditing & Informasi, 24(2), 1411–8831. https://doi.org/10.25105/mraai.v24i2.19953