PROSIDING SEMINAR NASIONAL SANATA DHARMA BERBAGI (USDB)
"Pendidikan Masa Depan"
https://e-conf.usd.ac.id/index.php/usdb
ISSN: 3063-556X | Vol 2, 2024

ANALISIS BLIBLIOMETRIK MENGENAI TREN YANG BERKEMBANG DALAM PENELITIAN SERANGAN SIBER TERHADAP SISTEM AKUNTANSI KEUANGAN

Dhimas Surya Guritno[1], Taufiq Arifin[2]
[1]Program Magister Akuntansi, Fakultas Ekonomi dan Bisnis Universitas Sebelas Maret, Indonesia
[2]Departemen Akuntansi, Fakultas Ekonomi dan Bisnis Universitas Sebelas Maret, Indonesia
dhimassuryaguritno@student.uns.ac.id dan taufiqar@staff.uns.ac.id
*korespondensi: dhimassuryaguritno@student.uns.ac.id

Abstrak
Penelitian ini bertujuan untuk menganalisis tren penelitian serangan siber terhadap sistem akuntansi keuangan melalui pendekatan bibliometrik. Metode yang digunakan melibatkan analisis bibliometrik menggunakan database Scopus, dengan fokus pada publikasi dari tahun 2014 hingga 2023. Data dianalisis menggunakan perangkat lunak VOSviewer untuk memetakan tren penelitian dan kolaborasi antar peneliti. Hasil penelitian menunjukkan adanya peningkatan signifikan dalam jumlah publikasi tentang keamanan siber, dengan puncaknya pada tahun 2023. Teknologi seperti pembelajaran mesin, kecerdasan buatan, dan blockchain sering digunakan dalam penelitian ini untuk mendeteksi dan menangani serangan siber. Amerika Serikat dan India merupakan kontributor utama dalam publikasi penelitian ini. Penelitian ini menekankan pentingnya deteksi dini dan strategi pencegahan yang proaktif untuk melindungi data keuangan yang sensitif. Analisis ini juga mengidentifikasi celah dalam penelitian yang membutuhkan pendekatan lebih spesifik untuk mengatasi ancaman siber pada sistem akuntansi keuangan.
Kata kunci: Keamanan Siber, Serangan Siber, Keuangan, Sistem Akuntansi

A Blibliometric Analysis of Emerging Trends in Research on Cyber Attacks on Financial Accounting Systems

Dhimas Surya Guritno[1], Taufiq Arifin[2]
[1]Program Magister Akuntansi, Fakultas Ekonomi dan Bisnis Universitas Sebelas Maret, Indonesia
[2]Departemen Akuntansi, Fakultas Ekonomi dan Bisnis Universitas Sebelas Maret, Indonesia
dhimassuryaguritno@student.uns.ac.id and taufiqar@staff.uns.ac.id
*correspondence author: dhimassuryaguritno@student.uns.ac.id

Abstract
This study aims to analyze the research trends of cyberattacks on financial accounting systems through a bibliometric approach. The method used involved bibliometric analysis using the Scopus database, focusing on publications from 2014 to 2023. The data was analyzed using VOSviewer software to map research trends and collaboration between researchers. The results showed a significant increase in the number of publications on cybersecurity, with a peak in 2023. Technologies such as machine learning, artificial intelligence, and blockchain are often used in this research to detect and deal with cyberattacks. The United States and India are the main contributors in the publication of this research. This research emphasizes the importance of early detection and proactive prevention strategies to protect sensitive financial data. The

analysis also identifies gaps in the research that require more specific approaches to address cyber threats to financial accounting systems.
Keywords: Cyber Security, Cyber Attack, Finance, Accounting System

Pendahuluan

Keamanan siber dalam sistem keuangan, khususnya terkait serangan terhadap sistem akuntansi keuangan, merupakan bidang penelitian penting yang membutuhkan analisis mendalam untuk memahami tren dan ancaman yang berkembang. Bidang sistem siber-fisik telah mengalami kemajuan yang signifikan dalam menangani ancaman siber, dengan penelitian yang berfokus pada berbagai aspek seperti deteksi serangan siber, ketahanan terhadap serangan, dan integrasi teknologi seperti blockchain untuk meningkatkan keamanan (Qasaimeh et al., 2022; Amin et al., 2020; Alasali, 2023). Perpaduan komponen siber dan fisik dalam sistem seperti jaringan pintar menimbulkan tantangan unik yang memerlukan analisis komprehensif untuk melindungi dari potensi serangan siber-fisik (Amin et al., 2020; Oyewole, 2024; Dawodu, 2023). Memahami dampak ancaman siber terhadap lembaga keuangan sangatlah penting, terutama dengan meningkatnya adopsi perbankan online dan meningkatnya kejahatan siber (Almahadeen, 2024; More, 2024).

Salah satu aspek kunci yang muncul dari literatur adalah kebutuhan akan mekanisme deteksi ancaman yang canggih dalam keamanan siber keuangan. Berbagai penelitian telah mengeksplorasi penggunaan model pembelajaran mesin, jaringan saraf, dan analisis data untuk meningkatkan kemampuan deteksi ancaman (Lee, 2023; Rana et al., 2022; Domashenko, 2023). Dengan memanfaatkan teknologi seperti autoencoder dan model hibrida, para peneliti bertujuan untuk meningkatkan deteksi anomali dan potensi ancaman siber dalam sistem keuangan (Lee, 2023). Selain itu, penggabungan intelijen ancaman siber, kontra intelijen, dan strategi serangan balik dapat memberikan pendekatan yang lebih proaktif terhadap keamanan siber, sehingga memungkinkan organisasi untuk mengantisipasi dan merespons ancaman siber secara efektif (Umoga, 2024).

