Jumistik
E-ISSN: 2964-3953 P-ISSN: 2964-3988
Jurnal Manajemen Informatika, Sistem Informasi dan Teknologi Komputer

Vol.5 No.1 Juni 2026
Hal 1166-1174
Https://ojs.amiklps.ac.id

CYBERSECURITY STRATEGIES IN BIG DATA ECOSYSTEMS: A SYSTEMATIC LITERATURE REVIEW

Anita Juniarti[1]
[1]Teknologi Informasi, Universitas Sapta Mandiri
E-mail: anitajuniarti@univsm.ac.id

INFO ARTIKEL

Sejarah Artikel
Diterima : 24/06/2026
Direvisi : 29/06/2026
Diterbitkan : 30/06/2026

***Corresponding author**
anitajuniarti@univsm.ac.id

DOI: 10.70247/jumistik.v5i1.338

GRAPHICAL ABSTRACT

ABSTRACT

The rapid growth of the big data ecosystem has significantly enhanced organizations' ability to process and analyze large-scale data while simultaneously increasing cybersecurity risks. Various cyber threats, including data breaches, malware, ransomware, and social engineering attacks, require more adaptive and comprehensive security strategies. This study aims to identify, analyze, and synthesize effective cybersecurity strategies for big data ecosystems using a Systematic Literature Review (SLR) approach. The review was conducted following the PRISMA 2020 guidelines through the stages of identification, screening, eligibility assessment, and selection of studies published between 2019 and 2025. The findings indicate that Artificial Intelligence (AI) and Machine Learning (ML) enhance real-time threat detection and anomaly identification, while blockchain technology improves authentication, data integrity, transparency, and resistance to data manipulation. Furthermore, adaptive cybersecurity governance and continuous security awareness programs play a crucial role in strengthening organizational cyber resilience. The study concludes that effective cybersecurity in big data environments requires the integration of advanced technologies, governance frameworks, and human factors. The findings provide valuable insights for researchers, practitioners, and policymakers in designing resilient and sustainable cybersecurity strategies for big data ecosystems.

***Keywords**: Big Data, Cybersecurity, Artificial Intelligence, blockchain, Systematic Literature Review*

ABSTRAK

Perkembangan ekosistem big data telah meningkatkan kemampuan organisasi dalam mengelola dan menganalisis data berskala besar, namun di sisi lain juga memperbesar risiko terhadap keamanan siber. Beragam ancaman, seperti pelanggaran data, serangan malware, ransomware, hingga rekayasa sosial, menuntut penerapan strategi keamanan yang lebih adaptif dan komprehensif. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mensintesis strategi keamanan siber yang efektif dalam ekosistem big data melalui pendekatan Systematic Literature Review (SLR). Proses tinjauan dilakukan dengan mengacu pada pedoman PRISMA 2020 melalui tahapan identifikasi, penyaringan, penilaian kelayakan, dan seleksi artikel yang dipublikasikan pada periode 2019–2025. Hasil sintesis menunjukkan bahwa penerapan Artificial Intelligence (AI) dan Machine Learning (ML) mampu meningkatkan kemampuan deteksi ancaman secara real-time, sementara teknologi blockchain berperan dalam memperkuat autentikasi, integritas data, dan transparansi. Selain itu, implementasi cybersecurity governance yang adaptif serta peningkatan security awareness menjadi faktor penting dalam membangun ketahanan organisasi terhadap ancaman siber. Penelitian ini menyimpulkan bahwa strategi keamanan siber yang efektif memerlukan integrasi antara teknologi,

tata kelola, dan faktor manusia. Hasil penelitian diharapkan dapat menjadi referensi bagi peneliti, praktisi, dan pembuat kebijakan dalam merancang sistem keamanan big data yang lebih tangguh dan berkelanjutan.

Kata kunci: *Big Data, Keamanan Siber, Kecerdasan Buatan, Blockchain, Systematic Literature Review*

PENDAHULUAN

Transformasi digital telah mendorong pertumbuhan data dalam jumlah yang sangat besar sehingga menjadikan big data sebagai salah satu aset strategis bagi organisasi di berbagai sektor, seperti pemerintahan, kesehatan, keuangan, pendidikan, dan industri. Karakteristik big data yang meliputi volume, velocity, variety, veracity, dan value memungkinkan organisasi memperoleh informasi secara lebih cepat dan akurat untuk mendukung pengambilan keputusan. Namun, di sisi lain, kompleksitas pengelolaan data dalam skala besar juga meningkatkan risiko terhadap keamanan informasi, seperti kebocoran data, akses tidak sah, serangan malware, ransomware, maupun manipulasi data. Oleh karena itu, keamanan siber (cybersecurity) menjadi aspek yang tidak dapat dipisahkan dari pengelolaan ekosistem big data karena berperan dalam menjaga kerahasiaan, integritas, dan ketersediaan data yang menjadi aset utama organisasi [1], [2], [3]

Seiring meningkatnya adopsi big data, ancaman keamanan siber juga berkembang semakin kompleks. Tidak hanya berasal dari serangan eksternal, ancaman juga muncul akibat kelemahan tata kelola keamanan, kesalahan konfigurasi sistem, serta faktor manusia yang masih menjadi penyebab utama terjadinya insiden keamanan informasi. [4] menjelaskan bahwa mekanisme perlindungan data seperti enkripsi masih menjadi fondasi utama dalam menjaga keamanan data berskala besar, namun implementasinya belum mampu mengatasi seluruh jenis ancaman yang berkembang. Selain itu, tantangan tata kelola keamanan informasi semakin meningkat seiring berkembangnya teknologi cerdas yang menghasilkan data dalam jumlah besar, sehingga organisasi dituntut memiliki kerangka keamanan yang adaptif dan berorientasi pada manajemen risiko [3], [5]

