Jurnal Multidisiplin West Science
Vol. 04, No. 05, Mei 2025, pp. 521-531

Analisis Bibliometrik tentang Keamanan siber dalam Ekosistem Keuangan

Loso Judijanto[1], Rival Pahrijal[2], Salwa Aulia Novitasari[3]
[1] IPOSS Jakarta, Indonesia dan losojudijantobumn@gmail.com
[2] Universitas Nusa Putra dan rivalpahrijal@gmail.com
[3] Universitas Nusa Putra dan salwa.auln12@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk memetakan perkembangan literatur ilmiah mengenai keamanan siber dalam ekosistem keuangan melalui pendekatan analisis bibliometrik. Data diambil dari database Scopus dengan rentang waktu tahun 2000–2024 dan dianalisis menggunakan perangkat lunak VOSviewer. Hasil analisis menunjukkan bahwa topik "cybersecurity" menjadi pusat perhatian utama, dengan keterkaitan erat terhadap tema seperti manajemen risiko, serangan siber, kecerdasan buatan, dan teknologi blockchain. Evolusi temporal mengindikasikan pergeseran fokus penelitian dari pendekatan manajerial menuju penerapan teknologi canggih, khususnya machine learning dan deteksi anomali. Selain itu, jaringan kolaborasi penulis menunjukkan dominasi oleh peneliti dari Asia Timur, namun juga membuka peluang kolaborasi lintas kawasan. Temuan ini memberikan gambaran menyeluruh tentang struktur dan tren penelitian keamanan siber serta arah pengembangan ke depan dalam sektor keuangan digital.

Kata Kunci: *Keamanan Siber, Ekosistem Keuangan, Machine Learning, Analisis, Bibliometrik*

ABSTRACT

This study aims to map the development of scientific literature on cybersecurity in the financial ecosystem using a bibliometric analysis approach. Data were retrieved from the Scopus database for the period 2000–2024 and analyzed using VOSviewer software. The results reveal that "cybersecurity" is the central focus, closely related to themes such as risk management, cyber attacks, artificial intelligence, and blockchain technology. Temporal evolution indicates a shift in research focus from managerial approaches toward advanced technological applications, particularly machine learning and anomaly detection. Furthermore, the co-authorship network shows dominance by researchers from East Asia, while also highlighting potential for cross-regional collaboration. These findings provide a comprehensive overview of the research structure and trends in cybersecurity and suggest future directions in the development of secure digital financial ecosystems.

Keywords: *Cybersecurity, Financial Ecosystem, Machine Learning, Analysis, Bibliometric*

PENDAHULUAN

Dalam era digital yang semakin terhubung, sektor keuangan menjadi salah satu industri yang paling terdampak oleh transformasi teknologi. Perkembangan teknologi informasi telah memfasilitasi efisiensi operasional, inovasi produk, dan perluasan akses layanan keuangan (Putra et al., 2024; Santoso, 2023). Namun, di balik kemajuan tersebut, muncul tantangan baru dalam bentuk risiko keamanan siber yang semakin kompleks dan merugikan. Ancaman siber terhadap lembaga keuangan tidak hanya bersifat teknis, tetapi juga berdampak sistemik terhadap stabilitas ekonomi dan kepercayaan publik. Berdasarkan laporan dari IMF, kerugian global akibat serangan siber pada sektor keuangan diperkirakan mencapai miliaran dolar setiap tahunnya, menjadikannya salah satu isu krusial dalam tata kelola industri keuangan modern (Napu et al., 2024).

Keamanan siber dalam ekosistem keuangan tidak lagi menjadi isu marginal, melainkan telah menjadi perhatian utama regulator, pelaku industri, dan akademisi. Ancaman seperti malware, ransomware, phishing, dan serangan denial-of-service (DoS) telah menargetkan bank, perusahaan fintech, bursa saham, dan infrastruktur keuangan lainnya (Ramadhani & Nasution, 2024). Dalam konteks ini, konsep *cyber resilience* menjadi penting, yaitu kemampuan sistem keuangan untuk mengantisipasi, menahan, dan pulih dari gangguan siber. Otoritas Jasa Keuangan di berbagai negara telah mengembangkan kerangka kerja keamanan siber seperti NIST Cybersecurity Framework, ISO/IEC 27001, dan regulasi spesifik seperti GDPR dan PSD2 di Uni Eropa, yang menunjukkan pentingnya pendekatan multidimensional terhadap isu ini (Rezki, 2023).

Selaras dengan urgensi tersebut, penelitian akademik tentang keamanan siber dalam sektor keuangan menunjukkan tren yang meningkat. Berbagai studi mengangkat topik tentang model deteksi intrusi, manajemen risiko siber, pengaruh regulasi terhadap perlindungan data, serta keterkaitan antara keamanan informasi dan kepercayaan konsumen (Alfi et al., 2023; Rossdiana & Fahrisa, 2023). Meskipun jumlah publikasi terus meningkat, masih terdapat keterbatasan dalam memahami pola dan evolusi literatur tersebut secara komprehensif. Oleh karena itu, diperlukan pendekatan sistematik untuk memetakan lanskap ilmiah terkait keamanan siber dalam ekosistem keuangan, guna mengidentifikasi arah penelitian, kesenjangan topik, dan kolaborasi ilmiah global (Qur'anisa et al., 2024).