Kesenjangan penelitian di bidang sistem siber-fisik dan keamanan siber keuangan terletak pada kebutuhan akan pendekatan yang lebih khusus untuk mengatasi tantangan spesifik yang dihadapi oleh lembaga keuangan. Meskipun penelitian yang ada memberikan wawasan yang berharga tentang praktik keamanan siber secara umum dan lanskap ancaman, ada kekurangan analisis mendalam yang berfokus secara khusus pada serangan siber yang menargetkan sistem akuntansi keuangan. Memahami seluk-beluk serangan ini, potensi dampaknya terhadap operasi keuangan, dan mengembangkan mekanisme pertahanan yang ditargetkan yang disesuaikan dengan sistem keuangan merupakan area krusial yang memerlukan eksplorasi lebih lanjut.

Selain itu, integrasi teknologi yang sedang berkembang seperti blockchain dan tekfin dalam sistem keuangan memperkenalkan dimensi baru dari tantangan keamanan yang perlu ditangani (Qasaimeh et al., 2022; Papuashvili, 2023). Dengan meneliti implikasi dari teknologi ini terhadap keamanan siber dan mengembangkan arsitektur keamanan yang berkelanjutan, para peneliti dapat berkontribusi secara signifikan untuk meningkatkan ketahanan sistem keuangan terhadap ancaman siber. Selain itu, sifat ancaman siber yang terus berkembang, mulai dari serangan phishing dan malware tradisional hingga ransomware yang canggih dan serangan rantai pasokan, menggarisbawahi pentingnya penelitian dan inovasi berkelanjutan dalam praktik keamanan siber.

Selain itu, literatur menekankan pentingnya penilaian risiko dan strategi mitigasi di sektor perbankan dan keuangan untuk secara proaktif mengidentifikasi dan mengatasi potensi kerentanan (More, 2024). Dengan melakukan penilaian risiko yang komprehensif, lembaga keuangan dapat memperkuat postur keamanan siber mereka dan menerapkan langkah-langkah pencegahan untuk mengurangi dampak ancaman siber. Selain itu, mengeksplorasi implikasi ketahanan siber pada sistem keuangan dan mengembangkan strategi untuk mengantisipasi,

bertahan, dan pulih dari insiden siber merupakan area penting yang memerlukan penyelidikan lebih lanjut.

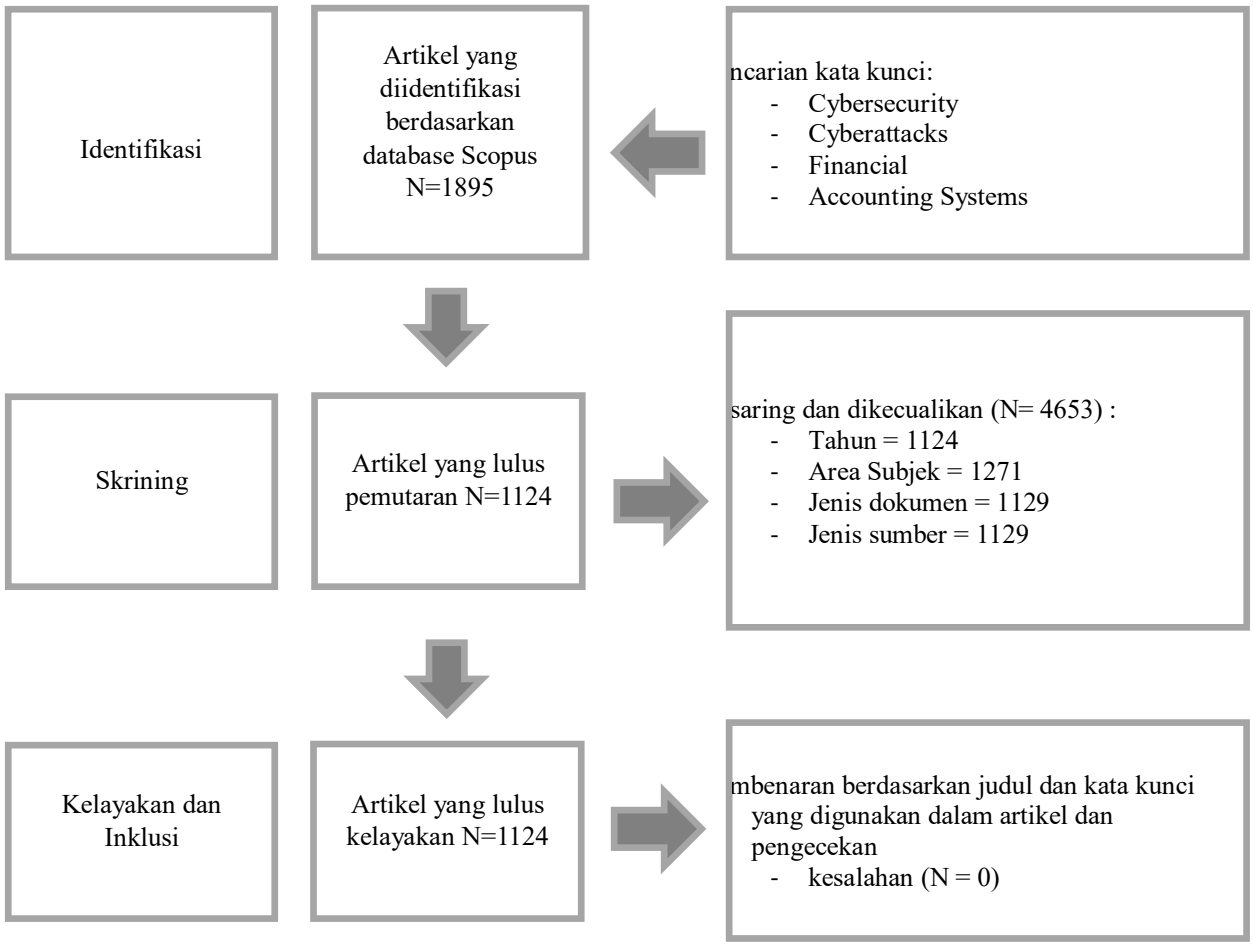
Analisis tren serangan siber terhadap sistem akuntansi keuangan dalam ranah sistem siber-fisik menyajikan lanskap penelitian yang kompleks dan terus berkembang. Dengan menggali lebih dalam tantangan spesifik yang dihadapi oleh lembaga keuangan, memanfaatkan teknologi canggih untuk mendeteksi ancaman, dan meningkatkan praktik keamanan siber melalui penilaian risiko dan strategi ketahanan, para peneliti dapat berkontribusi secara signifikan dalam memperkuat keamanan sistem keuangan dari ancaman siber.