Berbagai penelitian telah mengusulkan beragam pendekatan untuk meningkatkan keamanan ekosistem big data. Perkembangan teknologi Artificial Intelligence (AI) dan Machine Learning (ML) memungkinkan deteksi ancaman secara otomatis melalui analisis pola serangan dan identifikasi anomali secara real-time [6], [7]. Di sisi lain, teknologi blockchain mulai banyak diterapkan untuk meningkatkan integritas data, transparansi transaksi, dan ketahanan terhadap manipulasi data melalui mekanisme desentralisasi [8], [9]. Selain pendekatan berbasis teknologi, aspek tata kelola keamanan siber juga mendapat perhatian karena keberhasilan implementasi keamanan tidak hanya bergantung pada teknologi, tetapi juga pada kebijakan organisasi, kepatuhan terhadap standar keamanan, dan pengelolaan risiko secara berkelanjutan[10], [11].

Meskipun penelitian mengenai keamanan siber pada ekosistem big data telah berkembang pesat, sebagian besar studi masih berfokus pada satu pendekatan tertentu, seperti enkripsi data, penerapan machine learning, blockchain, atau tata kelola keamanan secara terpisah. Penelitian yang mengintegrasikan berbagai pendekatan tersebut ke dalam satu kerangka analisis yang komprehensif masih relatif terbatas. Selain itu, perkembangan teknologi terbaru, seperti Generative Artificial Intelligence, blockchain berbasis kecerdasan buatan, serta tantangan tata kelola data yang dihasilkan oleh sistem cerdas pada periode 2024–2025, belum banyak dibahas secara terpadu dalam penelitian sebelumnya[3], [12], [13]. Kondisi tersebut menunjukkan adanya research gap, yaitu belum tersedianya sintesis literatur yang mengkaji keterkaitan antara teknologi, tata kelola, dan faktor manusia dalam membangun ketahanan keamanan siber pada ekosistem big data.

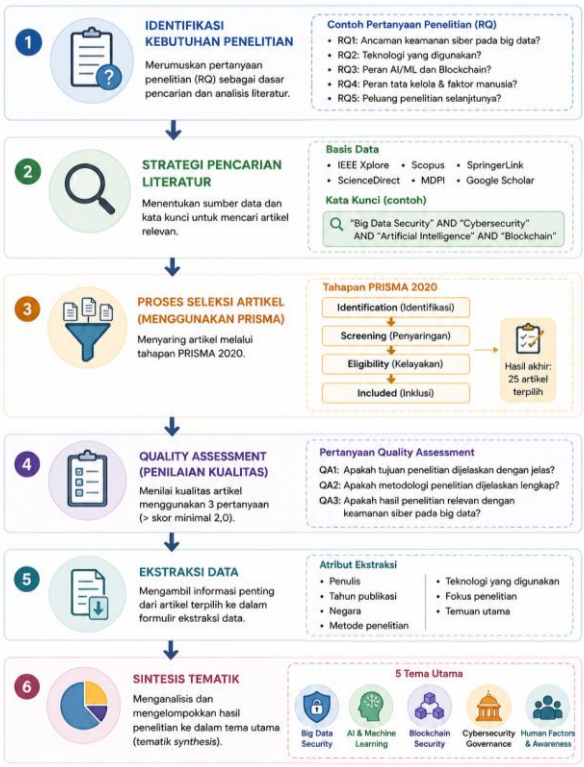
Berdasarkan research gap tersebut, penelitian ini menawarkan kebaruan (novelty) berupa sintesis literatur yang mengintegrasikan lima dimensi utama keamanan siber dalam ekosistem big data, yaitu (1) keamanan big data, (2) tata kelola keamanan siber, (3) penerapan Artificial Intelligence dan Machine Learning, (4) teknologi blockchain, serta (5) faktor manusia dan kesadaran keamanan informasi. Integrasi kelima dimensi tersebut memberikan perspektif yang lebih komprehensif dibandingkan penelitian sebelumnya yang umumnya hanya membahas satu aspek secara parsial. Selain itu, penelitian ini menggunakan literatur terbaru yang dipublikasikan pada periode 2019–2025, sehingga mampu menggambarkan perkembangan teknologi dan strategi keamanan siber yang paling mutakhir.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mensintesis berbagai strategi keamanan siber yang diterapkan dalam ekosistem big data melalui pendekatan Systematic Literature Review (SLR). Hasil penelitian diharapkan dapat memberikan kontribusi akademik berupa pemetaan perkembangan penelitian keamanan siber pada ekosistem big data serta memberikan rekomendasi praktis bagi organisasi dalam merancang strategi keamanan yang lebih efektif, adaptif, dan berkelanjutan untuk menghadapi dinamika ancaman siber di era transformasi digital.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode Systematic Literature Review (SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil penelitian mengenai strategi keamanan siber dalam ekosistem big data. Pendekatan SLR dipilih karena mampu memberikan proses peninjauan literatur yang sistematis, transparan, dan dapat direplikasi dibandingkan tinjauan literatur konvensional. Proses penelitian mengacu pada pedoman PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses)[14] serta panduan Systematic Literature Review yang dikembangkan oleh [15].

