Jurnal Inovasi Informatika (JII)

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

Analisis Bibliometrik Manajemen Risiko Serangan Siber Menggunakan Tableau dan Vosviewer

BIBLIOMETRIC ANALYSIS OF CYBER ATTACK RISK MANAGEMENT USING TABLEAU AND VOSVIEWER

Steven Dermawan[1)*]

[1] Sistem Informasi, Universitas Pradita, Tangerang, Indonesia, steven.dermawan@student.pradita.ac.id
*email korespondensi: steven.dermawan@student.pradita.ac.id

Abstrak

Meningkatnya kompleksitas ekosistem digital modern telah meningkatkan urgensi untuk melakukan kajian komprehensif mengenai Cyberattack Risk Management sebagai fondasi utama dalam membangun ketahanan siber. Penelitian ini menggunakan metode bibliometrik dengan dukungan VOSviewer dan Tableau untuk memetakan tren publikasi, jaringan sitasi, serta distribusi kata kunci selama periode 2020–2025. Metodologi penelitian mencakup proses pengumpulan dan pengolahan data, analisis menggunakan VOSviewer dan Tableau, serta interpretasi hasil analisis. Temuan penelitian menunjukkan adanya pertumbuhan publikasi yang konsisten, dominasi repositori ilmiah seperti arXiv dan Lecture Notes in Computer Science, serta keberadaan artikel-artikel berpengaruh yang membentuk struktur intelektual bidang ini, khususnya terkait dengan pemanfaatan data telemetri IoT dan perlindungan infrastruktur kritis. Pemetaan co-occurence mengungkapkan tiga klaster utama, yakni tata kelola dan kebijakan, pendekatan teknis, serta perlindungan data, sementara visualisasi kepadatan menunjukkan beberapa topik yang masih kurang dieksplorasi, termasuk smart grid, sektor kesehatan, perangkat IoT, dan isu privasi. Temuan ini menunjukkan adanya pergeseran dalam perkembangan pengetahuan menuju integrasi antara tata kelola risiko dan inovasi teknologi yang lebih adaptif. Lebih lanjut, meningkatnya minat terhadap pemodelan prediktif dan keamanan berbasis kecerdasan buatan (AI) mengindikasikan transformasi pendekatan dari deteksi yang bersifat reaktif menuju mitigasi yang lebih proaktif. Secara keseluruhan, penelitian ini menyajikan peta konseptual yang komprehensif untuk memperkuat arah penelitian di masa depan, pengembangan teknologi, serta perumusan kebijakan di bidang keamanan siber.

Kata kunci: Manajemen Risiko Serangan Siber; Bibliometrik; VOSviewer; Keamanan IoT; Ketahanan Siber.

Abstract

The increasing complexity of the modern digital ecosystem has heightened the urgency for a comprehensive study of Cyberattack Risk Management as a fundamental foundation for cyber resilience. This study employs a bibliometric method supported by VOSviewer and Tableau to map publication trends, citation networks, and keyword distributions over the 2020–2025 period. The research methodology includes data collection and processing, analysis using VOSviewer and Tableau, and interpretation of the results. The findings indicate a consistent growth in publications, the dominance of scientific repositories such as arXiv and Lecture Notes in Computer Science, as well as the presence of influential articles that shape the intellectual structure of the discipline, particularly regarding the utilization of IoT telemetry data and the protection of critical infrastructure. The co-occurrence mapping reveals three main clusters: governance and policy, technical approaches, and data protection, while the density visualization highlights several underexplored topics, including smart grids, the

healthcare sector, IoT devices, and privacy issues. These findings demonstrate a shift in the development of knowledge toward the integration of risk governance and more adaptive technological innovation. Furthermore, the growing interest in predictive modeling and AI-driven security indicates a transformation in approaches from reactive detection to proactive mitigation. Overall, this study presents a comprehensive conceptual map to strengthen future research directions, technological development, and cybersecurity policy formulation.

Keywords: Cyberattack Risk Management; Bibliometric; VOSviewer; IoT Security; Cyber Resilience.

Article history: Received 1 December 2025, Accepted 22 December 2025, Available online 30 April 2026

1 PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat dalam dua dekade terakhir telah membawa perubahan signifikan pada berbagai sektor kehidupan, mulai dari pemerintahan, bisnis, pendidikan, hingga layanan publik (Sangaji & Irianto, 2025). Transformasi digital yang terjadi secara masif mendorong efisiensi, kecepatan, dan kemudahan akses terhadap data serta informasi. Namun, di balik kemajuan tersebut, muncul pula tantangan besar berupa meningkatnya ancaman terhadap keamanan siber (Alfi, Yundari, & Tsaqif, 2023). Serangan siber (*cyber attack*s) kini menjadi salah satu risiko utama yang dihadapi organisasi di seluruh dunia, dengan potensi kerugian finansial, reputasi, dan operasional yang sangat besar (Syawaluddin, Putra, & Putra, 2025).

Dalam konteks ini, manajemen risiko keamanan siber menjadi aspek yang krusial. Manajemen risiko tidak hanya berfungsi sebagai mekanisme pertahanan teknis, tetapi juga sebagai strategi menyeluruh untuk mengidentifikasi, menganalisis, dan mengendalikan risiko yang dapat mengancam aset digital organisasi (Muliati, Supriadi, & Junaedi, 2025). Seiring meningkatnya kompleksitas ancaman siber, mulai dari ransomware, phishing, hingga serangan berbasis kecerdasan buatan, pendekatan sistematis dalam memahami tren dan arah penelitian di bidang manajemen risiko siber menjadi semakin penting (Sitorus, Maria, & Safa, 2024).