Pendekatan bibliometrik menjadi metode yang efektif untuk menelaah struktur, dinamika, dan perkembangan penelitian di suatu bidang secara kuantitatif. Dengan memanfaatkan perangkat lunak seperti VOSviewer atau Bibliometrix, analisis bibliometrik memungkinkan pemetaan tren publikasi, jaringan kolaborasi antar penulis dan institusi, serta identifikasi tema riset dominan melalui analisis kata kunci dan sitasi. Dalam konteks keamanan siber dan keuangan, metode ini dapat memberikan gambaran yang mendalam mengenai kontribusi ilmiah, arah pengembangan teori, dan potensi sinergi lintas disiplin antara ilmu komputer, manajemen risiko, dan ekonomi digital (Donthu et al., 2021).

Selain sebagai alat evaluasi akademik, analisis bibliometrik juga memiliki nilai praktis dalam mendukung kebijakan dan pengambilan keputusan di tingkat kelembagaan maupun regulator. Dengan memahami tren penelitian dan arah pemikiran ilmiah, pemangku kepentingan dapat merancang strategi perlindungan yang adaptif dan berbasis bukti. Dalam ekosistem keuangan yang semakin terbuka dan terdigitalisasi, keandalan keamanan siber menjadi elemen penting dalam membangun ekosistem yang inklusif dan berkelanjutan. Oleh karena itu, pemetaan bibliometrik atas literatur keamanan siber dalam ekosistem keuangan bukan hanya relevan secara akademis, tetapi juga strategis secara praktis.

Meskipun literatur tentang keamanan siber dalam ekosistem keuangan telah berkembang secara signifikan, belum banyak studi yang secara sistematis mengkaji peta intelektual bidang ini secara menyeluruh. Penelitian sebelumnya masih tersebar dalam berbagai disiplin tanpa integrasi yang kuat, sehingga sulit untuk mengidentifikasi topik-topik utama, kontributor terpenting, dan tren perkembangan penelitian secara global. Tanpa pemetaan yang terstruktur, peluang kolaborasi lintas disiplin dan perumusan kebijakan berbasis pengetahuan akan sulit dioptimalkan. Studi ini bertujuan untuk melakukan analisis bibliometrik terhadap literatur ilmiah mengenai keamanan siber dalam ekosistem keuangan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan analisis bibliometrik untuk mengevaluasi dan memvisualisasikan literatur ilmiah yang berkaitan dengan keamanan siber dalam ekosistem keuangan. Analisis bibliometrik merupakan metode kuantitatif yang digunakan untuk mengidentifikasi pola publikasi, hubungan antar entitas (seperti penulis, institusi, dan negara), serta tema-tema utama dalam suatu bidang studi. Pendekatan ini cocok digunakan untuk memperoleh gambaran menyeluruh tentang struktur, perkembangan, dan tren penelitian yang sedang berlangsung (Donthu et al., 2021).

A. Sumber Data dan Proses Pencarian

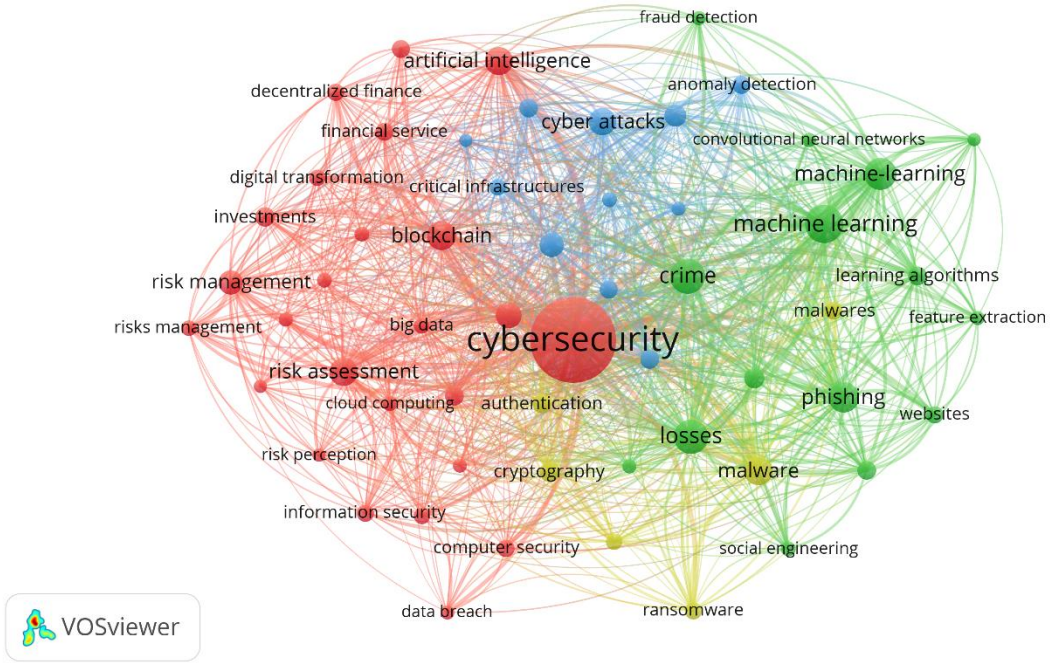
Data bibliografis dikumpulkan dari database Scopus, yang merupakan salah satu basis data ilmiah terbesar dan paling banyak digunakan dalam studi bibliometrik. Kata kunci yang digunakan dalam proses pencarian mencakup kombinasi istilah seperti "cybersecurity" OR "information security" OR "cyber threat". Kriteria inklusi mencakup artikel jurnal, proceeding conference, dan ulasan yang dipublikasikan antara tahun 2000 hingga 2024, menggunakan bahasa Inggris. Data yang diambil meliputi informasi penulis, institusi, negara, judul artikel, abstrak, kata kunci, sumber jurnal, dan jumlah sitasi. Hasil pencarian kemudian disaring untuk menghapus duplikasi dan artikel yang tidak relevan, sebelum diunduh dalam format BibTeX untuk analisis lebih lanjut.