Metodologi penelitian terdiri atas enam tahapan utama, yaitu: (1) identifikasi kebutuhan penelitian, (2) strategi pencarian literatur, (3) proses seleksi artikel menggunakan PRISMA, (4) quality assessment, (5) ekstraksi data, dan (6) sintesis tematik, sebagaimana ditunjukkan pada



Gambar 1. Tahap Metode Penelitian
Sumber. Tahap Penelitian SLR

Identifikasi Kebutuhan Penelitian

Tahap awal penelitian dilakukan dengan merumuskan pertanyaan penelitian (Research Questions/RQ) sebagai dasar proses pencarian dan analisis literatur. Pertanyaan penelitian disusun untuk memperoleh gambaran komprehensif mengenai perkembangan keamanan siber dalam ekosistem big data.

Adapun pertanyaan penelitian adalah sebagai berikut.

- **RQ1:** Apa saja ancaman keamanan siber yang paling dominan pada ekosistem big data?
- **RQ2:** Teknologi apa yang paling banyak digunakan untuk meningkatkan keamanan big data?
- **RQ3:** Bagaimana perkembangan penerapan Artificial Intelligence, Machine Learning, dan Blockchain dalam keamanan siber?
- **RQ4:** Bagaimana peran tata kelola keamanan siber dan faktor manusia dalam meningkatkan ketahanan organisasi?
- **RQ5:** Apa peluang penelitian selanjutnya berdasarkan perkembangan literatur tahun 2019–2025?

Strategi Pencarian Literatur

Proses pencarian literatur dilakukan secara sistematis pada beberapa basis data ilmiah internasional yang memiliki reputasi tinggi, yaitu:

- *IEEE Xplore*
- *Scopus*
- *SpringerLink*
- *ScienceDirect*
- *MDPI*
- *Google Scholar*

Pencarian dilakukan terhadap artikel yang dipublikasikan pada periode 2019–2025 untuk memperoleh perkembangan penelitian terkini mengenai keamanan siber pada ekosistem big data.

Kata kunci pencarian disusun menggunakan operator Boolean (AND dan OR), antara lain:

- *"Big Data Security"*
- *"Cybersecurity AND Big Data"*
- *"Artificial Intelligence AND Cybersecurity"*
- *"Machine Learning AND Cybersecurity"*
- *"Blockchain Security"*
- *"Cybersecurity Governance"*
- *"Human Factors in Cybersecurity"*

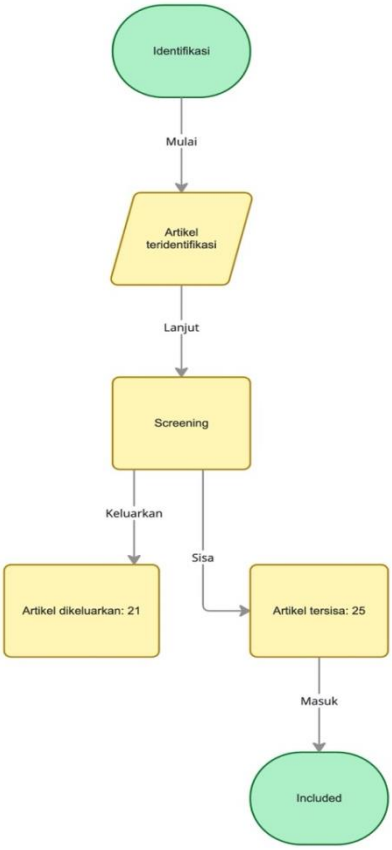
Strategi pencarian tersebut memungkinkan diperolehnya artikel yang relevan dengan ruang lingkup penelitian

Proses Seleksi Artikel Menggunakan PRISMA

Proses seleksi literatur dilakukan mengikuti tahapan **PRISMA 2020**, yang meliputi:

1. **Identification**, yaitu mengidentifikasi seluruh artikel yang diperoleh dari berbagai basis data.
2. **Screening**, yaitu menghapus artikel duplikat serta menyaring berdasarkan judul dan abstrak.
3. **Eligibility**, yaitu mengevaluasi kesesuaian isi artikel dengan tujuan penelitian melalui pembacaan teks lengkap.
4. **Included**, yaitu memilih artikel yang memenuhi seluruh kriteria inklusi untuk dianalisis lebih lanjut.

Tahapan seleksi tersebut disajikan dalam berupa PRISMA Flow Diagram.



Gambar 2. PRISMA Flow Diagram.
Sumber. Olah data

Agar artikel yang dianalisis memiliki kualitas dan relevansi yang tinggi, penelitian ini menerapkan kriteria inklusi dan eksklusi sebagai berikut.

Kriteria Inklusi

- Artikel dipublikasikan pada periode 2019–2025.
- Artikel membahas keamanan siber pada ekosistem big data.
- Artikel dipublikasikan pada jurnal internasional bereputasi atau jurnal nasional terakreditasi SINTA.
- Artikel tersedia dalam bentuk full text.
- Artikel menggunakan metode penelitian yang jelas.

Kriteria Eksklusi

- Artikel duplikat.
- Artikel yang tidak membahas keamanan big data.
- Editorial, book review, atau opini.
- Artikel yang tidak tersedia secara lengkap.

Quality Assessment

Untuk memastikan kualitas literatur yang digunakan, setiap artikel dievaluasi menggunakan tiga pertanyaan quality assessment yang diadaptasi dari [15]

Tabel 1. Quality Assessment (QA1–QA3).

Kode	*Pertanyaan*
QA1	Apakah tujuan penelitian dijelaskan dengan jelas?
QA2	Apakah metodologi penelitian dijelaskan secara lengkap?
QA3	Apakah hasil penelitian relevan dengan keamanan siber pada ekosistem big data?

Sumber. Olah Data

Setiap pertanyaan diberikan skor:

- Ya = 1
- Sebagian = 0,5
- Tidak = 0

Hanya artikel dengan skor minimal 2,0 yang dimasukkan ke tahap analisis.