Untuk memperoleh pemahaman yang komprehensif mengenai perkembangan penelitian dalam bidang ini, pendekatan bibliometrik digunakan sebagai alat analisis yang efektif. Analisis bibliometrik memungkinkan peneliti untuk memetakan struktur pengetahuan, mengidentifikasi topik penelitian yang sedang berkembang, serta melihat pola kolaborasi antarpeneliti dan institusi (Pratama & Setiawan, 2024). Dengan demikian, analisis ini dapat memberikan gambaran evolusi dan arah masa depan penelitian manajemen risiko keamanan siber.

Dalam beberapa tahun terakhir, berbagai perangkat lunak telah dikembangkan untuk mendukung analisis bibliometrik, di antaranya VOSviewer dan Tableau. VOSviewer berperan penting dalam memvisualisasikan jaringan kata kunci, hubungan antarpenulis, serta kluster penelitian yang terbentuk dari publikasi ilmiah (Nurul & Winoto, 2022). Sementara itu, Tableau digunakan untuk mengolah dan menampilkan data bibliometrik secara interaktif

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

melalui visualisasi yang informatif dan mudah dipahami. Kombinasi kedua alat ini memberikan pendekatan yang komprehensif dalam menelusuri dan menginterpretasikan dinamika penelitian.

2 TINJAUAN PUSTAKA

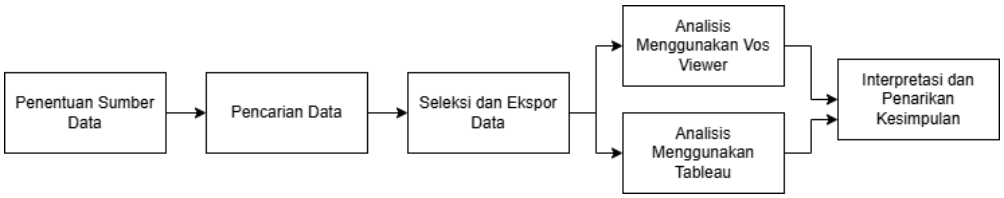
Penelitian ini merujuk kepada beberapa penelitian terdahulu yang terkait dengan bibliometrik. Pertama, penelitian Nazara, Fitriana, & Santoso (2024) terkait topik forensik audit menggunakan vosviewer pada tahun 2013-2022 dalam database scopus. Penelitian menunjukkan tren fluktuatif publikasi forensik audit dengan puncak pada 2016, terendah pada 2022, mencakup 9 klaster dan 58 kata kunci. Kedua, penelitian Karim, Soebagyo, Nuranti, & Uljanah (2021) terkait tren riset matematika terapan di Google Scholar pada tahun 2005-2021. Penelitian menunjukkan tren peningkatan fluktuatif dengan publikasi terbanyak di Elsevier, yang terbagi dalam 5 kluster.

Ketiga, penelitian Ernando & Atmojo (2024) terkait implementasi erp dalam organisasi pada tahun 2019-2023 di database dimension. Penelitian menunjukkan dari tahun 2019 sampai dengan 2023 tren penelitian terkait ERP terus mengalami peningkatan. Kata kunci terbanyak adalah humans. Keempat, penelitian Qorahman & Akbar (2024) terkait kebijakan keamanan siber pada tahun 2020-2023 di database google scholar. Penelitian menunjukkan tren naik dan turun publikasi. Penelitian terdiri dari enam kluster.

Kelima, penelitian Mulyana & Maha (2021) terkait kolaborasi dan distribusi penulis jurnal BACA pada tahun 2009-2019. Selain menggunakan vosviewer, peneliti menggunakan tableau. Penelitian menunjukkan fluktuasi publikasi dengan puncak pada tahun 2019. Penelitian terdiri dari 5 kluster.

Berdasarkan uraian penelitian terdahulu tersebut, dapat disimpulkan bahwa analisis bibliometrik telah banyak diterapkan untuk memetakan tren publikasi dan kluster tematik pada berbagai bidang kajian. Namun, kajian yang secara khusus memfokuskan pada manajemen risiko serangan siber melalui kombinasi Tableau dan VOSviewer masih relatif terbatas. Oleh karena itu, penelitian ini bertujuan untuk melakukan analisis bibliometrik terhadap publikasi ilmiah terkait manajemen risiko serangan siber guna mengidentifikasi tren penelitian global, artikel dan jurnal yang paling berpengaruh, serta tema-tema riset yang dominan dan prospektif dalam bidang keamanan siber. Hasil penelitian ini diharapkan mampu memperjelas posisi dan kontribusi kajian manajemen risiko serangan siber di antara studi bibliometrik keamanan siber yang telah ada, sekaligus menjadi referensi strategis bagi akademisi, praktisi, dan pembuat kebijakan dalam merumuskan kebijakan serta strategi mitigasi risiko siber yang lebih efektif di masa mendatang.