Metode

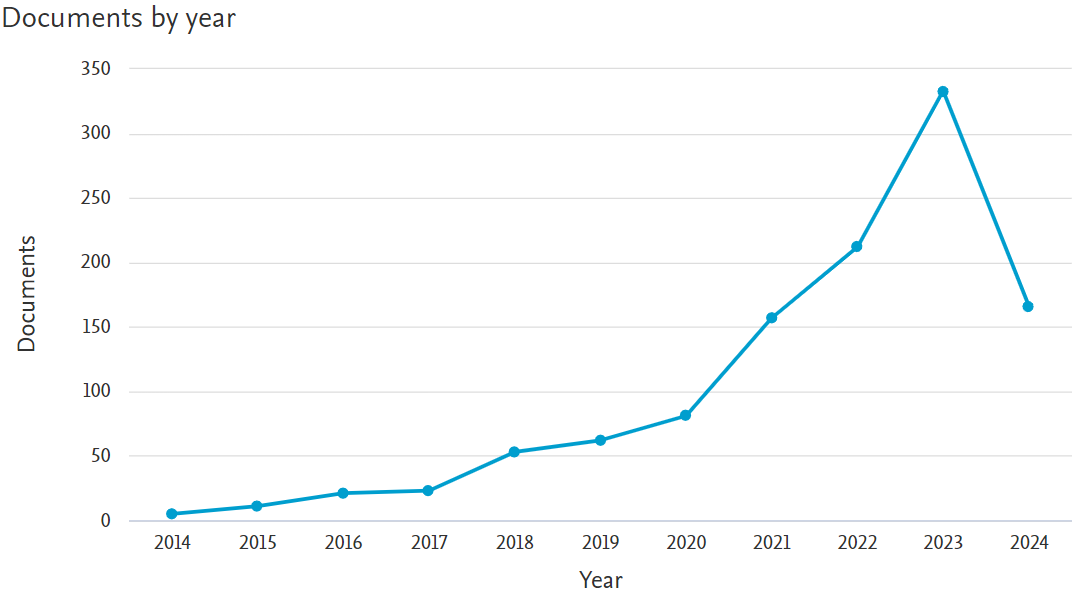
Analisis bibliometrik adalah metode kuantitatif yang melibatkan teknik statistik dan matematika untuk menganalisis publikasi akademis dalam bidang tertentu. Metode ini memungkinkan klasifikasi, peringkasan, dan pembatasan data berdasarkan kriteria tertentu, yang memberikan wawasan tentang dinamika dan tren bidang penelitian tertentu (Koç & Bayri, 2023; Ng dkk., 2023; Rejeb dkk., 2023; Lulewicz-Sas, 2017; Jamwal dkk., 2021). Metode ini mencakup berbagai teknik seperti analisis sitasi, analisis ko-sitasi, dan alat visualisasi seperti VOSviewer untuk memetakan tren penelitian dan kolaborasi (Rani et al., 2022; Shekhar, 2022; Serrano et al., 2019). Dengan menggunakan analisis bibliometrik, peneliti dapat mengevaluasi literatur yang ada secara objektif, mengidentifikasi bidang-bidang yang sedang berkembang, dan memahami evolusi topik penelitian dari waktu ke waktu (Zhang et al., 2021; Shekhar, 2022). Teknik ini membantu menghindari bias yang mungkin timbul dari pilihan bukti yang selektif, memberikan pendekatan yang kuat dan sistematis untuk menganalisis data ilmiah dalam jumlah besar (Rejeb et al., 2023; Gülhan & Kurutkan, 2021).

Data penelitian diperoleh dari database Scopus, yang merupakan sumber informasi ilmiah yang dapat diandalkan yang mencakup berbagai disiplin ilmu. Pencarian dilakukan dengan menggunakan kata kunci “Keamanan Siber”, “Serangan Siber”, “Keuangan”, dan “Sistem Akuntansi” untuk memastikan cakupan yang komprehensif. Artikel-artikel yang diterbitkan dalam 10 tahun terakhir (2014-2024) dipilih untuk mendapatkan gambaran terkini tentang tren penelitian pelaporan keberlanjutan. Artikel yang diperoleh dari pencarian awal disaring berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi meliputi artikel yang berfokus pada pelaporan keberlanjutan dan diterbitkan dalam jurnal yang telah melalui proses penelaahan sejawat. Artikel yang tidak relevan, seperti artikel yang berfokus pada topik lain atau tidak diulas oleh rekan sejawat, tidak disertakan dalam analisis. Proses penyaringan ini penting untuk memastikan bahwa data yang dianalisis representatif dan relevan dengan topik penelitian (Donthu et al., 2021). Analisis bibliometrik dilakukan dengan menggunakan perangkat lunak VOSviewer yang memungkinkan visualisasi jaringan dan analisis statistik.

