ANALISIS BIBLOMETRIK KEAMANAN PERUSAHAAN PENJUALAN ONLINE UNTUK MENCEGAH TERJADINYA KEJAHATAN SIBER

Rizky Adin Adriansyah [1], Aldof Faris Anugrah [2]
[1,2]Teknik Informatika, Universitas Majalengka
Jl. KH Abdul Halim No 103 Kabupaten Majalengka - Provinsi Jawa Barat, Indonesia
e-mail : *[1]rizkyadinadriansyah17@gmail.com,[2]aldoffaris02@gmail.com

Abstract
The present study conducts a comprehensive bibliometric analysis of the research landscape related to cybersecurity, cybercrime, and online sales companies. Utilizing Vosviewer, the analysis encompasses a wide array of publications, including authors, organizations, countries, keywords, and information sources. The primary objective is to identify the prominent trends, key contributors, and major research themes in the field. By shedding light on the evolving landscape of cybersecurity and cybercrime in the context of online sales companies, the study's goal is to provide helpful insights for researchers and practitioners. Furthermore, the analysis seeks to highlight the prevalence of cybercrime in online sales companies and explore the various dimensions of cybersecurity. The findings of this study are expected to not only contribute to the existing body of knowledge but also to guide future research endeavors and policy formulations in the domain of cybersecurity and cybercrime within online sales companies.

Keyword: *Bibliometric Analysis, Cyber Crime, Cyber Security, Online Sales Company, Vosviewer*

PENDAHULUAN

Dengan kemajuan teknologi yang begitu cepat, setiap masalah yang muncul dalam berbagai aktivitas sehari-hari dipengaruhi dan digunakan sebagai pedoman untuk menyelesaikan masalah saat ini. Keadaan tersebut bukan hanya sebatas kata-kata; itu benar-benar terjadi karena munculnya kegiatan pembangunan dalam berbagai industri yang sering bergantung pada teknologi informasi digital (Romdoni, Ruhiawati, and Gunawan 2022). Banyak perusahaan skala kecil dan menengah baru muncul di era industri 4.0. Setiap bisnis harus mampu beradaptasi dengan pesatnya perkembangan teknologi informasi jika mereka ingin tetap stabil dan berkelanjutan (Normah et al. 2022). Perusahaan online besar di Indonesia, seperti bukalapak.com, olx.co.id, dan lazada.com, sudah mulai menghasilkan uang. Semakin banyak pemilik dan pembeli yang tertarik dengan bisnis online (Srisadono 2018). Ini juga berlaku untuk jual-beli barang atau jasa yang dapat dilakukan secara online. Produk yang dijual dapat dengan mudah dilihat dari mana saja dengan koneksi internet melalui sebuah website penjualan (Nursari and Immanuel 2018).

Analisis bibliometrik adalah metode kuantitatif untuk menganalisis data bibliografi yang tercantum dalam artikel. Metode ini menggunakan pendekatan statistik dan dianggap efektif dalam menyediakan kumpulan data yang dapat meningkatkan kualitas penelitian. Banyak penelitian telah membahas analisis bibliometrik (Nandiyanto and Al Husaeni 2022). Tinjauan evaluasi digunakan untuk mengukur pengaruh penelitian *absolut* dari publikasi penelitian, penulis, organisasi, dan negara. Variabel produktivitas seperti jumlah kutipan, publikasi per tahun, dan jurnal termasuk dalam analisis ini. Tinjauan evaluatif kualitatif juga dapat dilakukan oleh pakar penilaian ahli tentang indikator dampak penelitian di bidang tertentu. Namun, keterkaitan antara ukuran evaluasi yang disebutkan di atas adalah fokus dari teknik tinjauan relasional. Jumlah output kolaboratif, hubungan kolaboratif, dan kekuatan hubungan terkait diukur dan dikomunikasikan. Kemunculan bersama, hubungan berbasis kutipan, dan analisis berbasis kutipan bersama adalah metrik hubungan yang berguna lainnya. Transfer informasi

antara berbagai kelompok penelitian dapat dilihat melalui hubungan penulis bersama (Sharma et al. 2023).