3 METODE PENELITIAN



Gambar 1. Metodologi Penelitian

Penelitian ini menggunakan pendekatan bibliometrik dengan bantuan perangkat lunak VOSviewer dan Tableau untuk menganalisis perkembangan riset mengenai *Cyber Attack Risk Management*. Data penelitian diperoleh dari database Dimensions. Tahapan penelitian ditampilkan pada Gambar 1, dengan alur pelaksanaan sebagai berikut:

3.1 Penentuan Sumber Data

Peneliti menggunakan Dimensions database sebagai sumber data utama karena memiliki cakupan publikasi yang luas, fitur sitasi yang terperinci, serta kemudahan dalam ekspor data bibliometrik.

3.2 Pencarian Data

Proses pencarian dilakukan menggunakan kata kunci "*Cyber Attack Risk Management*" dengan rentang tahun publikasi 2020–2025. Dari hasil pencarian, diperoleh sebanyak 1.897 publikasi yang relevan dengan topik penelitian.

3.3 Seleksi dan Ekspor Data

Seluruh jenis publikasi yang relevan, termasuk artikel jurnal, prosiding, dan review article**,** disertakan dalam analisis untuk memperoleh gambaran menyeluruh tentang perkembangan penelitian di bidang manajemen risiko serangan siber. Data hasil pencarian kemudian diekspor dalam format CSV untuk dianalisis lebih lanjut.

3.4 Analisis Menggunakan Vos Viewer

Data CSV diimpor ke perangkat lunak VOSviewer (versi 1.6.18) untuk melakukan analisis bibliometrik, meliputi:

- Analisis co-*occurrence*: mengidentifikasi kata kunci yang paling sering muncul serta keterkaitannya satu sama lain.

Hasil visualisasi berupa peta jaringan (network *visualization*), di mana ukuran lingkaran menunjukkan frekuensi kemunculan atau tingkat pengaruh suatu kata kunci.

3.5 Analisis Menggunakan Tableau

Data CSV juga kemudian diimpor ke Tableau dan diolah untuk menampilkan hasil dalam bentuk visualisasi interaktif. Analisis yang dilakukan meliputi:

- Tren publikasi tahunan untuk melihat perkembangan riset dari tahun 2020 hingga 2025.
- Distribusi jurnal dengan jumlah publikasi terbanyak.

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

- Artikel dengan sitasi tertinggi untuk mengidentifikasi karya yang paling banyak disitasi.

3.6 Interpretasi dan Penarikan Kesimpulan

Seluruh hasil analisis kemudian diinterpretasikan untuk mengetahui:

- Topik penelitian yang paling dominan dan berkembang dalam bidang manajemen risiko serangan siber.
- Jurnal dan artikel yang paling berpengaruh.
- Arah tren riset di masa mendatang.

4 HASIL DAN PEMBAHASAN

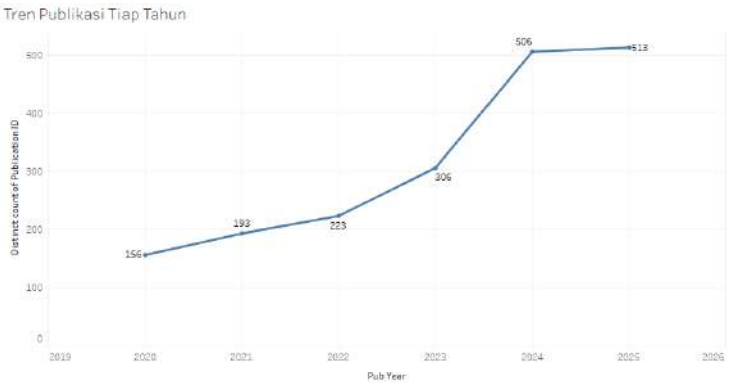
Berdasarkan hasil penelusuran data pada database Dimensions, menggunakan kata kunci "*Cyber Attack Risk Management*", didapati uraian pembahasan pertanyaan riset sebagai berikut.

4.1 Trend riset terkait dengan *cyber attack Risk Management* dari tahun ke tahun

Diketahui bahwa penelitian dengan topik tersebut mengalami peningkatan yang konsisten sepanjang periode 2020–2025. Tren perkembangan riset pada bidang ini menunjukkan pertumbuhan yang signifikan sejak awal tahun 2020, sebagaimana ditampilkan pada Tabel 1 dan Gambar 2.