Gambar 11
Protokol Penelitian

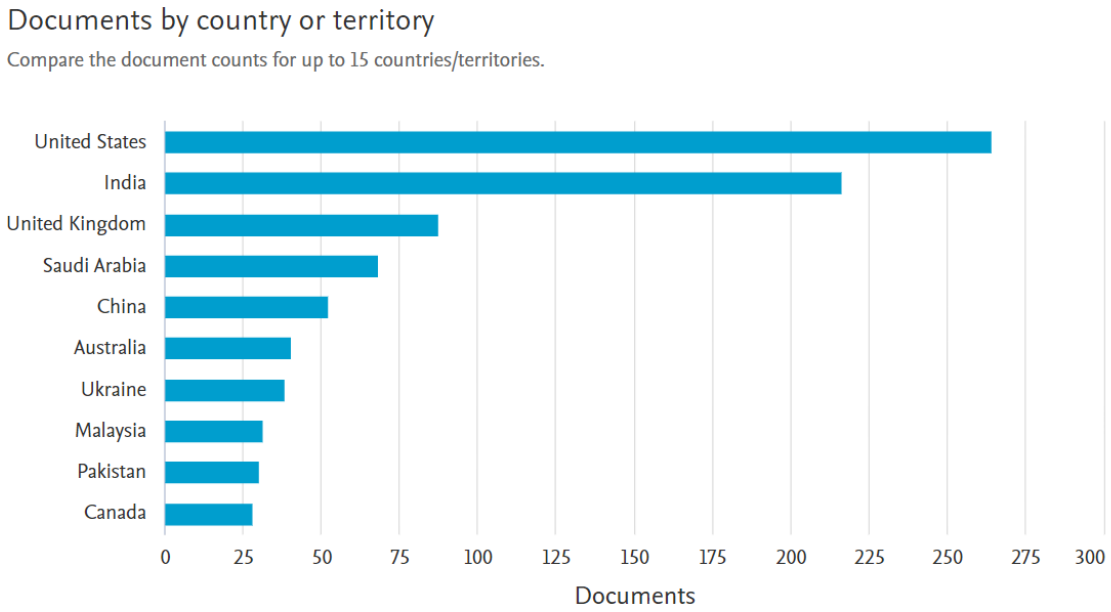


Hasil dan Pembahasan



Gambar 12
Dokumen Berdasarkan Tahun

Grafik yang disajikan pada Gambar 2 menunjukkan tren jumlah dokumen yang diterbitkan per tahun dari 2014 hingga 2024 terkait dengan penelitian serangan siber terhadap sistem akuntansi keuangan. Secara keseluruhan, terdapat peningkatan jumlah dokumen yang signifikan dari tahun 2014 hingga 2023, dengan puncak tertinggi pada tahun 2023. Dari tahun 2014 hingga 2017, jumlah dokumen yang diterbitkan tetap relatif rendah dan stabil, menunjukkan bahwa topik ini belum banyak mendapat perhatian dari peneliti selama periode tersebut. Mulai tahun 2018 hingga 2020, jumlah dokumen yang diterbitkan mulai meningkat dengan laju yang lebih tinggi, yang bisa diindikasikan sebagai tanda mulai adanya peningkatan minat terhadap penelitian serangan siber pada sistem akuntansi keuangan. Pada periode 2021 hingga 2023, terjadi peningkatan yang signifikan dalam jumlah dokumen yang diterbitkan, khususnya pada tahun 2022 dan mencapai puncaknya pada tahun 2023. Peningkatan yang tajam ini mungkin mencerminkan semakin tingginya kesadaran dan perhatian terhadap ancaman serangan siber dalam sistem akuntansi keuangan, serta kemungkinan adanya peningkatan insiden serangan siber yang mendorong lebih banyak penelitian di bidang ini. Namun, pada tahun 2024, terlihat adanya penurunan jumlah dokumen yang diterbitkan dibandingkan tahun 2023. Penurunan ini bisa diakibatkan oleh berbagai faktor, termasuk siklus publikasi yang belum selesai, perubahan fokus penelitian, atau kebijakan baru yang mempengaruhi jumlah publikasi. Secara keseluruhan, grafik ini menunjukkan bahwa penelitian mengenai serangan siber terhadap sistem akuntansi keuangan telah mendapatkan perhatian yang meningkat secara signifikan dalam beberapa tahun terakhir, dengan puncak perhatian pada tahun 2023.



Gambar 13
Dokumen Berdasarkan Negara atau Wilayah

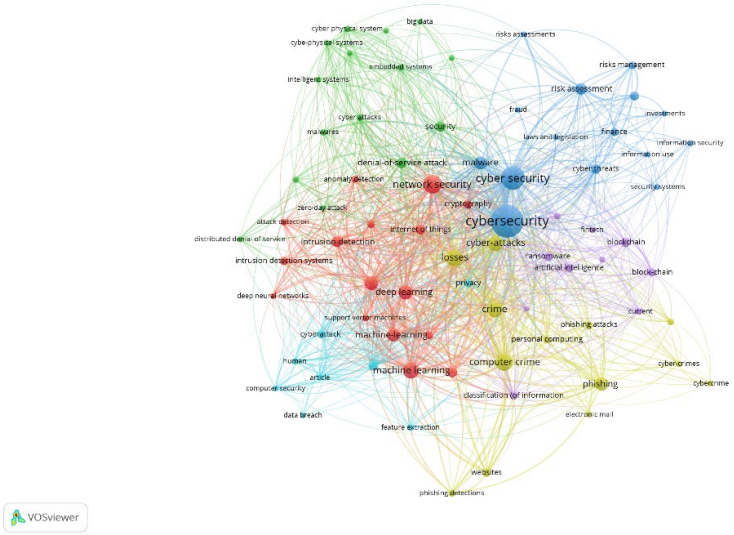
Negara/Wilayah	Dokumen
Amerika Serikat	265
India	216
Inggris	87
Arab Saudi	68
China	52
Australia	40
Ukraina	38
Malaysia	31
Pakistan	30
Kanada	28