Keamanan siber adalah ide tentang teknik komputer yang menjaga privasi, kerahasiaan, dan integritas data yang dikirimkan atau disimpan di jaringan internal atau di Internet itu sendiri (Furstenau et al. 2020). Dengan menggunakan solusi perangkat keras dan perangkat lunak, cyber security melindungi data, pemrosesan data, dan sistem penyimpanan (Istanbullu 2023). Dalam keamanan siber, melindungi sistem internal adalah hal yang paling penting, tetapi keamanan lingkungan jaringan juga sama pentingnya. Ini termasuk memantau entitas atau objek yang mencurigakan di luar jaringan secara real-time, mencari sumber serangan, dan memantau aplikasi berbahaya (Yildiz and Younes Gejam 2022). Keamanan siber sangat penting dalam memerangi kejahatan siber karena melindungi sistem, jaringan, dan data digital dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah. Kejahatan siber dapat mengambil banyak bentuk, seperti peretasan, *phishing, malware, dan ransomware*, dan dapat berdampak negatif pada orang dan organisasi (Mijwil, Aljanabi, and ChatGPT 2023).

Beberapa kategori kejahatan siber termasuk pelanggaran siber, seperti mengakses sistem tanpa izin; penipuan atau pencurian siber, seperti pencurian identitas dan penipuan daring; pornografi atau kecabulan siber, seperti eksploitasi seksual anak-anak di internet; dan kekerasan siber, seperti pelecehan siber atau terorisme siber. Karena tidak ada definisi hukum yang standar untuk kejahatan siber dan statistik yang cukup, sulit untuk menaksir jumlah kejahatan siber yang terjadi di banyak negara. Namun, ada bukti bahwa kejahatan dunia maya meningkat sementara kejahatan jalanan biasa turun (Bossler and Berenblum 2019). Kasus *cybercrime* tidak hanya terjadi sekali. Dari Januari hingga Desember 2019, Direktorat Tindak Pidana Siber Bareskrim Polri menerima 4.586 laporan tentang kasus *cybercrime* di Indonesia. Dengan 1.617 kasus, ini adalah laporan nomor dua tentang penipuan online. Korban *cybercrime* sebagian besar adalah pengguna atau pelaku penjualan online, yaitu pembeli dan penjual. Oleh karena itu, ini dapat dianggap sebagai bukti penting tentang seberapa baik masyarakat Indonesia memahami keamanan siber (Irfan, Elvia, and Dania 2023). Kasus-kasus di atas jelas menunjukkan fenomena bagaimana orang-orang yang tidak diketahui dapat diretas dan menginfeksi sistem informasi yang dimiliki oleh organisasi, instansi, atau lembaga elit. Sudah menjadi keharusan bahwa sistem informasi yang dimiliki oleh organisasi, instansi, atau lembaga elite dikelola oleh profesional yang berpengalaman di bidang mereka. Namun, secara praktis, para pelaku kejahatan masih dapat memasuki dan bahkan menghancurkan sistem tersebut secara permanen. Hal ini tentunya menimbulkan pertanyaan tentang apakah lembaga-lembaga terkemuka di Indonesia telah menerapkan keamanan siber informasi dengan benar (Kwarto and Angsito 2018).

Pada penelitian sebelumnya telah melakukan bertema analisis tentang keamanan siber dalam konteks penjualan online dari kejahatan siber. Penelitian menyoroti beberapa penelitian utama yang dijadikan acuan seperti ungkapan dari. Beberapa faktor, termasuk kurangnya pengetahuan, keinginan untuk hadiah palsu, tingginya tingkat pengangguran dan kemiskinan, dan kebijakan keamanan pemerintah yang kurang tegas, berkontribusi pada peningkatan kejahatan siber dalam transaksi *e-commerce*. Bentuk-bentuk kejahatan siber dalam *e-commerce* meliputi peretasan, pencurian identitas, pencurian data, *phising, spamming, pharming, pretexting, qui pro quo*, dan kontak langsung dengan korban (Elisanti et al. 2024). Solusi khusus diperlukan untuk mengatasi masalah kejahatan siber yang berkaitan dengan penjualan online. Meskipun bisnis modern menyukai penjualan online, ancaman keamanan dunia maya seperti ancaman keamanan siber mengancamnya. Meskipun perusahaan berinvestasi sejumlah besar uang untuk mengatasi masalah ini, hal itu masih sulit. Serangan siber menyerang data pribadi dan organisasi. Meskipun teknologi menawarkan banyak keuntungan dan metode baru untuk mengelola bisnis, akan selalu ada ancaman keamanan siber. Keunggulan dan kesuksesan bisnis bergantung pada investasi dalam keamanan *e-commerce*. Karena paparan data, tidak ada yang dapat kehilangan kepercayaan klien. Langkah-langkah pemantauan yang ketat diperlukan untuk organisasi dan kecelakaan yang melibatkan organisasi dan pelanggan (Desamsetti 2021). Hal ini didukung oleh fakta bahwa merek *e-commerce* menarik dan dibutuhkan di pasar bisnis kontemporer. Namun, hal ini menghadapi masalah keamanan siber. Meskipun bisnis terus berinvestasi banyak uang untuk