B. Alat Analisis

Analisis data dilakukan menggunakan perangkat lunak VOSviewer (versi 1.6.x), sebuah tools visualisasi bibliometrik yang banyak digunakan dalam penelitian ilmiah. VOSviewer digunakan untuk membangun dan memvisualisasikan jaringan bibliometrik seperti analisis co-authorship, analisis co-citation, dan analisis co-word. Setiap analisis dilakukan dengan metode full counting, di mana setiap keterkaitan diberi bobot yang sama. Untuk meningkatkan relevansi, batas minimum jumlah kemunculan kata kunci atau sitasi ditetapkan (misalnya minimal 5 kali untuk keyword co-occurrence), tergantung dari sebaran dan densitas data.

HASIL DAN PEMBAHASAN

A. Pemetaan Jaringan Kata Kunci



Gambar 1. Visualisasi Jaringan

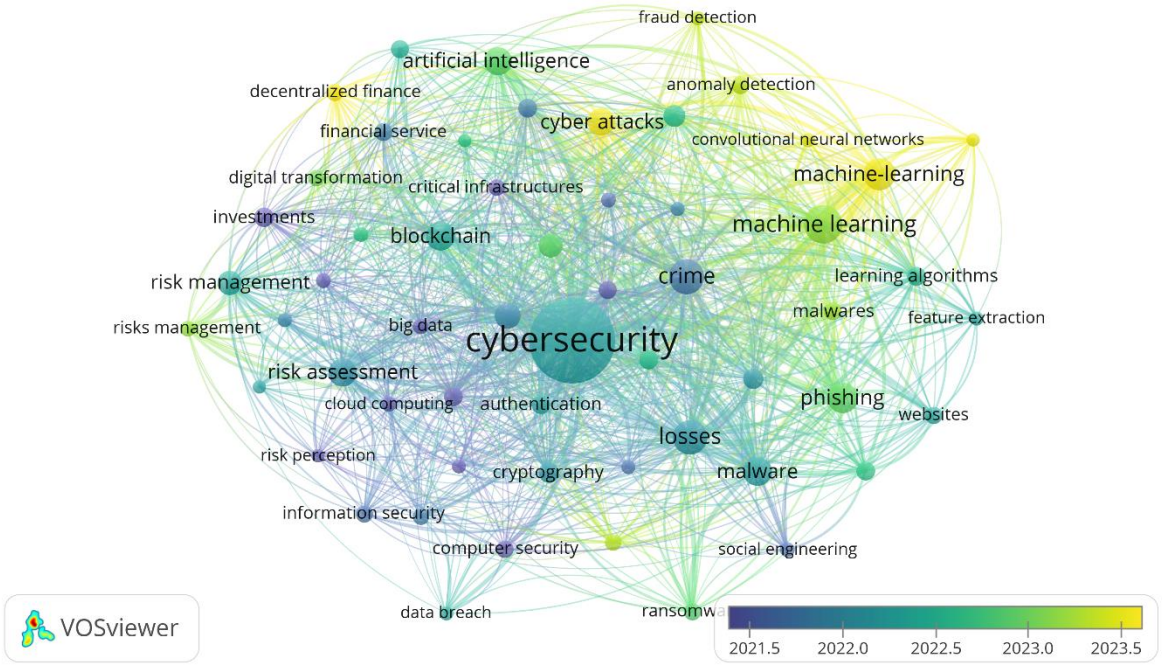
Sumber: Data Diolah, 2025

Gambar hasil analisis *keyword co-occurrence* ini memvisualisasikan struktur tematik dalam literatur ilmiah tentang keamanan siber, khususnya dalam konteks ekosistem keuangan. Jaringan ini menunjukkan hubungan antar istilah berdasarkan frekuensi kemunculan bersama dalam dokumen ilmiah. Ukuran lingkaran menunjukkan frekuensi relatif istilah tersebut, sedangkan warna mewakili klaster tematik yang berbeda. Klaster merah didominasi oleh istilah seperti *risk management*, *risk assessment*, *blockchain*, *financial service*, dan *digital transformation*. Klaster ini merepresentasikan fokus literatur pada integrasi keamanan siber dalam sistem manajemen risiko dan teknologi finansial (fintech). Topik seperti *decentralized finance*, *investments*, dan *cloud computing* juga muncul sebagai subtema penting. Keterkaitan antara istilah ini menunjukkan bahwa isu keamanan siber semakin dianggap sebagai bagian integral dari strategi mitigasi risiko dan inovasi digital di sektor keuangan.