Ekstraksi Data

Informasi penting dari setiap artikel diekstraksi menggunakan formulir ekstraksi data yang memuat beberapa atribut, yaitu:

- Penulis
- Tahun publikasi
- Negara
- Metode penelitian
- Teknologi yang digunakan
- Fokus penelitian
- Temuan utama

Sintesis Tematik

Data yang telah diekstraksi kemudian dianalisis menggunakan thematic synthesis. Pendekatan ini dipilih karena mampu mengelompokkan hasil penelitian berdasarkan tema-tema utama sehingga memudahkan identifikasi pola, kesenjangan penelitian, serta perkembangan teknologi keamanan siber.

Berdasarkan hasil sintesis, artikel dikelompokkan ke dalam lima tema utama, yaitu:

1. Big Data Security.
2. Cybersecurity Governance.
3. Artificial Intelligence dan Machine Learning.
4. Blockchain Security.
5. Human Factors dan Security Awareness.

Setiap tema dianalisis secara komparatif untuk mengidentifikasi persamaan, perbedaan, kelebihan, keterbatasan, serta peluang penelitian di masa mendatang

HASIL DAN PEMBAHASAN

Hasil Sileksi Literatur

Proses pencarian literatur dilakukan pada enam basis data ilmiah, yaitu IEEE Xplore, Scopus, SpringerLink, ScienceDirect, MDPI, dan Google Scholar menggunakan kata kunci yang telah ditentukan pada tahap metodologi. Berdasarkan proses identifikasi awal diperoleh sejumlah artikel yang berkaitan dengan keamanan siber pada ekosistem big data.

Selanjutnya dilakukan proses penyaringan menggunakan pedoman PRISMA 2020 yang meliputi identifikasi, screening, eligibility, dan inclusion. Artikel yang terduplikasi, tidak tersedia dalam bentuk full text, serta tidak sesuai dengan fokus penelitian dieliminasi. Setelah melalui proses quality assessment, diperoleh 25 artikel utama yang memenuhi seluruh kriteria inklusi dan digunakan sebagai dasar sintesis dalam penelitian ini.

Analisis terhadap artikel yang terpilih menunjukkan bahwa penelitian mengenai keamanan siber dalam ekosistem big data mengalami peningkatan yang signifikan selama periode 2019–2025. Peningkatan tersebut terutama dipengaruhi oleh berkembangnya teknologi Artificial Intelligence, Machine Learning, blockchain, serta meningkatnya perhatian terhadap tata kelola keamanan siber dan faktor manusia. Selain itu, sebagian besar penelitian dipublikasikan pada jurnal internasional bereputasi seperti IEEE Access, Computers & Security, Applied Sciences, Information, Future Internet, dan International Journal of Information Security.

Berdasarkan hasil ekstraksi data, artikel kemudian dikelompokkan ke dalam lima tema utama, yaitu (1) Big Data Security, (2) Artificial Intelligence dan Machine Learning, (3) Blockchain Security, (4) Cybersecurity Governance, serta (5) Human Factors dan Security Awareness. Pengelompokan ini menjadi dasar dalam melakukan sintesis dan analisis komparatif pada bagian pembahasan.

Tabel 2. Distribusi Artikel Berdasarkan Tema

Tema	*Jumlah*
Big Data Security	*5*
AI & Machine Learning	*5*
Blockchain Security	*5*
Cybersecurity Governance	*5*
Human Factors	*5*

Sumber. Olah Data

Tabel 3. Distribusi Artikel Berdasarkan Tahun

Tahun	*Jumlah Artikel*
2019	1
2020	4
2021	2
2022	3
2023	3
2024	3
2025	9

Sumber. Olah Data

Big Data Security

Keamanan merupakan aspek fundamental dalam pengelolaan ekosistem big data karena karakteristik data yang memiliki volume, kecepatan, variasi, dan kompleksitas yang tinggi. Semakin meningkatnya jumlah data yang diproses oleh organisasi menyebabkan permukaan serangan (*attack surface*) semakin luas, sehingga risiko terhadap pelanggaran data, akses tidak sah, ransomware, dan kebocoran informasi juga meningkat. Oleh karena itu, strategi keamanan tidak lagi hanya berfokus pada perlindungan data, tetapi berkembang menjadi pendekatan yang mengintegrasikan teknologi, tata kelola, serta pengelolaan risiko.

Hasil sintesis menunjukkan bahwa penelitian mengenai Big Data Security mengalami perkembangan yang signifikan selama periode 2019–2025. [1] menekankan bahwa keamanan harus diintegrasikan sejak tahap perancangan sistem (*secure-by-design*), sehingga pengembangan aplikasi big data telah mempertimbangkan identifikasi kerentanan, pengujian keamanan, serta pengelolaan risiko sepanjang siklus hidup perangkat lunak. Pendekatan ini berbeda dengan [4] yang lebih berfokus pada penerapan teknik enkripsi sebagai mekanisme utama untuk menjaga kerahasiaan data sensitif selama proses penyimpanan maupun transmisi.