menyelesaikan masalah ini, situasinya sulit. Serangan siber biasanya menargetkan data pribadi dan organisasi. Meskipun teknologi memberikan banyak keuntungan dan cara baru untuk berbisnis, masalah keamanan dunia maya akan tetap ada. Untuk mendapatkan keunggulan kompetitif dan keberhasilan bisnis e-commerce, investasi dan peningkatan keamanan *e-commerce* sangat penting (Liu et al. 2022). Penelitian ini untuk meningkatkan efisiensi investasi keamanan dalam hal penjualan online dengan menganalisis komponen yang mempengaruhi keberhasilan strategi keamanan dan menemukan solusi yang lebih tepat sasaran untuk mengatasi ancaman keamanan siber. Penelitian ini bertujuan untuk memberikan gambaran komprehensif tentang lanskap penelitian, mengidentifikasi kesenjangan penelitian utama, dan menawarkan wawasan untuk arah penelitian masa depan dalam keamanan siber dan kejahatan siber di perusahaan penjualan online.

METODE PENELITIAN

Pembuatan artikel ini adalah untuk menganalisis bagaimana artikel analisis bibliometrik perusahaan penjualan online untuk cyber security dari cyber crime. Penelitian menggunakan analisis bibliometrik, pendekatan kuantitatif dan sistematis dalam menganalisis publikasi penelitian. Vosviewer digunakan untuk memvisualisasikan jaringan publikasi, penulis, dan kata kunci.

1. Pencarian Spesifik

Analisis bibliometrik sebagai alat untuk mengeksplorasi dan menilai banyak data menjadi lebih populer dan diakui. Ini memungkinkan kami untuk mendekonstruksi perubahan morfologi kecil yang terjadi di suatu wilayah tertentu selama sejarahnya, sekaligus menjelaskan wilayah baru yang telah berkembang. Analisis kinerja adalah satu dan pemetaan ilmiah adalah dua jenis analisis bibliometrik. Ilmu pemetaan berfokus pada hubungan yang ada antara konstituen penelitian, sedangkan analisis kinerja mempertimbangkan kontribusi mereka. Ini adalah perbedaan utama antara keduanya. Proses dimulai dengan mencari frase dalam database Google. Frasa tersebut secara eksplisit membahas analisis biblometrik perusahaan penjualan online untuk cyber scurity dari cyber crime dengan Harzing's Publish or Perish. Scientometrics, Applied Sciences (AS), Sensors, Computers, & Security (CAS), Journal of Open Innovation (JOOI), Security Journal (SJ), dan Journal of Computer Information Systems (JCIS).

2. Jurnal Reputasi

Pada tahap ini, majalah yang memiliki kedudukan yang baik telah dipilih dan masih dalam proses hari ini. Tabel 1 menampilkan hasil pemeriksaan jurnal.

Tabel 1. menampilkan hasil pemeriksaan jurnal

Point of View	Sciento metrics	AS	Sensors	CAS	JOOI	SJ	JCIS
Publisher	Springer	Mdpi.com	Mdpi.com	Elsevier	Mdpi.com and Elsevier	Springer	Taylor & Francis
First published	2015	2021	2019	2013	2020	2020	2023
Last published	2022	2023	2023	2023	2022	2023	2023
Scopus Indexed	Ya	Ya	Ya	Ya	Ya	Ya	Ya
Sinta Kemdikbud	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
Impact factor by Scopus	1,02	0,49	0,76	1,61	0,74	0,33	0,69

Berdasarkan tabel 1, tersedia 7 jurnal yang ter indeks scopus dengan Scientometrics diklasifikasikan di Q1. AS diklasifikasikan di Q2. Sensors diklasifikasikan di Q1, CAS diklasifikasikan di Q1. JOOI diklasifikasikan di Q1, SJ diklasifikasikan di Q2. JCIS diklasifikasikan di Q1 dalam hal ini juga penting untuk dijelaskan.