Tabel 1. Perkembangan Publikasi Penelitian Berdasarkan Tahun

Tahun Publikasi	Jumlah
2020	156
2021	193
2022	223
2023	306
2024	506
2025	513



Gambar 2. Grafik Perkembangan Publikasi Penelitian Berdasarkan Tahun

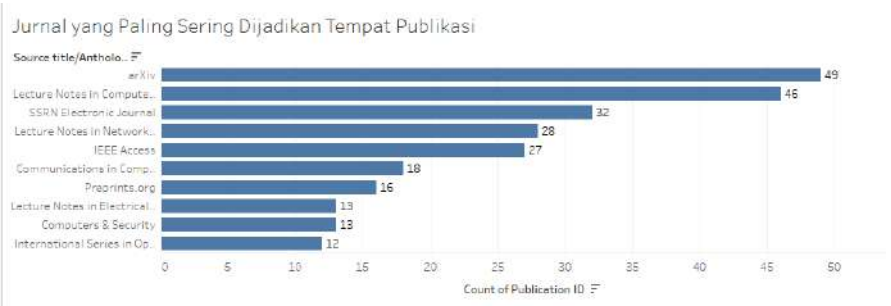
Berdasarkan Tabel 1 dan Gambar 2, terlihat bahwa publikasi penelitian dengan kata kunci "*Cyber Attack Risk Management*" mengalami tren peningkatan yang cukup konsisten selama periode 2020 hingga 2025. Pada awal periode tahun 2020 tercatat sebanyak 156 publikasi, kemudian meningkat menjadi 193 publikasi pada tahun 2021 dan 223 publikasi pada tahun 2022. Kenaikan yang lebih signifikan terjadi pada tahun 2023 dengan 306 publikasi, dan mencapai puncaknya pada tahun 2024 dengan 506 publikasi. Meskipun demikian, pada tahun 2025 jumlah publikasi hanya sedikit meningkat menjadi 513 publikasi, menunjukkan bahwa minat penelitian terhadap topik ini masih tinggi dan terus berkembang.

4.2 Jurnal terbanyak menjadi tempat publikasi

Berdasarkan hasil penelusuran pada database Dimensions, diperoleh peringkat sumber publikasi yang paling banyak menerbitkan artikel bertema *Cyber Attack Risk Management* selama periode penelitian. Seperti terlihat pada Gambar 3 dan Tabel 2, sumber publikasi yang menempati peringkat pertama adalah arXiv, dengan jumlah 49 artikel. Peringkat kedua ditempati oleh Lecture Notes in Computer Science dengan 46 artikel, diikuti oleh SSRN Electronic Journal sebanyak 32 artikel. Kemudian Lecture Notes in Networks and Systems menempati posisi keempat dengan 28 artikel, dan IEEE Access berada di posisi kelima dengan 27 artikel.

Tabel 2. Jurnal terbanyak menjadi tempat publikasi

Sumber Publikasi	Jumlah
arXiv	49
Lecture Notes in Computer Science	46
SSRN Electronic Journal	32
Lecture Notes in Networks and Systems	28
IEEE Access	27
Communications in Computer and Information Science	18
Preprints	16
Lecture Notes in Electrical Engineering	13
Computers & Security	13
International Series in Operations Research and Management Science	12



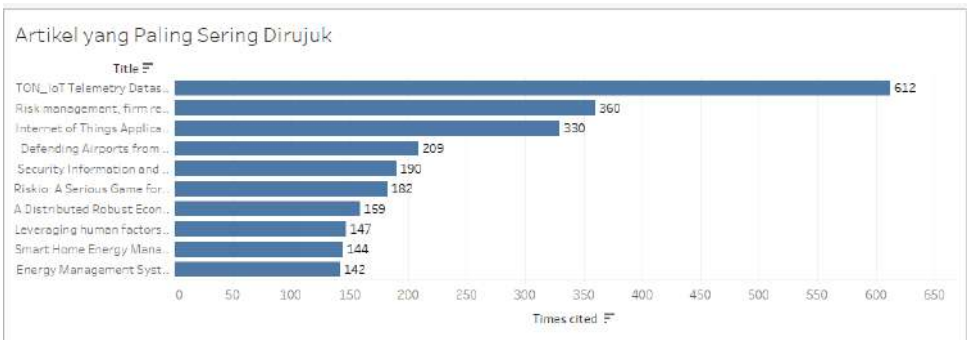
Gambar 3. Grafik jurnal terbanyak menjadi tempat publikasi

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

Hasil ini menunjukkan bahwa penelitian bertema *Cyber Attack Risk Management* banyak dipublikasikan pada repositori terbuka seperti arXiv dan platform prosiding bereputasi seperti Lecture Notes in Computer Science, yang sering menjadi wadah publikasi hasil penelitian di bidang keamanan siber dan manajemen risiko teknologi informasi.

4.3 Sepuluh artikel jurnal terbanyak yang dijadikan rujukan

Bagian ini menyajikan 10 artikel jurnal yang paling banyak dirujuk dalam penelitian manajemen risiko serangan siber. Pada Tabel 3, kolom "No" menunjukkan urutan peringkat berdasarkan jumlah sitasi, di mana No 1 merupakan artikel dengan sitasi tertinggi. Selain itu, Tabel 3 juga memuat analisis mengenai kontribusi utama masing-masing artikel terhadap pengembangan manajemen risiko siber. Adapun Gambar 4 menampilkan visualisasi tingkat sitasi tiap artikel.



Gambar 4. Grafik sepuluh artikel terbanyak yang dijadikan rujukan

Gambar 4 mengilustrasikan sepuluh artikel dengan frekuensi sitasi tertinggi dalam korpus penelitian manajemen risiko serangan siber. Terlihat bahwa artikel "TOL: IoT Telemetry Data…" menempati posisi paling dominan dengan 612 sitasi, menunjukkan bahwa topik pemanfaatan data telemetri IoT memiliki pengaruh signifikan dalam membentuk kerangka konseptual dan metodologis di bidang ini. Dua artikel berikutnya, "*Risk Management*, Firm…" (360 sitasi) dan "Internet of Things Applicat…" (330 sitasi), menegaskan kuatnya orientasi riset terhadap integrasi prinsip manajemen risiko konvensional dengan perkembangan teknologi IoT. Sementara itu, artikel-artikel lain dengan rentang sitasi 142 hingga 209 memberikan kontribusi terhadap isu keamanan infrastruktur kritis, pengolahan informasi keamanan, hingga pemanfaatan pendekatan simulatif dalam mengedukasi pemangku kepentingan terkait ancaman siber. Pola sitasi ini secara keseluruhan mengindikasikan bahwa literatur yang banyak digunakan dalam studi manajemen risiko siber berpusat pada kajian IoT, perlindungan aset strategis, dan pendekatan analitis berbasis teknologi, yang bersama-sama membentuk fondasi pengetahuan dalam disiplin ini.