Klaster hijau mengelompokkan kata kunci seperti *malware*, *phishing*, *ransomware*, *social engineering*, dan *losses*, yang merupakan representasi dari berbagai jenis ancaman siber. Di dalam klaster ini, istilah teknis seperti *machine learning*, *anomaly detection*, dan *convolutional neural networks* menunjukkan bahwa deteksi dan mitigasi serangan siber menjadi topik dominan, dengan pendekatan berbasis kecerdasan buatan semakin banyak digunakan. Tema ini sangat penting dalam konteks ekosistem keuangan, di mana kerentanan terhadap serangan siber dapat menyebabkan kerugian finansial besar. Klaster biru meliputi topik *cyber attacks*, *crime*, *critical infrastructures*, dan *fraud detection*. Fokusnya berada pada dimensi kriminalitas dan dampak serangan terhadap infrastruktur keuangan yang vital. Kata kunci ini menunjukkan perhatian literatur terhadap upaya perlindungan sistem keuangan dari ancaman sistemik, termasuk kejahatan terorganisir dan serangan terhadap jaringan strategis. Peran lembaga penegak hukum dan penguatan kebijakan keamanan nasional dalam ekosistem keuangan juga dapat dikaitkan dengan temuan dari klaster ini.

Istilah *cybersecurity* menempati posisi sentral dan merupakan node terbesar dalam jaringan, menunjukkan bahwa hampir seluruh tema dan subtema memiliki keterkaitan langsung dengannya. Ini menegaskan bahwa keamanan siber menjadi konsep payung yang mencakup beragam dimensi, mulai dari aspek teknis seperti *cryptography* dan *authentication*, hingga aspek manajerial seperti *risk perception* dan *information security*. Hubungan erat antara tema-tema ini menunjukkan bahwa pendekatan multidisipliner diperlukan dalam menangani isu keamanan siber di sektor keuangan. Peta visual ini menunjukkan bahwa penelitian keamanan siber dalam ekosistem keuangan telah berkembang ke arah yang semakin kompleks dan interdisipliner. Penggabungan antara teknologi baru seperti *AI* dan *blockchain*, dengan praktik manajemen risiko dan perlindungan konsumen, menjadi ciri utama literatur modern. Implikasi praktis dari hasil ini adalah pentingnya kolaborasi antara pakar teknologi, pengambil kebijakan, dan sektor keuangan untuk merancang sistem keamanan yang adaptif. Penelitian ke depan dapat difokuskan pada sinergi antara klaster, misalnya bagaimana *machine learning* digunakan dalam konteks *risk management* atau bagaimana *blockchain* mendukung *fraud detection*.

B. Analisis Tren Penelitian



Gambar 2. Visualisasi *Overlay*

Sumber: Data Diolah, 2025

Gambar ini merupakan visualisasi analisis bibliometrik berdasarkan waktu kemunculan kata kunci (overlay visualization) dalam literatur tentang *cybersecurity* dalam ekosistem keuangan. Warna dalam visualisasi menunjukkan waktu publikasi rata-rata terkait masing-masing kata kunci—mulai dari warna ungu (lebih lama, sekitar 2021) hingga kuning (lebih baru, sekitar 2023). Visualisasi ini memberikan wawasan evolusi tema penelitian dalam periode 2021 hingga 2023.5. Topik-topik seperti *risk management*, *risk assessment*, *cloud computing*, *data breach*, dan *information security* muncul dalam nuansa ungu kebiruan, menandakan bahwa tema ini mendominasi publikasi

awal pada 2021 hingga awal 2022. Ini mencerminkan fokus awal literatur pada aspek fundamental dan manajerial dalam keamanan siber, khususnya terkait dengan identifikasi dan mitigasi risiko dalam infrastruktur keuangan. Istilah seperti *blockchain* dan *decentralized finance* juga muncul dalam spektrum warna lebih tua, mengindikasikan bahwa adopsi teknologi ini menjadi perhatian awal dalam konteks keamanan keuangan digital.

Seiring waktu, fokus literatur mulai bergeser ke arah teknologi pendukung keamanan yang lebih canggih. Hal ini ditunjukkan dengan kata kunci seperti *cryptography*, *authentication*, *cyber attacks*, dan *crime* yang memiliki warna hijau kebiruan, menandakan fokus pada deteksi dan pencegahan serangan yang lebih teknis. Ini mengindikasikan bahwa peneliti mulai mengintegrasikan pendekatan sistematis berbasis teknologi keamanan ke dalam praktik finansial dan kebijakan perlindungan data. Penguatan perlindungan terhadap *critical infrastructures* juga menjadi perhatian penting dalam periode ini. Area berwarna kuning dan hijau terang—seperti *machine learning*, *convolutional neural networks*, *feature extraction*, *learning algorithms*, dan *anomaly detection*—menandai tema-tema yang sangat baru dan mengalami lonjakan perhatian dalam setahun terakhir. Hal ini menunjukkan peningkatan minat pada penerapan kecerdasan buatan dan teknik analitik canggih untuk mengidentifikasi ancaman siber secara otomatis dan real-time. Dengan munculnya serangan yang semakin kompleks, pendekatan prediktif dan berbasis AI menjadi tren utama dalam literatur keamanan siber di sektor keuangan menjelang pertengahan 2023.