3. Informasi Jurnal Metrik

Dalam bagian ini, profil dan mebrik dari dua jurnal yang dipilih, Sensors, CAS, dan SJ, digambarkan. Tabel 2 menunjukkan beberapa hal penting yang harus diketahui dari tiga jurnal yang dipilih. Informasi metrik ini dikumpulkan dari metadata data melalui aplikasi Publish atau Perish (PoP) pada 10 November 2023.

Tabel 2. Informasi terpilih jurnal metrik

Metrics data	Sensors	CAS	SJ
Publication years	2019-2023	2013-2023	2020-2023
Citation years	4	10	3
Papers	21	11	6
Citations	620	420	33
Cites/year	155,00	42,00	11,00
Cites/paper	29,52	38,18	5,50
Authors/paper	166,62	144,22	21,92
h-index	12	7	3
g-index	21	11	5
hI,norm	7	6	3
hI,annual	1,75	0,60	1,00
hA-index	12	6	3

4. Manajemen Referensi

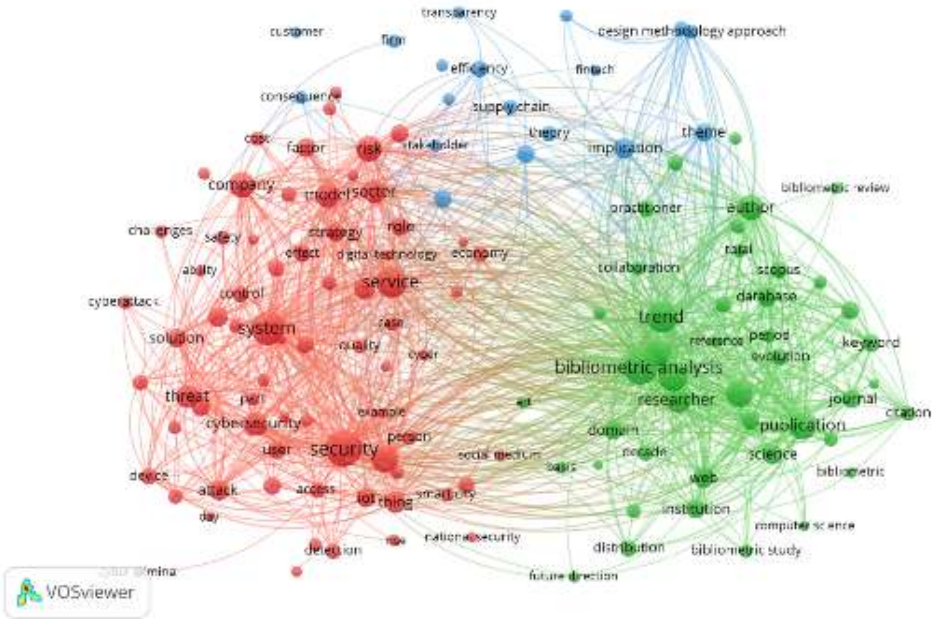
Setelah artikel diunduh dari dua situs jurnal, langkah berikutnya adalah mengatur referensi menggunakan aplikasi Mendeley. Ini memastikan bahwa metadata setiap artikel, yang mencakup informasi tentang penulis, kata kunci, dan detail lainnya, diatur dengan mudah dan lengkap.

5. Analisis Bibliometrik

Analisis bibliometrik dilakukan setelah metadata lengkap artikel dikonfirmasi. VosViewer, yang didasarkan pada file database, digunakan untuk menganalisis bibliometrik dalam artikel ini.csv yang didownload dari situs Google Scholar dengan kata kunci pencarian analisis biblometrik keamanan perusahaan penjualan online untuk mencegah terjadinya kejahatan siber.

HASIL DAN PEMBAHASAN

Tujuan pertama makalah ini adalah untuk menentukan bagaimana artikel analisis biblometrik keamanan perusahaan penjualan online untuk mencegah terjadinya kejahatan siber diklasifikasikan dari beberapa jurnal yang diunduh dari Google Scholar. Selanjutnya, saya menggunakan perangkat lunak VosViewer untuk melakukan analisis saya, membuat peta berdasarkan data teks menggunakan judul dan bidang abstrak, dan menemukan 14844 istilah dengan metode penghitungan biner. 237 ambang batas ditemukan dengan jumlah kejadian minimum dalam 20 kali waktu. Namun, untuk masing-masing 142 istilah, Skor relevansi dihitung, dan berdasarkan skor tersebut, istilah yang paling relevan secara otomatis dipilih sebanyak 60%. Sehingga, kita memperoleh 142 kata yang paling sesuai. Meskipun demikian, proses verifikasi tetap diperlukan secara manual dengan menghapus kata-kata seperti editorial, sampel, abstrak, dan lainnya yang tidak relevan. Dengan demikian, jumlah total kata yang dapat dimasukkan dalam pembuatan peta adalah sebanyak 133 kata.