Tabel 2
Dokumen Berdasarkan Negara atau Wilayah

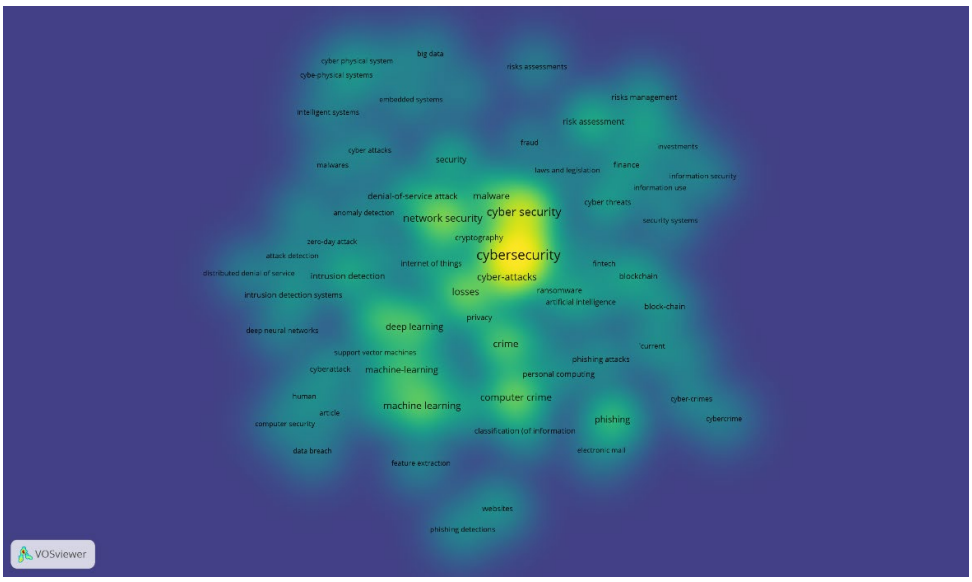
Gambar 3 dan Tabel 1 yang disajikan menampilkan jumlah dokumen yang diterbitkan oleh berbagai negara terkait dengan penelitian serangan siber terhadap sistem akuntansi keuangan. Amerika Serikat memimpin dengan 265 dokumen, menunjukkan kontribusi penelitian yang sangat signifikan, yang mungkin didorong oleh infrastruktur penelitian yang kuat, dukungan pemerintah, dan tingginya tingkat insiden serangan siber. India berada di posisi kedua dengan 216 dokumen, mencerminkan meningkatnya perhatian dan upaya penelitian di India terhadap ancaman siber dalam sistem akuntansi, yang didukung oleh pertumbuhan ekonomi pesat dan adopsi teknologi tinggi. Inggris menempati posisi ketiga dengan 87 dokumen, menunjukkan partisipasi aktif dalam penelitian ini, didorong oleh sektor keuangan yang maju dan kebutuhan untuk melindungi infrastruktur keuangan yang kompleks.Saudi Arabia memiliki 68 dokumen yang diterbitkan, mengindikasikan kesadaran yang meningkat akan pentingnya keamanan siber dalam sistem akuntansi keuangan seiring dengan modernisasi ekonominya. China dengan 52 dokumen menunjukkan partisipasi yang signifikan, mengingat posisinya sebagai salah satu ekonomi terbesar dunia yang menghadapi banyak tantangan dalam keamanan siber. Australia memiliki 40 dokumen, menandakan kesadaran dan perhatian yang cukup terhadap masalah serangan siber dalam sistem akuntansi di negara tersebut. Ukraina dengan 38 dokumen

menunjukkan keterlibatan aktif, mungkin dipengaruhi oleh kondisi geopolitik dan pengalaman dengan serangan siber. Malaysia memiliki 31 dokumen, menunjukkan kontribusi yang signifikan dalam penelitian ini, sementara Pakistan dengan 30 dokumen juga menunjukkan minat yang substansial seiring dengan perkembangan teknologi di negara tersebut. Kanada berada di posisi terakhir dengan 28 dokumen, meskipun jumlahnya lebih sedikit, tetap menunjukkan komitmen dalam penelitian serangan siber terhadap sistem akuntansi keuangan.

Secara keseluruhan, tabel ini menunjukkan bahwa penelitian mengenai serangan siber terhadap sistem akuntansi keuangan tersebar luas di berbagai negara, dengan Amerika Serikat dan India sebagai kontributor utama. Negara-negara lain seperti Inggris, Saudi Arabia, dan China juga menunjukkan partisipasi yang signifikan. Perbedaan jumlah dokumen yang diterbitkan mencerminkan tingkat perhatian, kapasitas penelitian, dan tingkat ancaman siber yang dihadapi oleh setiap negara, membantu memahami distribusi geografis dari penelitian di bidang ini dan mengidentifikasi area-area yang memerlukan perhatian lebih lanjut.