Dengan melihat dominasi sitasi pada Gambar 4, dapat dipahami bahwa sepuluh artikel tersebut tidak hanya berperan sebagai rujukan paling berpengaruh, tetapi juga mencerminkan spektrum isu strategis yang menjadi fokus utama dalam manajemen risiko siber, mulai dari keamanan IoT, ketahanan infrastruktur kritis, hingga pendekatan berbasis analitik dan edukasi. Untuk memperjelas kontribusi konseptual maupun metodologis dari masing-masing artikel, Tabel 3 kemudian menyajikan uraian mendalam mengenai analisis utama serta relevansi setiap penelitian terhadap pengembangan kerangka manajemen risiko siber.

Tabel 3. Sepuluh artikel terbanyak yang dijadikan rujukan

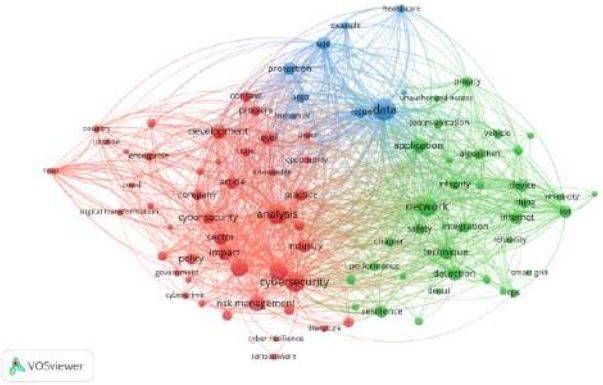
No	Analisis Utama dan Kontribusi terhadap Manajemen Risiko Siber
1	Penelitian ini mengembangkan dataset TON_IoT yang berisi data telemetri, log sistem operasi, dan lalu lintas jaringan IoT/IIoT untuk mendukung pelatihan dan evaluasi sistem deteksi intrusi berbasis *machine learning* dan *deep learning*. Kontribusinya terletak pada penyediaan benchmark dataset yang komprehensif dan representatif untuk meningkatkan efektivitas manajemen risiko siber pada ekosistem IoT (Alsaedi, Mustafa, Tari, Mahmood, & Anwar, 2020).
2	Penelitian ini mengembangkan model untuk menganalisis dampak serangan siber terhadap nilai perusahaan dan kebijakan manajemen risiko. Hasilnya menunjukkan bahwa serangan yang menyebabkan kebocoran data keuangan pribadi menimbulkan kerugian besar bagi pemegang saham, menurunkan pertumbuhan penjualan, serta mendorong perusahaan untuk memperkuat manajemen risiko dan mengurangi tingkat pengambilan risiko di masa mendatang (Kamiya, Jun-Koo, Jungmin, Milidonis, & Stulz, 2021).
3	Studi ini meninjau berbagai isu keamanan pada setiap lapisan IoT dengan fokus pada serangan *Distributed Denial of Service* (DDoS) serta membandingkan model *Intrusion Detection* and *Prevention System* untuk mitigasinya. Kontribusinya terletak pada penyajian klasifikasi sistem deteksi intrusi, teknik anomali, serta penerapan *machine learning* dan *deep learning* guna memperkuat manajemen risiko siber dan ketahanan keamanan IoT di masa depan (Mishra & Pandya, 2021).
4	Penelitian ini membahas peningkatan insiden drone di sekitar bandara serta meninjau berbagai teknologi sensor dan sistem Counter-Unmanned Aerial Systems (C-UAS) untuk mendeteksi, mengidentifikasi, dan menanggulangi ancaman tersebut. Kontribusinya terletak pada pengembangan rencana perlindungan dan ketahanan bagi infrastruktur bandara guna memperkuat manajemen risiko siber terhadap ancaman udara yang disebabkan oleh penyalahgunaan drone (Lykou, Moustakas, & Gritzalis, 2020).
5	Kajian ini menyoroti evolusi sistem Security Information and Event Management (SIEM) sebagai alat utama dalam pencegahan, deteksi, dan respons terhadap serangan siber, yang kini mulai terintegrasi dengan analitik big data. Kontribusinya terletak pada analisis fungsi utama, faktor eksternal, serta rekomendasi peningkatan generasi berikutnya dari SIEM untuk memperkuat manajemen risiko dan ketahanan keamanan infrastruktur kritis (González-Granadillo, González-Zarzosa, & Diaz, 2021).
6	Penelitian ini memperkenalkan Riskio, sebuah permainan edukatif berbasis papan yang dirancang untuk meningkatkan kesadaran keamanan siber bagi karyawan non-teknis melalui pembelajaran aktif tentang serangan dan pertahanan siber. Kontribusinya terletak pada pengembangan metode pelatihan interaktif yang mendukung strategi manajemen risiko siber organisasi dengan cara yang menarik dan efektif (Hart, Margheri, Paci, & Sassone, 2020).
7	Artikel ini membahas strategi *distributed robust economic dispatch* pada sistem energi terintegrasi (IES) untuk menghadapi risiko serangan siber melalui penerapan protokol perlindungan privasi dan mekanisme deteksi berbasis reputasi. Kontribusinya terletak pada pengembangan metode manajemen energi yang tangguh terhadap serangan terkoordinasi maupun independen, sekaligus menjaga keandalan transmisi informasi dan stabilitas operasional sistem energi (Huang, Li, Zhan, Sun, & Zhang, 2022).