Gambar 1. Jaringan kata kunci peta visualisasi

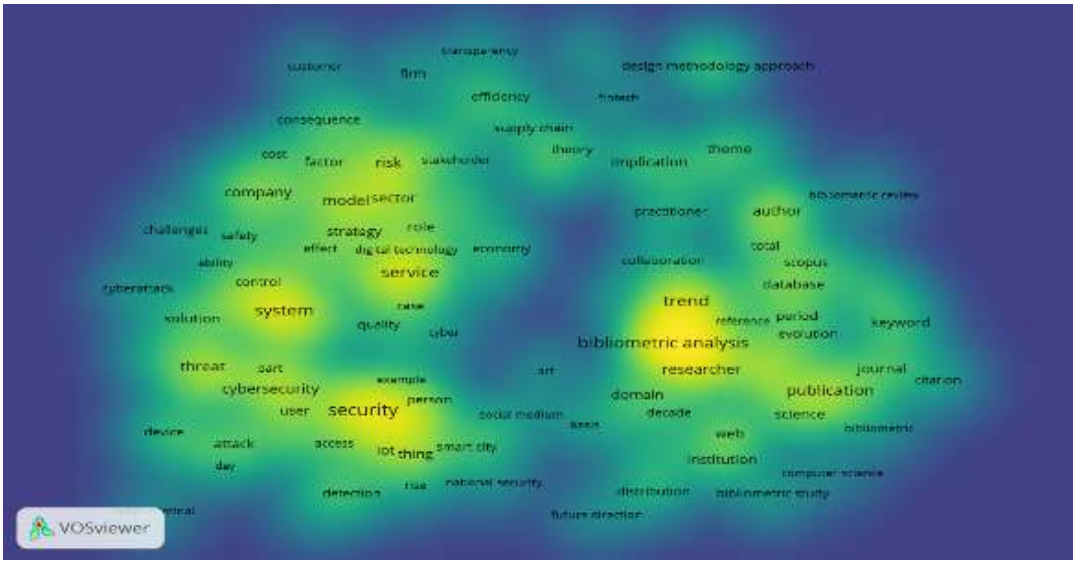
Gambar 1 menunjukkan beberapa kelompok yang diberi tanda biru merah dan hijau. Berdasarkan jumlah artikel yang diterbitkan, beberapa kata dalam kelompok tertentu muncul paling sering. Sembilan kategori artikel telah diterbitkan sejauh ini, seperti yang ditunjukkan dalam Tabel 3.

Tabel 3. Cluster dan kata kunci didalamnya

Cluster	Total items	Most frequent keywords (occurrences)	Keywords
1	71	Cyber (8) Security (6) Attack (3)	ability, access, adoption, attack ,case ,casestudy, challenges, chapter, cloud computing, company, complexity, computer, consumer, control, cost, covid, cyber, cyber attack, cyber criminal, cyber security, cyber threat, cyber attack, cyber crime, cyber security , data security, day, detection, device, digital technology, digitalization, e commerce, economy, effect, environment, example, factor, healthcare, individual, Information security, information technology, infrastructure, internet, iot, machine, metaverse, model ,national security, pandemic, part, person, product, quality, recomendation, rise, risk ,role, safety, sector, security, service, smart city, social medium, solution, strategy, system, survey, thing, threat, user, vulnerability, way
2	44	Bibliometric (4) Analysis (2) Science (2) Direction (2) Future (2)Research (4) database (2) trend (2)	art, author, basis, bibliometric, bibliometric analysis, bibliometric review, bibliometric study, citation, cluster, collaboration, computer science, content analysis, country, database, decade, distribution, document, domain, evolution, field, further research, future direction, future research, future research direction, india, institution, journal, keyword, period, practitioner, publication, reference, research area, research trend, researcher, scholar ,science, scopus, scopus database, topic, total, trend, vosviewer, web