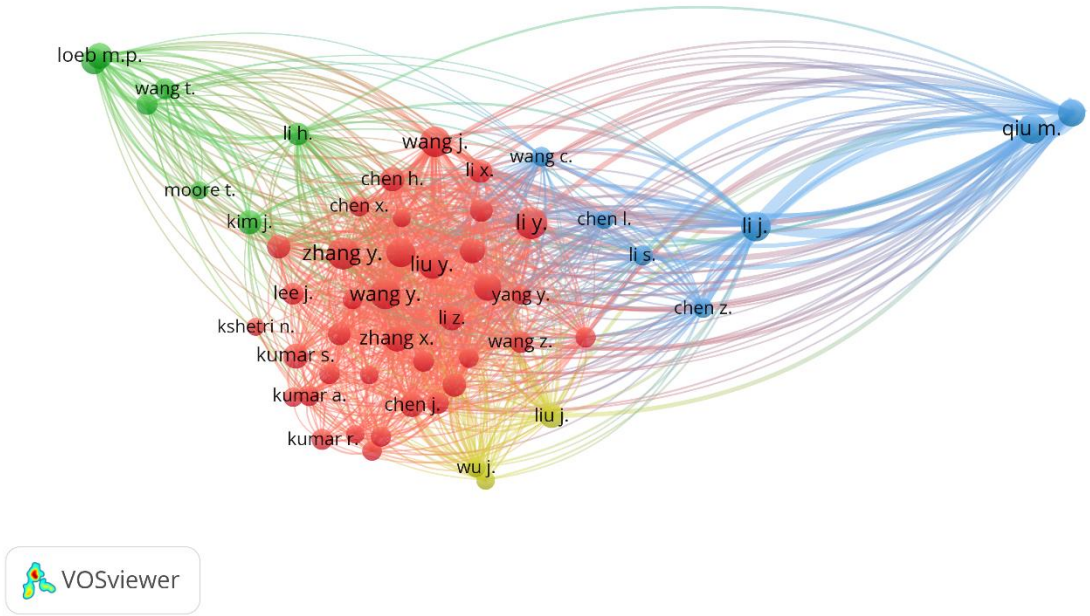
C. Top Cited Literature

Tabel 1. Literatur Teratas yang Disitir

Jumlah Kutipan	Penulis	Judul
703	(Ali et al., 2018)	Applications of Blockchains in the Internet of Things: A Comprehensive Survey
303	(Lin & Bergmann, 2016)	IoT privacy and security challenges for smart home environments
302	(Mhlanga, 2020)	Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion
280	(Mylrea & Gourisetti, 2017)	Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security
210	(Demirkan et al., 2020)	Blockchain technology in the future of business cyber security and accounting
204	(Li et al., 2017)	Intelligent cryptography approach for secure distributed big data storage in cloud computing
184	(Pugliese et al., 2021)	Machine learning-based approach: Global trends, research directions, and regulatory standpoints
177	(Ileberi et al., 2022)	A machine learning based credit card fraud detection using the GA algorithm for feature selection
177	(Lu & Da Xu, 2018)	Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management
167	(Allen et al., 2021)	A Survey of Fintech Research and Policy Discussion