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

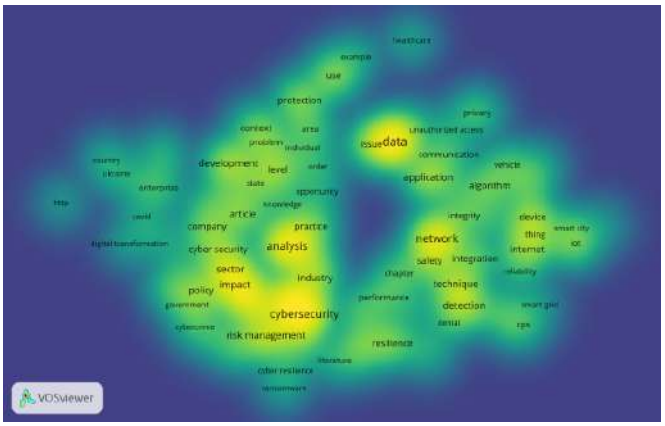
8	Studi ini mengusulkan pendekatan *Human Factors* (HF) yang holistik dalam manajemen keamanan siber, dengan menyoroti peran faktor individu, organisasi, dan teknologi di sektor kesehatan. Kontribusinya terletak pada integrasi solusi teknis dan non-teknis, seperti peningkatan kesadaran pengguna, untuk membangun budaya keamanan siber yang lebih matang dan efektif dalam mengurangi kerentanan manusia terhadap ancaman siber (Pollini et al., 2022).
9	Penelitian ini menganalisis *Smart Home Energy Management Systems* (SHEMs) sebagai solusi pengelolaan energi rumah pintar yang efisien, namun menemukan tantangan utama terkait keamanan, privasi, dan interoperabilitas sistem. Kontribusinya terletak pada identifikasi risiko siber dalam sistem rumah pintar serta rekomendasi peningkatan atribut keamanan untuk mencegah serangan siber dan menjaga kenyamanan serta kesehatan penghuni (Aliero, Qureshi, Pasha, & Jeon, 2021).
10	Penelitian ini meninjau integrasi energi terbarukan dalam sistem microgrid (MG) yang dapat meningkatkan efisiensi dan keandalan energi, namun juga menimbulkan risiko terhadap stabilitas dan keamanan siber sistem tenaga. Kontribusinya terletak pada pengembangan strategi manajemen energi dan kebijakan perlindungan MG untuk meminimalkan dampak serangan siber serta meningkatkan kemampuan pemulihan sistem secara cepat (Zahraoui et al., 2021).

4.4 Pemetaan bibliometrik terkait penelitian

Kata kunci dalam literatur mengenai *Cyber Attack Risk Management* dianalisis menggunakan jaringan co-*occurrence* pada perangkat lunak VOSviewer. Gambar 5 menampilkan *Network visualization*, sedangkan Gambar 6 menunjukkan *Density Visualization*.



Gambar 5. Network *Visualization*



Gambar 6. Density *Visualization*

Pada tahap analisis ini, ambang batas minimum kemunculan (*occurrence*) kata kunci pada judul dan abstrak ditetapkan sebanyak 100 kali. Hasil pemetaan menunjukkan bahwa kata *data* (*occurrence*: 1318), *cybersecurity* (*occurrence*: 1097), *analysis* (*occurrence*: 1096), *network* (*occurrence*: 989), dan *strategy* (*occurrence*: 855) merupakan istilah yang paling sering muncul (lihat Gambar 5). Secara keseluruhan, analisis mengidentifikasi 41.954 kata kunci, dan sebanyak 149 kata memenuhi ambang batas sehingga dapat dikelompokkan ke dalam tiga kluster utama. Di antara seluruh kata tersebut, *data* muncul sebagai istilah paling dominan.

Melalui pendekatan co-*occurrence clustering*, diperoleh tiga kelompok besar dengan total 89 item. Ketiga kluster tersebut terdiri dari:.

- Cluster 1: Berisi kata kunci terkait konsep manajerial dan kebijakan, seperti *analysis, asset, business, company, cyber resilience, cyber risk, cybersecurity, digital transformation, enterprise, government, information security, organisation, policy, ransomware, risk assessment, risk management,* hingga *strategy*. Kluster ini mencerminkan fokus penelitian pada aspek tata kelola, kebijakan, serta strategi mitigasi risiko siber di berbagai sektor industri dan pemerintahan.
- Cluster 2: Mencakup istilah teknis dan teknologi pendukung, seperti *algorithm, application, attacker, blockchain, cloud, CPS, critical infrastructure, detection, IoT, machine learning, mitigation, network, privacy, resilience, smart city, smart grid, hingga unauthorized access*. Kluster ini menggambarkan orientasi penelitian pada pendekatan teknologi untuk mendeteksi, mencegah, dan merespons serangan siber.
- Cluster 3: Memuat istilah yang berkaitan dengan isu perlindungan data dan konteks pengguna, seperti *confidentiality*, data, *healthcare*, *issue*, *protection*, dan *use*.