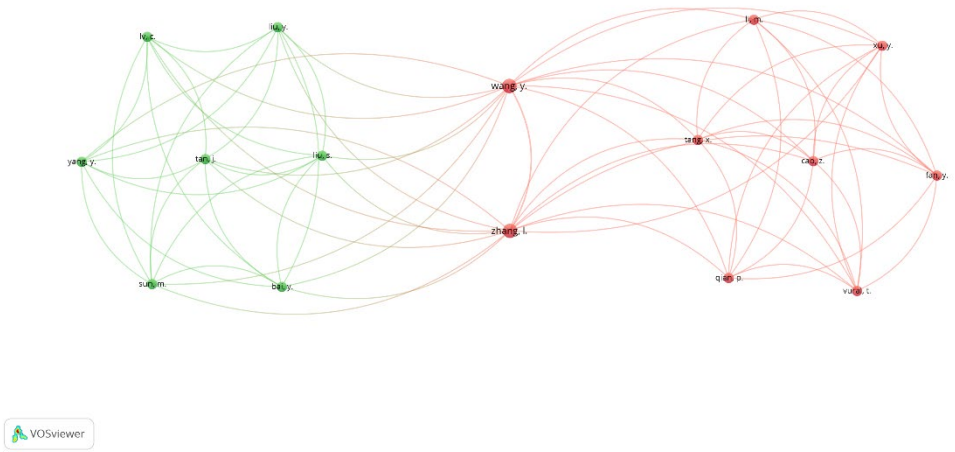
Gambar 14
Grafik Co-Occurance Network Visualization



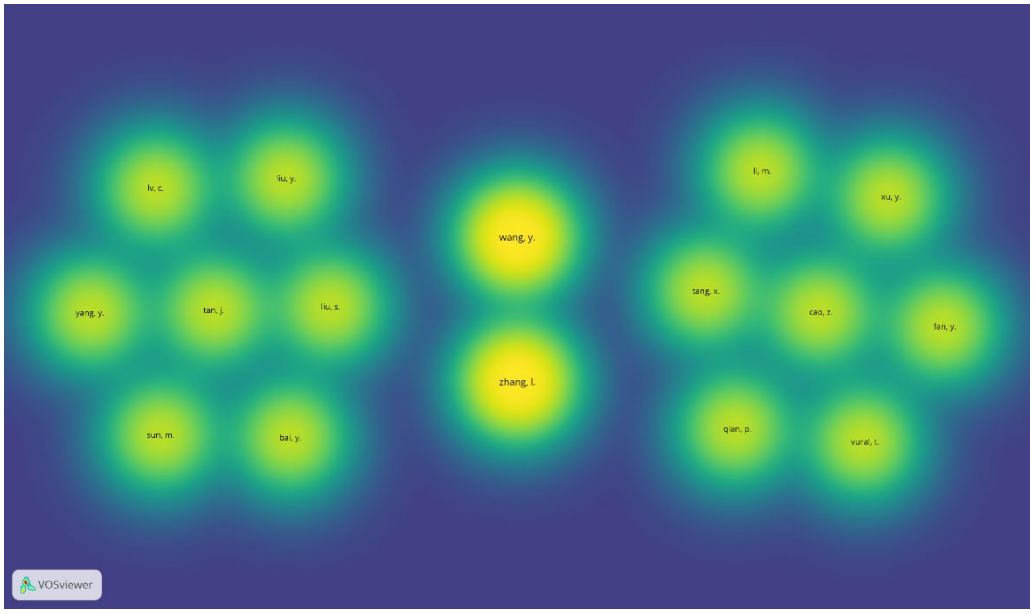
Gambar 15
Grafik Co-Occurance Density Visualization

Gambar visualisasi jaringan bibliometrik dari VOSviewer menunjukkan hubungan antara kata kunci dan topik dalam penelitian tentang serangan siber terhadap sistem akuntansi keuangan. Dalam visualisasi ini, kata kunci seperti "cybersecurity," "cyber attacks," dan "network security" berada di pusat jaringan, menunjukkan bahwa topik-topik ini merupakan fokus utama dalam penelitian ini. Cluster merah mengelompokkan kata kunci seperti "deep learning," "network security," dan "cyber attacks," yang menunjukkan bahwa penelitian ini sering menggabungkan teknologi pembelajaran mendalam dengan keamanan jaringan untuk mengatasi serangan siber. Cluster hijau mencakup kata kunci seperti "cyber physical systems," "big data," dan "intrusion detection," yang menunjukkan fokus pada sistem siber-fisik dan penggunaan big data untuk deteksi intrusi.

Cluster biru mengelompokkan kata kunci seperti "risk management," "investments," dan "cyber security," yang mengindikasikan perhatian pada manajemen risiko dan investasi dalam keamanan siber. Sementara itu, cluster kuning berfokus pada kata kunci seperti "phishing," "personal data protection," dan "computer crime," yang menunjukkan perhatian terhadap kejahatan komputer dan perlindungan data pribadi. Garis-garis yang menghubungkan kata kunci ini menunjukkan kekuatan hubungan antar topik, dengan garis yang lebih tebal menandakan hubungan yang lebih kuat atau lebih sering disebutkan bersama dalam literatur.



Gambar 16
Grafik Co-Authorship Network Visualization



Gambar 17
Grafik Co-Authorship Density Visualization

Gambar 6 menunjukkan jaringan kolaborasi antara peneliti berdasarkan analisis bibliometrik dalam penelitian tentang serangan siber terhadap sistem akuntansi keuangan. Visualisasi ini mengelompokkan peneliti berdasarkan kolaborasi dan hubungan antara satu dengan yang lain. Cluster hijau mengelompokkan peneliti seperti "liu y.," "tan j.," dan "yang y.," yang sering bekerja sama satu sama lain, menunjukkan adanya kolaborasi yang erat di antara mereka. Cluster merah, yang mencakup peneliti seperti "wang y." dan "zhang l.," menunjukkan kelompok kolaborasi lainnya. Garis yang menghubungkan peneliti-peneliti ini menunjukkan frekuensi dan kekuatan kolaborasi, dengan garis yang lebih tebal mengindikasikan kolaborasi yang lebih sering terjadi. Peneliti yang berada di pusat dari cluster, seperti "wang y." dan "zhang l.," tampaknya memiliki banyak kolaborasi dan berperan sebagai pusat utama dalam jaringan penelitian ini.