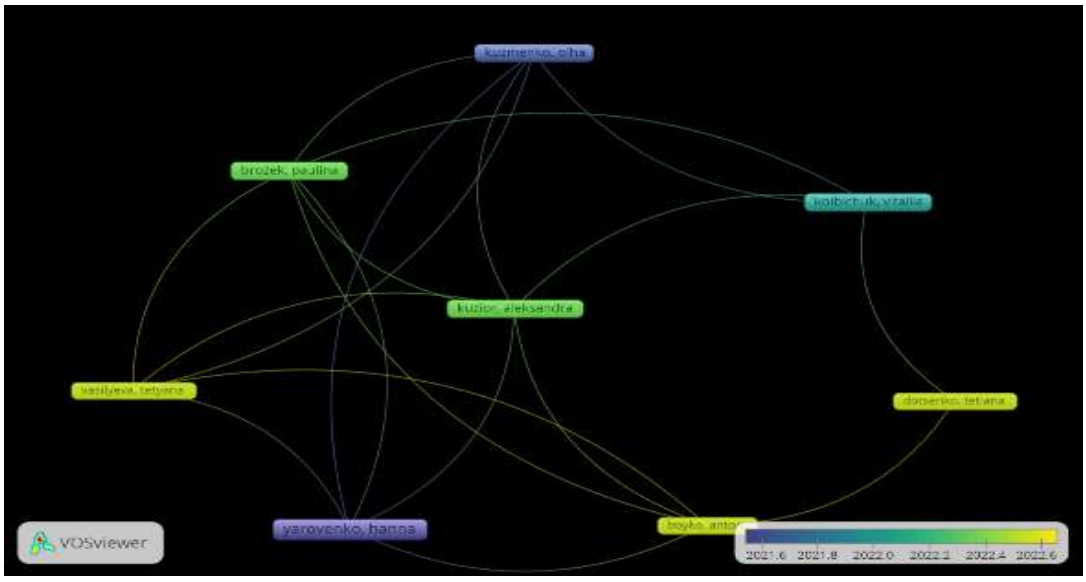
3	18	Implication (2)	blockchain technology, consequence, customer, design methodology approach, digital transformation, efficiency, fintech, firm, implementation, implication, originality value, practical implication, stakeholder, supply chain, theme, theory, transparency, trust

Kemudian kita dapat melihat jawaban sebenarnya dari cluster itu sendiri untuk menjawab tren analisis keamanan cyber dari kejahatan cyber. Gambar 2 menunjukkan cara untuk melihat kepadatan artikel. Kata-kata seperti cyber biblometrik dan keamanan sering muncul.



Gambar 2. Peta visualisasi kepadatan kata kunci

Cluster 1.2. dan 3 dari hasil pemetaan ini mencakup cyber, biblometrik, dan keamanan. Selain itu, beberapa kata jarang muncul dalam kata kunci seperti ilmu komputer, fintech, seni, dan arah masa depan. Artinya, masih ada ketidakseimbangan dalam penelitian yang mungkin menjadi tren di masa depan. Tentu saja, ini akan disesuaikan dengan keadaan dunia saat ini dan masa depan. dari perspektif para peneliti, seperti yang ditunjukkan pada Gambar 3.



Gambar 3. Peta visualisasi jaringan penulis

Gambar 3 menunjukkan bahwa masing-masing cluster memiliki lima nama besar, yang masing-masing ditunjukkan dengan titik besar. Hanya penulis yang terkait dalam publikasi mereka yang ditampilkan yang dapat dilihat pada gambar; warna biru menunjukkan tahun peneliti menerbitkan artikel terlama (2021), dan warna kuning menunjukkan tahun peneliti menerbitkan artikel terbaru.

KESIMPULAN

Studi ini melihat 68 artikel yang membahas analisis biblometrik dari jurnal jurnal yang terindeks scopus. Scientometrics, Applied Sciences (AS), Sensors, Computers, & Security (CAS), Journal of Open Innovation (JOOI), Security Journal (SJ), dan Journal of Computer Information Systems (JCIS) adalah sumber artikel ini. Dalam penelitian ini, kami menemukan bahwa jurnal analisis di atas memiliki pengaruh yang lebih besar di bidang cyber scurity daripada cyber crime saat ini. Ini karena analisis cyber scurity dari cyber crime dapat digunakan sebagai subjek artikel.