Selanjutnya [2] menunjukan bahwa perlindungan privasi pada aplikasi big data tidak cukup hanya mengandalkan enkripsi. Penelitian tersebut menegaskan pentingnya kombinasi antara kontrol akses, manajemen identitas, anonimisasi data, dan kepatuhan terhadap regulasi perlindungan data untuk mengurangi risiko kebocoran informasi. Temuan tersebut diperkuat oleh [3] yang mengidentifikasi bahwa berkembangnya teknologi cerdas, seperti Internet of Things (IoT), Artificial Intelligence (AI), dan sistem otonom, menghasilkan tantangan baru dalam tata kelola data. Menurut penelitian tersebut, keamanan big data saat ini harus mempertimbangkan kualitas data, kepemilikan data, interoperabilitas, serta mekanisme tata kelola yang adaptif terhadap perubahan teknologi

Hasil perbandingan menunjukkan adanya perubahan paradigma dalam penelitian keamanan big data. Penelitian awal lebih menitikberatkan pada perlindungan data melalui mekanisme teknis, seperti enkripsi dan kontrol akses. Namun, penelitian terbaru mengarah pada pendekatan yang lebih komprehensif dengan mengintegrasikan aspek teknologi, tata kelola, manajemen risiko, serta kepatuhan terhadap regulasi. Pergeseran tersebut menunjukkan bahwa keamanan big data tidak lagi dipandang sebagai permasalahan teknis semata, melainkan sebagai bagian dari strategi organisasi dalam menjaga keberlangsungan layanan digital.

Meskipun demikian, hasil sintesis juga mengidentifikasi beberapa kesenjangan penelitian. Sebagian besar penelitian masih mengevaluasi efektivitas setiap mekanisme keamanan secara terpisah, misalnya hanya membahas enkripsi, privasi, atau tata kelola data, tanpa mengembangkan kerangka keamanan yang mampu mengintegrasikan seluruh komponen tersebut. Selain itu, sebagian besar penelitian dilakukan pada lingkungan komputasi awan (*cloud computing*) atau organisasi berskala

besar, sehingga implementasinya pada organisasi dengan sumber daya terbatas masih relatif sedikit dibahas. Tantangan lain yang mulai muncul adalah meningkatnya penggunaan Artificial Intelligence dalam pengelolaan data yang berpotensi menimbulkan ancaman baru, seperti *data poisoning*, *model manipulation*, dan penyalahgunaan data untuk pelatihan model AI.

Berdasarkan hasil sintesis tersebut, penelitian ini berpendapat bahwa pengembangan keamanan big data di masa mendatang perlu mengadopsi pendekatan yang lebih adaptif melalui integrasi mekanisme perlindungan data, tata kelola keamanan, serta teknologi cerdas. Pendekatan tersebut diharapkan mampu meningkatkan ketahanan organisasi dalam menghadapi ancaman siber yang terus berkembang sekaligus mendukung pemanfaatan big data secara aman dan berkelanjutan.

Tabel 4. Sintesis Penelitian Big Data Security

PENULIS	FOKUS PENELITIAN	KONTRIBUSI	KETERBATASAN
Moreno Et Al. (2019)	Secure Development	Secure-by-Design	Belum membahas AI
Banasode & Padmannavar (2020)	Enkripsi	Perlindungan data sensitif	Fokus pada kerahasiaan data
Rafiq Et Al. (2022)	Data Privacy	Privasi dan kontrol akses	Belum mengintegrasikan governance
Bena Et Al. (2025)	Big Data Governance	Tata kelola data cerdas	Implementasi masih konseptual

Sumber. Olah Data

Artificial Intelligence dan Machine Learning untuk Cybersecurity

Perkembangan Artificial Intelligence (AI) dan Machine Learning (ML) telah mengubah paradigma keamanan siber dari pendekatan reaktif menjadi proaktif. Kemampuan AI dalam menganalisis data dalam jumlah besar memungkinkan sistem mengenali pola serangan, mendeteksi anomali, serta memprediksi potensi ancaman secara real-time. Pada ekosistem big data, kemampuan tersebut menjadi sangat penting karena volume dan kecepatan data yang tinggi tidak lagi dapat dianalisis secara efektif menggunakan metode konvensional.

Hasil sintesis menunjukkan bahwa AI dan ML telah menjadi teknologi yang paling banyak diteliti dalam keamanan siber selama lima tahun terakhir. [7] menjelaskan bahwa algoritma supervised learning, unsupervised learning, dan deep learning mampu meningkatkan akurasi sistem deteksi intrusi (*Intrusion Detection System/IDS*) dibandingkan metode berbasis aturan (*rule-based detection*). Selanjutnya, [6] menunjukkan bahwa penerapan AI tidak hanya meningkatkan kemampuan deteksi ancaman, tetapi juga mempercepat proses respons insiden melalui otomatisasi analisis log dan identifikasi aktivitas abnormal.

Penelitian yang lebih mutakhir oleh memperlihatkan bahwa model ML telah berkembang ke arah *adaptive learning*, sehingga mampu mempelajari pola serangan baru tanpa memerlukan pembaruan aturan secara manual. Di sisi lain, [13] mengungkap bahwa kemunculan Generative Artificial Intelligence menghadirkan dua sisi yang saling bertolak belakang. Teknologi tersebut mampu meningkatkan otomatisasi keamanan siber, namun juga dimanfaatkan oleh pelaku kejahatan siber untuk menghasilkan phishing yang lebih meyakinkan, malware adaptif, dan serangan berbasis rekayasa sosial yang semakin sulit dideteksi.

Selain itu, [12] menunjukkan bahwa kombinasi AI, blockchain, dan Software Defined Networking (SDN) menghasilkan sistem keamanan yang lebih adaptif dibandingkan penggunaan satu teknologi secara terpisah. Pendekatan tersebut memperlihatkan bahwa integrasi beberapa teknologi cerdas memberikan tingkat deteksi dan respons yang lebih tinggi terhadap serangan siber.

Meskipun demikian, sebagian besar penelitian masih berfokus pada peningkatan akurasi model AI. Aspek transparansi model (*Explainable AI*), ketahanan terhadap *adversarial attack*, serta konsumsi sumber daya komputasi masih menjadi tantangan yang belum banyak dibahas. Dengan demikian, penelitian mendatang perlu mengembangkan model AI yang tidak hanya akurat, tetapi juga transparan, efisien, dan mampu mempertahankan performa ketika menghadapi pola serangan baru.