Gambar 7 merupakan visualisasi density atau kepadatan kolaborasi antar peneliti. Pusat-pusat kepadatan menunjukkan peneliti yang memiliki banyak kolaborasi dan sering disebut dalam literatur. "wang y." dan "zhang l." terlihat sebagai pusat utama kepadatan, menunjukkan bahwa mereka adalah peneliti yang sangat aktif dan berpengaruh dalam bidang ini. Warna hijau yang lebih terang dalam visualisasi ini menunjukkan kepadatan kolaborasi yang lebih tinggi, mengindikasikan bahwa peneliti di area tersebut sering bekerja sama dengan banyak peneliti lain dan memiliki peran kunci dalam jaringan penelitian.

Kesimpulan

Penelitian ini mengungkapkan adanya peningkatan signifikan dalam jumlah dokumen yang diterbitkan mengenai serangan siber terhadap sistem akuntansi keuangan dari tahun 2014 hingga 2023, dengan puncaknya terjadi pada tahun 2023. Hal ini mencerminkan meningkatnya perhatian dan kesadaran terhadap ancaman serangan siber dalam sistem akuntansi keuangan. Secara geografis, Amerika Serikat memimpin dengan kontribusi terbesar dalam penelitian ini, diikuti oleh India dan Inggris. Negara-negara dengan infrastruktur penelitian yang kuat dan tingkat kejadian serangan siber yang tinggi cenderung menghasilkan lebih banyak publikasi terkait topik ini.

Penelitian banyak memfokuskan pada penggunaan teknologi canggih seperti pembelajaran mesin (machine learning), kecerdasan buatan (AI), dan teknologi blockchain untuk mendeteksi

dan mengatasi serangan siber. Model autoencoder-MLP dan teknik jaringan saraf lainnya sering disebut sebagai metode efektif untuk meningkatkan kemampuan deteksi ancaman. Pentingnya deteksi dan pencegahan dini terhadap serangan siber menjadi salah satu fokus utama penelitian. Dengan menggunakan teknik analisis data dan intelijen ancaman siber, lembaga keuangan dapat mengidentifikasi dan mengatasi risiko keamanan sebelum eskalasi.

Sistem fisik siber (cyber-physical systems) menghadirkan tantangan unik, termasuk risiko serangan yang dapat mengganggu infrastruktur kritis. Model optimisasi seperti Lotka–Volterra digunakan untuk menilai dan memperbaiki keamanan sistem ini, menunjukkan pendekatan proaktif dalam mitigasi risiko. Serangan siber tidak hanya menyebabkan kerugian finansial tetapi juga memiliki dampak luas terhadap stabilitas pasar dan kepercayaan investor. Penelitian menunjukkan bahwa serangan seperti terorisme siber dapat mempengaruhi valuasi pasar saham, menekankan perlunya langkah-langkah keamanan siber yang kuat untuk melindungi aset keuangan.

Visualisasi jaringan kolaborasi menunjukkan bahwa penelitian mengenai serangan siber terhadap sistem akuntansi keuangan melibatkan kolaborasi yang erat antara peneliti. Beberapa peneliti seperti "wang y." dan "zhang l." menonjol sebagai pusat kolaborasi, menunjukkan peran penting mereka dalam jaringan penelitian. Pengembangan strategi resiliensi siber menjadi perhatian penting untuk memastikan kontinuitas operasi dan melindungi data keuangan sensitif. Penelitian menekankan pentingnya kerangka kerja resiliensi siber untuk memperkuat sektor keuangan terhadap potensi gangguan.

Penggunaan analisis bibliometrik dan alat visualisasi seperti VOSviewer membantu memahami dinamika dan tren penelitian. Ini memungkinkan klasifikasi, penyederhanaan, dan pembatasan data berdasarkan kriteria tertentu, memberikan wawasan tentang evolusi topik penelitian dari waktu ke waktu. Penelitian ini mengidentifikasi celah dalam analisis mendalam mengenai serangan siber yang menargetkan sistem akuntansi keuangan. Pemahaman yang lebih mendalam tentang serangan ini, dampaknya terhadap operasi keuangan, dan pengembangan mekanisme pertahanan yang ditargetkan sangat diperlukan.

Analisis bibliometrik ini memberikan wawasan yang mendalam mengenai tren dan celah penelitian yang ada, serta kebutuhan untuk memperkuat upaya penelitian dan pengembangan dalam keamanan siber. Dengan demikian, penelitian ini berkontribusi pada literatur dengan menyediakan dasar yang kuat untuk penelitian lebih lanjut yang bertujuan meningkatkan ketahanan sistem akuntansi keuangan terhadap ancaman siber yang terus berkembang.

Daftar Pustaka

Alasali, F. (2023). Smart grid resilience for grid-connected pv and protection systems under cyber threats. *Smart Cities, 7*(1), 51-77. https://doi.org/10.3390/smartcities7010003

Almahadeen, L. (2024). Enhancing threat detection in financial cyber security through auto encoder-mlp hybrid models. International Journal of Advanced *Computer Science and Applications, 15*(4). https://doi.org/10.14569/ijacsa.2024.0150495

Amin, B., Taghizadeh, S., Rahman, M., Hossain, M., Varadharajan, V., & Chen, Z. (2020). Cyber attacks in smart grid – dynamic impacts, analyses and recommendations. *Iet Cyber-Physical Systems Theory & Applications, 5*(4), 321-329. https://doi.org/10.1049/iet-cps.2019.0103

Dawodu, S. (2023). Cybersecurity risk assessment in banking: methodologies and best practices. *Computer Science & It Research Journal, 4*(3), 220-243. https://doi.org/10.51594/csitrj.v4i3.659