Sumber: Scopus, 2025

D. Analisis Kolaborasi Penulis

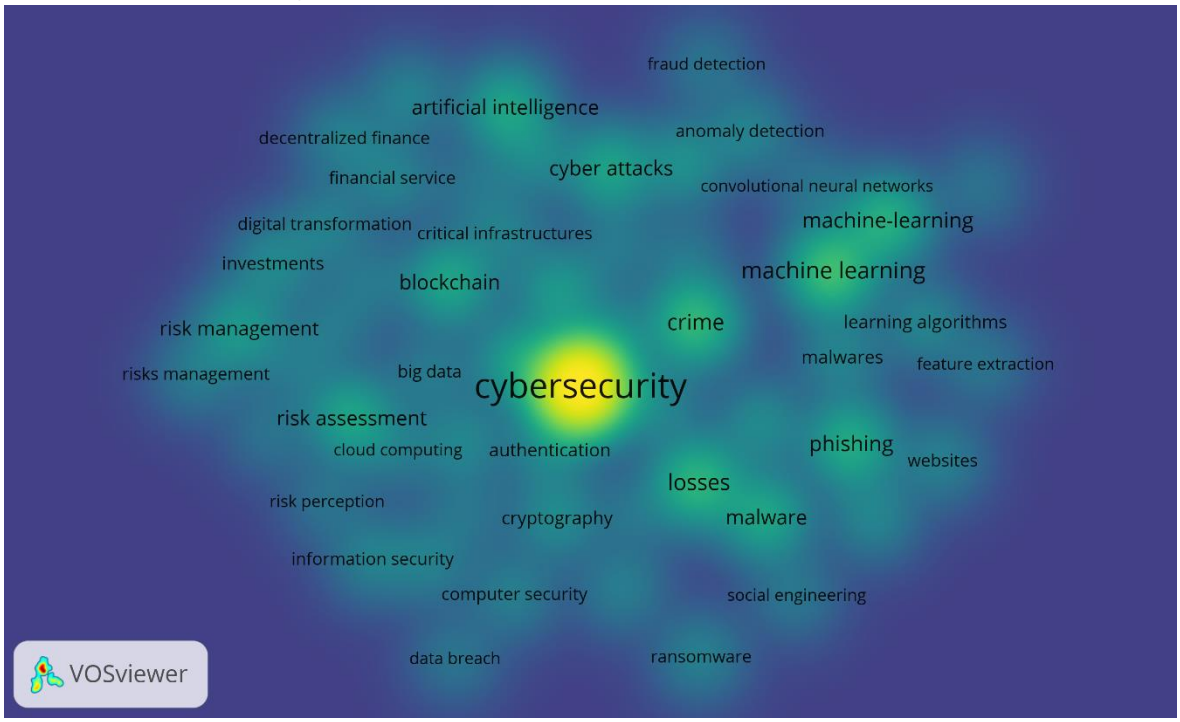


Gambar 3. Analisis Kolaborasi Penulis

Sumber: Data Diolah, 2025

Visualisasi ini menampilkan jaringan kolaborasi penulis (co-authorship) dalam bidang keamanan siber pada ekosistem keuangan. Ukuran lingkaran menunjukkan produktivitas atau jumlah publikasi seorang penulis, sedangkan warna menandai kelompok kolaborasi (cluster) yang teridentifikasi melalui keterkaitan antar penulis. Klaster merah mendominasi peta dengan konsentrasi kolaborasi tinggi di antara penulis dari Asia Timur (terutama dengan nama belakang seperti Zhang, Wang, Liu, dan Chen), menunjukkan pusat aktivitas riset yang sangat intens. Di sisi kanan, terdapat klaster biru dengan tokoh utama seperti *Qiu M.* dan *Li J.* yang menunjukkan kolaborasi kuat namun lebih eksklusif, mengindikasikan kelompok riset yang mungkin berasal dari institusi atau wilayah tertentu. Sementara itu, klaster hijau di sisi kiri menampilkan penulis seperti *Loeb M.P.* dan *Wang T.*, yang berkolaborasi secara aktif namun berada di luar pusat utama jaringan. Jaringan ini menyoroti adanya komunitas ilmiah besar yang terkonsentrasi dan kolaboratif, namun juga menunjukkan beberapa kelompok riset yang terhubung secara lebih longgar lintas klaster.

E. Analisis Peluang Penelitian



Gambar 5. Visualisasi Densitas

Sumber: Data Diolah, 2025

Gambar ini merupakan visualisasi density map dari analisis *keyword co-occurrence* dalam literatur tentang keamanan siber di ekosistem keuangan. Warna kuning menunjukkan area dengan frekuensi kemunculan kata kunci yang sangat tinggi, sedangkan area berwarna hijau hingga biru menandai frekuensi yang lebih rendah. Istilah *cybersecurity* berada di pusat peta dengan intensitas warna paling terang, menunjukkan bahwa topik ini merupakan inti dari seluruh diskursus ilmiah dalam bidang ini. Di sekitarnya, terdapat kata kunci penting lain seperti *risk assessment*, *malware*, *machine learning*, dan *losses*, yang memiliki kepadatan tinggi dan mencerminkan fokus utama penelitian yang berkaitan langsung dengan upaya deteksi dan mitigasi risiko digital di sektor keuangan. Di bagian tepi peta, kata kunci seperti *ransomware*, *social engineering*, *data breach*, dan *decentralized finance* tampak berada dalam zona biru-kehijauan, menandakan bahwa tema-tema ini meskipun relevan, masih muncul dengan frekuensi lebih rendah dibanding inti topik. Ini bisa diartikan bahwa isu-isu tersebut sedang berkembang dan memiliki potensi menjadi tren penelitian ke depan. Sementara itu, keberadaan kata kunci seperti *artificial intelligence*, *blockchain*, dan *convolutional neural networks* di area dengan warna sedang menunjukkan adanya integrasi teknologi mutakhir dalam diskursus keamanan siber yang mulai mendapat perhatian luas. Peta ini memberikan gambaran yang jelas tentang struktur intensitas penelitian dan arah eksplorasi ilmiah yang sedang berlangsung dalam domain ini.