SARAN

Studi saat ini setidaknya memiliki dua keterbatasan. Pertama, studi ini sebagian besarhanya terbatas pada jurnal yang ter-indeks dalam scopus, meskipun banyak jurnal diluar yangtidak ter-indeks scopus namun tidak menutup kemungkinan bahwa artikel yang diterbitkan tidak berkualitas, Studi-studi mendatang sebaiknya mempertimbangkan penggunaan sampel yanglebih luas dan melibatkan berbagai sumber, bahkan jika sumber-sumber tersebut tidak terindeks oleh Scopus, meskipun penilaian subjektif oleh penulis masih ada dan masih dapat menyebabkan pengenalan kesalahan, meskipun penelitian ini menggunakan alat formal seperti perangkat lunak PoP, Mendeley, dan VOSviewer.

DAFTAR PUSTAKA

Bossler, Adam M., and Tamar Berenblum. 2019. "Introduction: New Directions in *Cybercrime* Research." *Journal of Crime and Justice* 42(5): 495–99. https://doi.org/10.1080/0735648X.2019.1692426.

Desamsetti, Harshith. 2021. "Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenges." *American Journal of Trade and Policy* 8(3): 239–46.

Elisanti, Evi et al. 2024. "Analysis of *Cybercrime* Potential in E-Commerce Buying and Selling Transactions." 6(1): 163–80.

Furstenau, Leonardo Bertolin et al. 2020. "20 Years of Scientific Evolution of Cyber Security: A Science Mapping." *Proceedings of the International Conference on Industrial Engineering and Operations Management* 0(March): 314–25.

Irfan, Muhammad, Mairisa Elvia, and Shaquila Dania. 2023. "Ancaman *Cybercrime* Dan Peran Cybersecurity Pada E-Commerce: Systematic Literature Review." *Jursima* 11(1): 110–21.

Istanbullu, Aslihan. 2023. "How Should I Start Research in Cyber Security? Suggestions for Researchers According to Bibliometric Analysis Data." *Sakarya University Journal of Education* 13(1): 119–39. https://dergipark.org.tr/en/pub/suje/issue/76975/1219710.

Kwarto, Febrian, and Madya Angsito. 2018. "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan." *Jurnal Akuntansi Bisnis* 11(2): 99–110.

Liu, Xiang et al. 2022. "Cyber Security Threats: A Never-Ending Challenge for e-Commerce." *Frontiers in Psychology* 13(October): 1–15.

Mijwil, Maad M., Mohammad Aljanabi, and ChatGPT. 2023. "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime." *Iraqi Journal for Computer Science and Mathematics* 4(1): 65–70.

Nandiyanto, Asep Bayu Dani, and Dwi Fitria Al Husaeni. 2022. "Bibliometric Analysis of Engineering Research Using Vosviewer Indexed By Google Scholar." *Journal of Engineering Science and Technology* 17(2): 883–94.

Normah, Bakhtiar Rifai, Satrio Vambudi, and Rifki Maulana. 2022. "Analisa Sentimen Perkembangan Vtuber Dengan Metode Support Vector Machine Berbasis SMOTE." *Jurnal Teknik Komputer AMIK BSI* 8(2): 174–80. https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/13041/pdf.

Nursari, Sri Rezeki Candra, and Yossela Immanuel. 2018. "Perancangan Sistem Informasi Penjualan Online." *CCIT Journal* 11(1): 102–14.

Romdoni, Mochamad Yusuf, Irma Yunita Ruhiawati, and Waliadi Gunawan. 2022. "Perancangan Aplikasi Rental Mobil Travel Desktop Pada Perusahaan Tirtayasa Trans." *Jurnal Sistem Informasi dan Informatika (Simika)* 5(2): 133–42.

Sharma, Deepak et al. 2023. "A Bibliometric Analysis of Cyber Security and Cyber Forensics Research." *Results in Control and Optimization* 10. https://www.sciencedirect.com/science/article/pii/S2666720723000061.

Srisadono, Wahyu. 2018. "Strategi Perusahaan E-Commerce Membangun Brand Community Di Media Sosial Dalam Meningkatkan Omset Penjualan." *Jurnal Pustaka Komunikasi* 1(1): 167–79.

Yildiz, Bülent, and Elham Hasan Younes Gejam. 2022. "Cyber-Physical Systems and Cyber Security: A Bibliometric Analysis." *OPUS Toplum Araştırmaları Dergisi* 19(45): 35–49.