Domashenko, S. (2023). Blockchain and fintech technologies in the digital space of financial and industrial companies. *Sustainable Engineering and Innovation Issn 2712-0562, 5*(2), 281-302. https://doi.org/10.37868/sei.v5i2.id232

Gülhan, P. and Kurutkan, M. (2021). Bibliometric analysis of covid-19 publications in the field of chest and infectious diseases. *Düzce Tıp Fakültesi Dergisi, 23*(1), 30-40. https://doi.org/10.18678/dtfd.826465

Jamwal, A., Agrawal, R., Sharma, M., Kumar, V., & Garza-Reyes, J. (2021). Machine learning applications for sustainable manufacturing: a bibliometric-based review for future research. *Journal of Enterprise Information Management, 35*(2), 566-596. https://doi.org/10.1108/jeim-09-2020-0361

Karamdel, S., Liang, X., Faried, S., & Mitolo, M. (2022). Optimization models in cyber-physical power systems: a review. *Ieee Access, 10*, 130469-130486. https://doi.org/10.1109/access.2022.3229626

Koç, F. and Bayri, O. (2023). Analysis of publications in the field of accounting auditing with traditional bibliometric methods and citespace based visual mapping techniques. Eskişehir Osmangazi Üniversitesi İktisadi Ve İdari *Bilimler Dergisi, 18*(1), 162-186. https://doi.org/10.17153/oguiibf.1233546

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security, 45*, 58-74. https://doi.org/10.1016/j.cose.2014.05.006

Lee, J. (2023). Generating ics anomaly data reflecting cyber-attack based on systematic sampling and linear regression. *Sensors, 23*(24), 9855. https://doi.org/10.3390/s23249855

Lulewicz-Sas, A. (2017). Corporate social responsibility in the light of management science – bibliometric analysis. *Procedia Engineering, 182*, 412-417. https://doi.org/10.1016/j.proeng.2017.03.124

More, S. (2024). Enhanced intrusion detection systems performance with unsw-nb15 data analysis. *Algorithms, 17*(2), 64. https://doi.org/10.3390/a17020064

Ng, J., Liu, H., Shah, A., Wieland, L., & Moher, D. (2023). Characteristics of bibliometric analyses of the complementary, alternative, and integrative medicine literature: a scoping review protocol. *F1000research, 12*, 164. https://doi.org/10.12688/f1000research.130326.1

Oyewole, A. (2024). Cybersecurity risks in online banking: a detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews, 21*(3), 625-643. https://doi.org/10.30574/wjarr.2024.21.3.0707

Papuashvili, D. (2023). Cyber resilience implications for the financial system. *BARP, 8*(a). https://doi.org/10.62232/barp.8.2023.6774

Qasaimeh, M., Hammour, R., Yassein, M., Al-Qassas, R., Torralbo, J., & Lizcano, D. (2022). Advanced security testing using a cyber-attack forecasting model: a case study of financial institutions. *Journal of Software Evolution and Process, 34*(11). https://doi.org/10.1002/smr.2489

Rana, M., Ellahi, O., Alam, M., Webber, J., Mehbodniya, A., & Khan, S. (2022). Offensive security: cyber threat intelligence enrichment with counterintelligence and counterattack. *Ieee Access, 10*, 108760-108774. https://doi.org/10.1109/access.2022.3213644

Rani, P., Yadav, A., Kumar, D., Pandey, J., Gull, M., Ansari, M., … & Sahni, B. (2022). A bibliometric analysis of literature on covid-19 and mental health. *National Journal of Community Medicine, 13*(09), 642-650. https://doi.org/10.55489/njcm.130920222131

Rejeb, A., Rejeb, K., & Treiblmaier, H. (2023). Mapping metaverse research: identifying future research areas based on bibliometric and topic modeling techniques. *Information, 14*(7), 356. https://doi.org/10.3390/info14070356

Serrano, L., Sianes, A., & Ariza-Montes, A. (2019). Using bibliometric methods to shed light on the concept of sustainable tourism. *Sustainability, 11*(24), 6964. https://doi.org/10.3390/su11246964

Sha, M. (2022). Artificial intelligence in cyber security: a survey. International *Journal of Computer Engineering in Research Trends, 9*(10), 201-205. https://doi.org/10.22362/ijcert/2022/v9/i10/v9i1003

Sharif, M. and Mohammed, M. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews, 15*(1), 138-156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Smith, K., Smith, L., Burger, M., & Boyle, E. (2023). Cyber terrorism cases and stock market valuation effects. *Information and Computer Security, 31*(4), 385-403. https://doi.org/10.1108/ics-09-2022-0147

Sufi, F. (2023). A new ai-based semantic cyber intelligence agent. *Future Internet, 15*(7), 231. https://doi.org/10.3390/fi15070231

Umoga, U. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive, 11(*1), 1810-1817. https://doi.org/10.30574/ijsra.2024.11.1.0284

Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I., … & Kurchenko, O. (2021). Development of a method for assessing the security of cyber-physical systems based on the lotka–volterra model. *Eastern-European Journal of Enterprise Technologies, 5*(9 (113)), 30-47. https://doi.org/10.15587/1729-4061.2021.241638

Zhang, Y., Porter, A., Cunningham, S., Chiavetta, D., & Newman, N. (2021). Parallel or intersecting lines? intelligent bibliometrics for investigating the involvement of data science in policy analysis. *Ieee Transactions on Engineering Management, 68*(5), 1259-1271. https://doi.org/10.1109/tem.2020.2974761

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). Bagaimana melakukan analisis bibliometrik: Tinjauan umum dan pedoman. *Jurnal Penelitian Bisnis, 133*, 285-296.