Tabel 5. Sintesis Penelitian AI dan Machine Learning

PENULIS	FOKUS	KONTRIBUSI	KETERBATASAN
Shaukat Et Al. (2020)	Machine Learning	IDS berbasis ML	Belum membahas Explainable AI
Okdem & Okdem (2024)	AI Security	Otomasi deteksi ancaman	Studi kasus terbatas
Alshuaibi Et Al. (2025)	Adaptive ML	Pembelajaran adaptif	Validasi masih terbatas
Orpak (2025)	Generative AI	Peluang dan ancaman AI	Belum ada framework mitigasi
Shahzad Et Al. (2025)	AI + Blockchain	Pendekatan hibrida	Implementasi kompleks

Sumber. Olah Data

Blockchain Security

Blockchain berkembang menjadi salah satu teknologi yang menjanjikan dalam meningkatkan keamanan ekosistem big data karena menyediakan mekanisme penyimpanan data yang terdistribusi, transparan, dan sulit dimanipulasi. Berbeda dengan sistem basis data terpusat, blockchain mampu meningkatkan integritas data melalui mekanisme

konsensus dan pencatatan transaksi yang bersifat permanen.

Hasil sintesis menunjukkan bahwa [16] menekankan efektivitas blockchain dalam menjaga keamanan data pada sistem energi cerdas dan big data. Sementara itu, [17] menjelaskan bahwa blockchain mampu meningkatkan autentikasi, integritas data, dan ketahanan terhadap serangan manipulasi.

Penelitian terbaru oleh [8] mengidentifikasi bahwa blockchain tetap memiliki berbagai kerentanan, seperti serangan *51% attack*, *smart contract vulnerabilities*, dan eksploitasi protokol konsensus. Hasil tersebut diperkuat oleh [18] yang menunjukkan bahwa penerapan AI dalam mendeteksi anomali transaksi blockchain mampu meningkatkan efektivitas mitigasi serangan secara signifikan.

Selanjutnya, [9] mengemukakan bahwa integrasi blockchain dengan AI membuka peluang terbentuknya sistem keamanan yang bersifat desentralisasi dan cerdas. Integrasi tersebut memungkinkan pengambilan keputusan dilakukan secara otomatis tanpa mengurangi integritas data.

Meskipun menawarkan tingkat keamanan yang tinggi, sebagian besar penelitian masih menghadapi kendala pada aspek skalabilitas, interoperabilitas, serta konsumsi energi yang tinggi. Oleh karena itu, penelitian selanjutnya perlu mengembangkan model blockchain yang lebih ringan, efisien, dan mudah diintegrasikan dengan sistem big data modern.

Cybersecurity Governance

Hasil sintesis menunjukkan bahwa perkembangan teknologi keamanan tidak selalu diikuti oleh peningkatan kualitas tata kelola keamanan siber. Padahal, tata kelola merupakan faktor yang menentukan keberhasilan implementasi teknologi keamanan dalam organisasi.

[19] menjelaskan bahwa cybersecurity governance mencakup proses pengambilan keputusan, kebijakan keamanan, manajemen risiko, serta kepatuhan terhadap regulasi. Pendekatan tersebut kemudian dikembangkan oleh Melaku (2023) melalui kerangka kerja keamanan siber yang adaptif sehingga organisasi mampu menyesuaikan strategi keamanan sesuai perubahan ancaman.

Penelitian oleh [11] menunjukkan bahwa model *Three Lines of Defense* masih menjadi pendekatan yang banyak digunakan dalam mengelola risiko keamanan informasi. Namun demikian, model tersebut perlu disesuaikan dengan meningkatnya kompleksitas ancaman digital.

Selanjutnya, [5] menegaskan bahwa organisasi sektor publik mulai mengintegrasikan tata kelola keamanan informasi ke dalam strategi organisasi secara menyeluruh. Hal serupa ditemukan oleh [20] yang menunjukkan bahwa pemerintah daerah menghadapi tantangan berupa keterbatasan sumber daya manusia, anggaran, serta koordinasi antarlembaga.

Hasil sintesis memperlihatkan bahwa penelitian mengenai cybersecurity governance telah bergeser dari penyusunan kebijakan menuju pembangunan organisasi yang tangguh (*cyber resilience*). Namun demikian, belum banyak penelitian yang mengintegrasikan tata kelola dengan teknologi AI, blockchain, dan analitik big data secara bersamaan. Kondisi tersebut membuka peluang pengembangan model tata kelola keamanan siber yang lebih adaptif dan berbasis teknologi cerdas.

Tabel 6. Sintesis Penelitian Cybersecurity Governance

PENULIS	FOKUS	TEMUAN
Albalas Et Al. (2022)	Governance	Framework keamanan
Melaku (2023)	Adaptive Governance	Tata kelola dinamis
Valkenburg & Bongiovanni (2024)	Three Lines Model	Manajemen risiko
Magnusson Et Al. (2025)	Public Sector	Tata kelola sektor publik
Hossain Et Al. (2025)	Local Government	Tantangan implementasi

Sumber. Olah Data

Human Factors dan Security Awareness

Hasil sintesis menunjukkan bahwa faktor manusia masih menjadi penyebab dominan terjadinya insiden keamanan siber meskipun berbagai teknologi keamanan telah berkembang pesat. Sebagian besar serangan modern memanfaatkan kelemahan perilaku pengguna melalui teknik *phishing*, *social engineering*, penyalahgunaan kredensial, dan kelalaian dalam menerapkan kebijakan keamanan.