Pembahasan

A. Struktur Tematik dan Dominasi Konsep Utama

Visualisasi *co-occurrence* menunjukkan bahwa "cybersecurity" merupakan konsep sentral yang memiliki keterkaitan erat dengan berbagai kata kunci lainnya. Ukuran node besar dan posisi

sentral dari kata ini mencerminkan dominasi topik keamanan siber dalam literatur terkait ekosistem keuangan. Sekitar istilah tersebut, muncul beberapa klaster yang menunjukkan fokus riset spesifik. Klaster merah, misalnya, menekankan pada integrasi keamanan siber dengan *risk management*, *blockchain*, dan *digital transformation*. Ini mencerminkan upaya strategis sektor keuangan dalam mengadopsi pendekatan pencegahan melalui manajemen risiko digital dan teknologi terdistribusi. Sementara itu, klaster hijau mengelompokkan istilah seperti *malware*, *phishing*, *ransomware*, dan *machine learning*, yang menyoroti dimensi teknis ancaman dan solusi. Meningkatnya frekuensi kemunculan istilah *machine learning* dan *anomaly detection* mengindikasikan kecenderungan kuat menuju penerapan teknologi cerdas dalam mendeteksi dan merespons serangan siber secara real-time. Di sisi lain, klaster biru memperlihatkan fokus terhadap isu *cyber attacks*, *crime*, dan *critical infrastructures*, yang menunjukkan pergeseran literatur ke arah pendekatan sistemik dan makro dalam melihat keamanan siber sebagai bagian dari ketahanan ekosistem keuangan global.

B. Tren Temporal dan Evolusi Topik

Visualisasi overlay berdasarkan waktu kemunculan kata kunci menunjukkan pergeseran fokus penelitian dari topik-topik fundamental menuju tema-tema yang lebih mutakhir. Topik seperti *risk management*, *cloud computing*, dan *information security* mendominasi sekitar tahun 2021–2022, menunjukkan bahwa literatur awal masih berfokus pada pemahaman dasar dan infrastruktur keamanan informasi. Hal ini logis, mengingat peningkatan eksponensial digitalisasi keuangan akibat pandemi COVID-19 mendorong instansi keuangan untuk memperkuat pertahanan dasar mereka terlebih dahulu. Namun, mulai tahun 2022 hingga pertengahan 2023, terjadi lonjakan minat pada penerapan teknologi canggih seperti *convolutional neural networks*, *feature extraction*, dan *learning algorithms*. Istilah-istilah ini menempati posisi spektrum warna kuning dalam overlay map, menandakan kebaruan dan popularitasnya dalam literatur terkini. Ini menunjukkan bahwa pendekatan berbasis kecerdasan buatan menjadi arus utama dalam pengembangan sistem keamanan keuangan yang lebih prediktif dan adaptif terhadap ancaman yang semakin kompleks. Selain itu, istilah *blockchain* dan *decentralized finance* muncul cukup awal namun masih berperan penting. Meskipun kemunculannya mendahului topik AI modern, tren ini tetap relevan karena teknologi blockchain dianggap sebagai solusi untuk meningkatkan transparansi dan imutabilitas data dalam transaksi keuangan digital, sehingga mendukung keamanan siber secara struktural.

C. Jaringan Kolaborasi Penulis

Analisis co-authorship mengungkap struktur kolaborasi yang menarik. Teridentifikasi bahwa sebagian besar penelitian di bidang ini didominasi oleh penulis dari Asia Timur, khususnya dari Tiongkok, sebagaimana terlihat dari dominasi klaster merah yang dipenuhi nama-nama seperti Zhang, Wang, Liu, dan Chen. Hal ini mencerminkan tingginya produktivitas ilmiah dari kawasan ini, kemungkinan besar didorong oleh kebijakan strategis nasional dan ekosistem riset teknologi yang kuat. Menariknya, kelompok biru yang relatif eksklusif dipimpin oleh *Qiu M.* dan *Li J.* menunjukkan kekompakan internal namun sedikit konektivitas dengan klaster lain. Hal ini bisa mengindikasikan keberadaan laboratorium atau institusi tertentu yang sangat aktif namun masih belum terbuka terhadap kolaborasi eksternal. Sementara itu, klaster hijau yang mencakup *Loeb M.P.*, *Moore T.*, dan *Kim J.* menunjukkan keterlibatan dari penulis luar Asia, dengan pola kolaborasi lintas negara yang lebih longgar. Temuan ini menunjukkan bahwa meskipun literatur keamanan siber

bersifat global, terdapat disparitas dalam hal intensitas kolaborasi antar penulis lintas kawasan. Penguatan kerja sama internasional dan lintas disiplin menjadi peluang besar untuk meningkatkan kualitas dan relevansi riset di masa depan.

D. Kepadatan dan Fokus Riset Berdasarkan Density Map

Peta densitas yang dihasilkan menunjukkan bahwa istilah *cybersecurity*, *risk assessment*, *malware*, dan *machine learning* adalah titik panas dalam literatur. Warna kuning terang pada area ini menandakan frekuensi kemunculan tinggi dan keterkaitan kuat dengan kata kunci lain. Dengan demikian, dapat disimpulkan bahwa kombinasi antara pendekatan manajerial dan teknis masih menjadi inti penelitian di bidang ini. Sebaliknya, istilah seperti *social engineering*, *ransomware*, dan *feature extraction* muncul di area dengan warna hijau ke biru, menandakan bahwa topik-topik ini masih berkembang dan memiliki ruang untuk eksplorasi lebih lanjut. Hal ini dapat dimaknai sebagai potensi arah penelitian di masa depan, terutama dalam memahami dan mengantisipasi pola serangan non-teknis dan aspek perilaku manusia dalam risiko siber. Kata kunci seperti *blockchain* dan *artificial intelligence* yang berada dalam area menengah mengindikasikan bahwa integrasi teknologi disruptif ke dalam sistem keamanan siber telah menjadi perhatian tetapi masih belum tuntas dieksplorasi secara maksimal. Oleh karena itu, peneliti dan praktisi perlu memperkuat eksplorasi di area yang belum padat ini untuk memperluas cakupan solusi dan inovasi di bidang keamanan siber.