Pada *density visualization*, setiap titik menunjukkan gradasi warna dari biru (rendah), hijau (sedang), hingga kuning (tinggi), yang menandakan tingkat intensitas kemunculan kata kunci. Berdasarkan pemetaan pada Gambar 6, terlihat bahwa beberapa topik masih berada di area berwarna biru hingga hijau, menandakan frekuensi pembahasan yang relatif lebih rendah. Topik tersebut antara lain *smart grid*, *healthcare*, *IoT devices*, serta isu terkait *privacy*.

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

Temuan ini mengindikasikan adanya sejumlah area penelitian yang masih kurang dieksplorasi dan berpotensi menjadi ruang pengembangan studi lanjutan, khususnya dalam konteks peningkatan ketahanan dan pengelolaan risiko serangan siber pada infrastruktur kritis dan sistem berbasis IoT. Selain itu, rendahnya intensitas pembahasan pada topik seperti *smart grid*, *healthcare*, *IoT devices*, dan isu privacy menegaskan bahwa penguatan aspek teknis serta tata kelola keamanan pada sektor-sektor tersebut menjadi semakin relevan.

Perkembangan teknologi digital yang semakin kompleks, ditambah dengan meningkatnya ketergantungan pada sistem terhubung (*interconnected* systems), mendorong urgensi penelitian yang tidak hanya berfokus pada mitigasi serangan, tetapi juga pada permodelan risiko, prediksi kerentanan, serta integrasi teknologi baru seperti *blockchain*, *zero-trust architecture*, dan *AI-driven threat intelligence*. Dengan demikian, celah penelitian yang teridentifikasi melalui visualisasi ini memberikan arah strategis bagi peneliti untuk mengembangkan pendekatan yang lebih komprehensif dan adaptif dalam memperkuat manajemen risiko serangan siber di masa depan.

Secara praktis, hasil pemetaan ini dapat dijadikan dasar oleh pembuat kebijakan untuk menyusun regulasi berbasis risiko yang secara eksplisit mewajibkan penerapan standar keamanan siber minimum, audit keamanan berkala, serta mekanisme perlindungan data dan privasi yang ketat pada sektor *smart grid*, layanan kesehatan digital, dan ekosistem IoT. Bagi industri, temuan ini memberikan acuan konkret dalam menentukan prioritas investasi pada arsitektur keamanan seperti *zero-trust*, deteksi anomali berbasis AI, dan integrasi *blockchain* guna meningkatkan ketahanan operasional sistem serta meminimalkan dampak gangguan layanan dan kebocoran data.

5 KESIMPULAN

Hasil analisis bibliometrik terhadap penelitian bertema *Cyber Attack Risk Management* menunjukkan bahwa perkembangan literatur pada periode 2020–2025 mengalami peningkatan signifikan, baik dari segi volume publikasi, preferensi outlet publikasi, maupun struktur intelektual yang membentuk disiplin ini. Tren pertumbuhan publikasi yang konsisten, dominasi repositori terbuka seperti arXiv dan prosiding bereputasi seperti Lecture Notes in Computer Science, serta identifikasi artikel-artikel paling berpengaruh menegaskan bahwa lanskap penelitian ini sangat dinamis dan terus berkembang seiring meningkatnya kompleksitas ancaman siber. Analisis co-*occurrence* mengungkapkan tiga kluster pengetahuan utama, tata kelola dan kebijakan, pendekatan teknis dan teknologi pendukung, serta isu perlindungan data, yang membentuk kerangka epistemik penelitian manajemen risiko siber. Peta *density visualisation* juga memperlihatkan adanya area penting yang masih

kurang dieksplorasi, seperti *smart grid*, *healthcare*, *IoT devices*, dan isu *privacy*, sehingga memberikan gambaran yang lebih komprehensif mengenai arah perkembangan disiplin ini.

Berdasarkan temuan penelitian, diperlukan studi lanjutan untuk memperdalam kajian pada area-area yang masih memiliki tingkat densitas penelitian yang relatif rendah, khususnya pada sektor dengan tingkat risiko tinggi seperti layanan kesehatan, infrastruktur energi cerdas, serta ekosistem *Internet of Things* (IoT) yang terus berkembang. Seiring meningkatnya keterhubungan sistem digital, integrasi pendekatan mutakhir seperti *AI-driven threat intelligence, zero-trust architecture*, dan pemanfaatan *blockchain* dalam permodelan risiko siber menjadi semakin relevan guna memperkuat ketahanan sistem yang bersifat *interconnected*. Selain itu, penelitian komparatif lintas industri, pengembangan model prediktif kerentanan berbasis pembelajaran mesin, serta evaluasi efektivitas kebijakan dan tata kelola manajemen risiko siber di berbagai yurisdiksi perlu dikembangkan agar kontribusi literatur tidak hanya bertambah secara kuantitatif, tetapi juga memberikan nilai strategis dan substantif dalam menghadapi tantangan keamanan siber di masa depan.