[21] menjelaskan bahwa perilaku pengguna merupakan komponen penting dalam sistem keamanan informasi karena keputusan individu sering kali menjadi titik masuk serangan siber. Selanjutnya, [22] menunjukkan bahwa pelatihan keamanan siber yang dilakukan secara berkelanjutan lebih efektif dibandingkan pelatihan satu kali karena mampu meningkatkan perubahan perilaku pengguna dalam jangka panjang.

Penelitian terbaru oleh [23] mengungkap bahwa tekanan waktu (*time pressure*) berpengaruh terhadap meningkatnya kesalahan pengguna ketika menghadapi ancaman keamanan siber. Sementara itu, [24] menemukan bahwa tingkat kesadaran keamanan di lingkungan pendidikan masih relatif rendah sehingga memerlukan strategi pelatihan yang berkelanjutan dan disesuaikan dengan karakteristik pengguna.

Dari perspektif kebijakan nasional, [25] menunjukkan bahwa pembangunan budaya keamanan siber harus menjadi bagian dari strategi nasional melalui kolaborasi antara pemerintah, organisasi, dan masyarakat. Temuan tersebut memperkuat pandangan bahwa keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada kesiapan sumber daya manusia dalam menerapkan praktik keamanan yang baik.

Secara keseluruhan, hasil sintesis menunjukkan bahwa penguatan security awareness perlu menjadi bagian integral dari cybersecurity governance. Program pelatihan berbasis simulasi, evaluasi perilaku pengguna secara berkala, serta pemanfaatan AI untuk mempersonalisasi materi pelatihan merupakan arah penelitian yang menjanjikan dalam meningkatkan ketahanan organisasi terhadap ancaman siber berbasis manusia.

Tabel 7. Sintesis Penelitian Human Factors

PENULIS	FOKUS	TEMUAN
Rohan Et Al. (2021)	Human Factors	Perilaku pengguna memengaruhi keamanan
Prümmer Et Al. (2023)	Training	Pelatihan berkelanjutan lebih efektif
Saputri & Syaifullah (2024)	Security Awareness	Tekanan waktu meningkatkan risiko
Netshiunda & Madzvamuse (2025)	Awareness	Kesadaran keamanan masih rendah
Muawwan (2021)	Cyber Sovereignty	Budaya keamanan mendukung ketahanan nasional

Sumber. Olah Data

KESIMPULAN

Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mensintesis perkembangan strategi keamanan siber dalam ekosistem big data melalui pendekatan Systematic Literature Review (SLR) berdasarkan pedoman PRISMA 2020. Berdasarkan hasil sintesis terhadap literatur yang dipublikasikan pada periode 2019–2025, dapat disimpulkan bahwa keamanan big data telah berkembang dari pendekatan konvensional yang berfokus pada perlindungan data menuju pendekatan yang lebih komprehensif dengan mengintegrasikan teknologi cerdas, tata kelola keamanan, dan faktor manusia.

Hasil kajian menunjukkan bahwa penerapan Artificial Intelligence (AI) dan Machine Learning (ML) memberikan kemampuan deteksi ancaman secara proaktif melalui analisis pola serangan dan identifikasi anomali secara real-time. Di sisi lain, teknologi blockchain berkontribusi dalam meningkatkan integritas data, autentikasi, transparansi, dan ketahanan terhadap manipulasi data melalui mekanisme desentralisasi dan kriptografi. Namun demikian, kedua teknologi tersebut masih menghadapi tantangan berupa skalabilitas, kompleksitas implementasi, ancaman terhadap model AI, serta kerentanan pada smart contract dan mekanisme konsensus blockchain.

Selain aspek teknologi, hasil penelitian juga menegaskan bahwa cybersecurity governance dan human factors merupakan komponen yang tidak dapat dipisahkan dalam membangun ketahanan keamanan siber. Tata kelola yang adaptif, kebijakan keamanan yang jelas, manajemen risiko, serta peningkatan kesadaran keamanan (*security awareness*) melalui pelatihan berkelanjutan menjadi faktor penting dalam mengurangi risiko serangan siber. Dengan demikian, efektivitas keamanan big data tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kesiapan organisasi dalam mengelola proses, kebijakan, dan sumber daya manusia secara terpadu.

Kontribusi utama penelitian ini adalah menyajikan sintesis literatur terkini yang mengintegrasikan lima perspektif utama, yaitu Big Data Security, Artificial Intelligence/Machine Learning, Blockchain Security, Cybersecurity Governance, dan Human Factors, sehingga memberikan gambaran yang lebih komprehensif mengenai perkembangan penelitian keamanan siber pada ekosistem big data. Hasil sintesis ini dapat menjadi referensi bagi akademisi, praktisi, maupun pembuat kebijakan dalam merancang strategi keamanan siber yang lebih adaptif, terintegrasi, dan berkelanjutan.

Penelitian ini memiliki keterbatasan karena hanya menggunakan artikel yang dipublikasikan pada rentang waktu 2019–2025 dan berasal dari basis data akademik yang telah ditentukan. Oleh karena itu, penelitian selanjutnya disarankan untuk memperluas cakupan basis data, mengintegrasikan pendekatan bibliometric analysis atau meta-analysis, serta mengevaluasi implementasi model keamanan berbasis AI, blockchain, dan Zero Trust Architecture pada berbagai sektor industri guna memperoleh pemahaman yang lebih mendalam mengenai efektivitas strategi keamanan siber dalam menghadapi ancaman yang terus berkembang

TINJAUAN PUSTAKA

[1] J. Moreno, E. B. Fernandez, M. A. Serrano, dan E. Fernandez-Medina, "Secure Development of Big Data Ecosystems," *IEEE Access*, vol. 7, hlm. 96604–96619, 2019, doi: 10.1109/ACCESS.2019.2929330.