E. Implikasi Praktis dan Akademik

Hasil diskusi ini memiliki dua implikasi penting. Pertama, secara akademik, penelitian ini menegaskan pentingnya pendekatan interdisipliner dan kolaboratif dalam memahami dan menangani isu keamanan siber. Studi keamanan siber dalam ekosistem keuangan tidak dapat berdiri sendiri dalam domain teknologi informasi, tetapi harus mencakup ilmu manajemen risiko, keuangan digital, dan ilmu perilaku. Hal ini dapat diwujudkan dengan membentuk jaringan riset lintas institusi dan lintas negara, serta memperkuat publikasi dalam jurnal-jurnal yang menjembatani sains dan kebijakan. Kedua, secara praktis, temuan ini mendukung perlunya penguatan strategi keamanan siber di sektor keuangan melalui penerapan teknologi prediktif seperti AI, integrasi blockchain untuk transparansi transaksi, dan penguatan perlindungan terhadap infrastruktur keuangan yang kritis. Pemangku kebijakan dapat menggunakan peta tren ini untuk merancang regulasi yang adaptif terhadap perkembangan teknologi dan ancaman yang terus berubah, serta mendorong investasi pada riset dan pengembangan sistem keamanan digital nasional.

KESIMPULAN

Berdasarkan hasil analisis bibliometrik terhadap literatur keamanan siber dalam ekosistem keuangan, dapat disimpulkan bahwa topik *cybersecurity* menempati posisi sentral dalam kajian ilmiah dan memiliki keterkaitan erat dengan isu-isu seperti manajemen risiko, serangan siber, teknologi kecerdasan buatan, dan penerapan blockchain. Evolusi penelitian menunjukkan pergeseran dari fokus pada aspek fundamental seperti *information security* dan *risk assessment* menuju pendekatan teknis yang lebih canggih seperti

machine learning dan *anomaly detection*. Selain itu, pola kolaborasi penulis mengungkapkan dominasi regional oleh peneliti Asia Timur, dengan potensi perluasan kerja sama lintas kawasan yang masih terbuka. Secara keseluruhan, studi ini memberikan pemetaan menyeluruh terhadap arah, tren, dan peluang riset keamanan siber dalam sektor keuangan, serta menegaskan pentingnya pendekatan interdisipliner dan responsif terhadap dinamika teknologi dan ancaman digital yang terus berkembang.

REFERENSI

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.

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1676–1717.

Allen, F., Gu, X., & Jagtiani, J. (2021). A survey of fintech research and policy discussion. *Review of Corporate Finance*, *1*(3–4).

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285–296.

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 24.

Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. *Information Sciences*, *387*, 103–115.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44.

Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115.

Mhlanga, D. (2020). Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies*, *8*(3), 45.

Mylrea, M., & Gourisetti, S. N. G. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. *2017 Resilience Week (RWS)*, 18–23.

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha Kecil Menengah di Era Ekonomi Digital di Indonesia. *Sanskara Ekonomi Dan Kewirausahaan*, *2*(03), 156–167.

Pugliese, R., Regondi, S., & Marini, R. (2021). Machine learning-based approach: Global trends, research directions, and regulatory standpoints. *Data Science and Management*, *4*, 19–29.

Putra, A. N. M., Rahma, F., & Wahyuni, E. G. (2024). Kajian Literatur: Kesadaran Keamanan Siber pada Pengguna E-Wallet. *Prosiding Seminar Nasional Teknik Elektro, Sistem Informasi, Dan Teknik Informatika (SNESTIK)*, *1*(1), 404–411.

Qur'anisa, Z., Herawati, M., Lisvi, L., Putri, M. H., & Feriyanto, O. (2024). Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital: Studi Literatur. *GEMILANG: Jurnal Manajemen Dan Akuntansi*, *4*(3), 99–114.

Ramadhani, N., & Nasution, M. I. P. (2024). Tantangan Dan Solusi Keamanan Siber Dalam Transaksi E-Commerce. *Jurnal Penelitian Sistem Informasi (JPSI)*, *2*(2), 134–144.

Rezki, J. F. (2023). *ISU KEAMANAN SIBER PERBANKAN DAN POTENSI BANK RUN*.

Rossdiana, R. A., & Fahrisa, T. R. (2023). Strategi Keamanan Siber Pemerintah India Dari Perspektif Kautilya: Serangan Siber Mumbai 2020. *Indonesian Journal of International Relations*, *7*(1), 140–164.

Santoso, J. T. (2023). Teknologi Keamanan Siber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–173.