Meskipun demikian, penelitian ini memiliki keterbatasan karena analisis bibliometrik hanya menggunakan satu database, yaitu Dimensions. Kondisi tersebut berpotensi membatasi cakupan publikasi yang dianalisis dan belum sepenuhnya merepresentasikan perkembangan penelitian secara global. Oleh karena itu, penelitian selanjutnya disarankan untuk memanfaatkan database lain seperti Scopus dan Google Scholar. Selain itu, perlu dilakukan perluasan dan variasi kata kunci pencarian guna meningkatkan kelengkapan data serta menghasilkan pemetaan penelitian yang lebih komprehensif dan representatif.

DAFTAR PUSTAKA

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5. https://doi.org/10.7454/jkskn.v6i2.10082

Aliero, M. S., Qureshi, K. N., Pasha, M. F., & Jeon, G. (2021). Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services. *Environmental Technology & Innovation*, *22*, 101443. https://doi.org/https://doi.org/10.1016/j.eti.2021.101443

Alsaedi, A., Mustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON _ IoT Telemetry Dataset : A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access*, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862

Ernando, R., & Atmojo, W. T. (2024). ANALISIS BIBLIOMETRIC DALAM IMPLEMENTASI ERP SEBUAH ORGANISASI. *Jurnal Tikomsin*, *12*(2), 1–7.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures.

Vol. 08 (10), April 2026: Hal 9-22
DOI: http://doi.org/10.51170/jii.v8i1.333
e-ISSN: 2686-1615

Sensors, *21*, 4759.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio : A Serious Game for Cyber Security Awareness and Education. *Computers and Security*, *95*, 101827.

Huang, B., Li, Y., Zhan, F., Sun, Q., & Zhang, H. (2022). A Distributed Robust Economic Dispatch Strategy for Integrated Energy System Considering Cyber-Attacks. *IEEE Transactions on Industrial Informatics*, *18*(2), 880–890. https://doi.org/10.1109/TII.2021.3077509

Kamiya, S., Jun-Koo, K., Jungmin, K., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/https://doi.org/10.1016/j.jfineco.2019.05.019

Karim, A., Soebagyo, J., Nuranti, R. P., & Uljanah, A. L. (2021). Analisis Bibliometrik Menggunakan Vosviewer Terhadap Trend Riset Matematika Terapan Di Google Scholar. *Jurnal Riset Pendidikan Matematika Jakarta*, *3*(2), 23–33.

Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors*, *20*, 1–40.

Mishra, N., & Pandya, S. (2021). Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. *IEEE Access*, *9*, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408

Muliati, S. F., Supriadi, F., & Junaedi, D. I. (2025). Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur. *Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro Dan Informatika*, *3*(2), 27–39.

Mulyana, S., & Maha, R. N. (2021). ANALISIS BIBLIOMETRIK KOLABORASI PENULIS DAN TREN PUBLIKASI PENELITIAN PADA JURNAL BACA 2009-2019. *BIBLIOTIKA : Jurnal Kajian Perpustakaan Dan Informasi*, *5*(2), 105–113.

Nazara, D. S., Fitriana, F., & Santoso, R. A. (2024). Analisis Bibliometrik Dengan Vosviewer Terhadap Perkembangan Penelitian Forensic Audit. *Jurnal Sains Dan Teknologi*, *5*(3), 714–719.

Nurul, F., & Winoto, Y. (2022). Pemetaan bibliometrik terhadap perkembangan penelitian dengan topik arsitektur informasi pada Google scholar menggunakan Vosviewer. *Informatio: Journal of Library and Information Science*, *2*(1), 43–60.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity : an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pratama, R. A., & Setiawan, A. (2024). ANALISIS BIBLIOMETRIK PERKEMBANGAN

PENELITIAN DIGITAL GOVERNANCE. *JURNAL TRIAS POLITIKA*, *8*(2), 306–328.

Qorahman, O., & Akbar, N. N. (2024). A bibliometric analysis of the of cybersecurity policy research. *Informatio: Journal of Library and Information Science*, *4*(1), 65–78.

Sangaji, M. S. J., & Irianto, J. (2025). Transformasi Inovasi Pelayanan Publik menuju Pemerintahan Digital. *Jurnal Jejaring Administrasi Publik*, *17*(1), 54–70. https://doi.org/10.20473/jap.v17i1.72708

Sitorus, M. G. B., Maria, N., & Safa, Y. N. (2024). Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman. *Jurnal Manajemen Informatika*, *14*(2), 187–198.

Syawaluddin, A. S., Putra, A. F., & Putra, M. (2025). CYBER SECURITY DAN KETAHANAN NASIONAL : TANTANGAN DAN SOLUSI DI ERA DIGITAL. *JURNAL MEDIA AKADEMIK*, *3*(6), 1–11.

Zahraoui, Y., Alhamrouni, I., Mekhilef, S., Khan, M. R. B., Seyedmahmoudian, M., Stojcevski, A., & Horan, B. (2021). Energy Management System in Microgrids : A Comprehensive Review. *Sustainability*, *13*, 10492.

Kutipan Artikel

Steven Dermawan (2026), *Analisis Bibliometrik Manajemen Risiko Serangan Siber Menggunakan Tableau dan Vosviewer*, JII, Vol: 08, No: 01, Hal: 9-22: April. DOI: http://doi.org/10.51170/jii.v8i1.333