[2] F. Rafiq, M. J. Awan, A. Yasin, H. Nobanee, A. M. Zain, dan S. A. Bahaj, "Privacy Prevention of Big Data Applications: A Systematic Literature Review," *Sage Open*, vol. 12, no. 2, Apr 2022, doi: 10.1177/21582440221096445.

[3] Y. A. Bena *dkk.*, "Big Data Governance Challenges Arising From Data Generated by Intelligent Systems Technologies: A Systematic Literature Review," 2025, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2025.3528941.

[4] P. Banasode dan S. Padmannavar, "Protecting and Securing Sensitive Data in a Big Data Using Encryption," *EAI Endorsed Transactions on Smart Cities*, vol. 0, no. 0, hlm. 163991, Jul 2018, doi: 10.4108/eai.13-7-2018.163991.

[5] L. Magnusson, S. Iqbal, P. Elm, dan F. Dalipi, "Information security governance in the public sector: investigations, approaches, measures, and trends," *Int. J. Inf. Secur.*, vol. 24, no. 4, Agu 2025, doi: 10.1007/s10207-025-01097-x.

[6] S. Okdem dan S. Okdem, "Artificial Intelligence in Cybersecurity: A Review and a Case Study," *Applied Sciences (Switzerland)*, vol. 14, no. 22, Nov 2024, doi: 10.3390/app142210487.

[7] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, dan M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, hlm. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[8] M. K. Siam *dkk.*, "Securing Decentralized Ecosystems: A Comprehensive Systematic Review of Blockchain Vulnerabilities, Attacks, and Countermeasures and Mitigation Strategies," 1 April 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/fi17040183.

[9] M. S. Al Jasem, T. De Clark, dan A. K. Shrestha, "Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems," 1 September 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/info16090765.

[10] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, hlm. 327–350, Sep 2023, doi: 10.3390/jcp3030017.

[11] B. Valkenburg dan I. Bongiovanni, "Unravelling the three lines model in cybersecurity: a systematic literature review," *Comput. Secur.*, vol. 139, Apr 2024, doi: 10.1016/j.cose.2024.103708.

[12] M. Shahzad, S. Rizvi, T. A. Khan, S. Ahmad, dan A. A. Ateya, "An Exhaustive Parametric Analysis for Securing SDN Through Traditional, AI/ML, and Blockchain Approaches: A Systematic Review," 1 Juni 2025, *Springer Science and Business Media B.V.* doi: 10.1007/s44227-024-00055-8.

[13] K. Orpak, "Generative AI and cybersecurity: Exploring opportunities and threats at their intersection," *Maandblad voor Accountancy en Bedrijfseconomie*, vol. 99, no. 4, hlm. 221–230, Sep 2025, doi: 10.5117/mab.99.149299.

[14] M. J. Page *dkk.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," 29 Maret 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.

[15] B. Kitchenham dan P. Brereton, "A systematic review of systematic review process research in software engineering," 2013, *Elsevier B.V.* doi: 10.1016/j.infsof.2013.07.010.

[16] M. K. Hasan *dkk.*, "Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations," 2022, *Hindawi Limited*. doi: 10.1155/2022/9065768.

[17] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, dan Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, hlm. 2490–2510, 2022, doi: 10.1109/TSC.2020.3038641.

[18] R. Shevchuk, V. Martsenyuk, B. Adamyk, V. Benson, dan A. Melnyk, "Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions," 1 Agustus 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/app15158330.

[19] T. Albalas, A. Modjtahedi, dan R. Abdi, "CYBERSECURITY GOVERNANCE: A SCOPING REVIEW," *International Journal of Professional Business Review*, vol. 7, no. 4, 2022, doi: 10.26668/businessreview/2022.v7i4.e629.

[20] S. T. Hossain, T. Yigitcanlar, K. Nguyen, dan Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," 1 Maret 2025, *Elsevier B.V.* doi: 10.1016/j.ugj.2024.12.010.

[21] R. Rohan, S. Funilkul, D. Pal, dan W. Chutimaskul, "Understanding of Human Factors in Cybersecurity: A Systematic Literature Review," dalam *2021 International Conference on Computational Performance Evaluation, ComPE 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, hlm. 133–140. doi: 10.1109/ComPE53109.2021.9752358.

[22] J. Prümmer, T. van Steen, dan B. van den Berg, "A systematic review of current cybersecurity training methods," *Comput. Secur.*, vol. 136, Jan 2024, doi: 10.1016/j.cose.2023.103585.

[23] A. M. Saputri dan S. Syaifullah, "DEVELOPMENTS AND TRENDS IN CYBERSECURITY AGAINST HUMAN FACTORS AND TIME PRESSURE USING BIBLIOMETRIC ANALYSIS," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 18, no. 1, hlm. 107, Jan 2024, doi: 10.22146/ijccs.92636.

[24] H. Netshiunda dan S. Madzvamuse, "A Systematic Literature Review of Cybersecurity Awareness and Strategy in Rural-Based Universities," *International Journal of Applied Research in Business and Management*, vol. 6, no. 5, Des 2025, doi: 10.51137/wrp.ijarbm.350.

[25] Muawwan, "Halaman: 171-184 Terakreditasi Peringkat 5 (SINTA 5) sesuai SK RISTEKDIKTI Nomor," 2021. [Daring]. Tersedia pada: http://ejurnal.ubharajaya.ac.id/index.php/JKI