Studi Komprehensif Keamanan Siber: Perbandingan Teknologi AI dengan Sistem Non-AI dalam Deteksi dan Pencegahan Ancaman

Yollandaru Yoga Santika[1*], Rianto Rianto[2], EIH Ujianto[3]
[1,2,3]Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
*email: yollandaru.6240211005@student.uty.ac.id

DOI: https://doi.org/10.31603/komtika.v9i1.13149

Received: 06-02-2025, Revised: 07-04-2025, Accepted: 15-04-2025

ABSTRACT

This research examines cybersecurity approaches in Indonesia, focusing on the implementation of Artificial Intelligence (AI) technology compared to non-AI systems in detecting and preventing threats. The study identifies the advantages of AI, such as its capabilities in large-scale data analysis, detection of suspicious patterns, and reduction of human error. The methodology follows PRISMA guidelines for systematic literature review. Findings reveal that while AI can enhance threat detection effectiveness and resilience against attacks, the adoption of this technology in Indonesia remains limited by infrastructure, resources, and technical expertise. This research is expected to provide insights for more proactive national cybersecurity policies and support the development of AI technology in future information security initiatives.

Keywords: *Cybersecurity, Artificial Intelligence, Non-AI Systems, PRISMA, Information Security Policy.*

ABSTRAK

Penelitian ini membahas pendekatan keamanan siber di Indonesia, dengan fokus pada penerapan teknologi Kecerdasan Buatan (*Artificial Intelligence/AI*) dibandingkan sistem non-AI dalam mendeteksi dan mencegah ancaman. Studi ini mengidentifikasi manfaat AI, seperti kemampuannya dalam analisis data skala besar, deteksi pola mencurigakan, dan mengurangi kesalahan manusia. Metodologi yang digunakan mengikuti pedoman PRISMA untuk tinjauan literatur. Studi ini menemukan bahwa meskipun AI dapat meningkatkan efektivitas deteksi ancaman dan ketahanan terhadap serangan, adopsi teknologi ini di Indonesia masih terbatas oleh infrastruktur, sumber daya, dan pengetahuan yang belum optimal. Temuan ini diharapkan dapat memberikan wawasan untuk kebijakan keamanan siber nasional yang lebih proaktif dan mendukung pengembangan teknologi AI dalam keamanan informasi di masa depan.

Keywords: Keamanan Siber, Kecerdasan Buatan, Sistem Non-AI, PRISMA, Kebijakan Keamanan Informasi.

PENDAHULUAN

Keamanan sistem informasi menjadi isu yang semakin krusial seiring dengan pesatnya perkembangan teknologi dan digitalisasi. Di Indonesia, perhatian terhadap keamanan sistem informasi terus meningkat, terutama dengan maraknya serangan siber yang menargetkan berbagai sektor, termasuk pemerintahan, perbankan, dan industri. Meskipun berbagai metode keamanan telah diterapkan, tantangan dalam mitigasi ancaman siber masih besar. Salah satu solusi yang berkembang secara global adalah pemanfaatan teknologi *Artificial Intelligence* (AI) dalam sistem keamanan informasi. AI memungkinkan sistem untuk mengidentifikasi pola anomali, mendeteksi ancaman dengan cepat, serta meningkatkan efisiensi dalam *merespons* insiden siber.

Berbagai penelitian telah menunjukkan bahwa penerapan AI dalam keamanan sistem informasi dapat meningkatkan efektivitas perlindungan data dan sistem. Contohnya, penelitian

yang dilakukan oleh Buczak dan Guven (2016) membahas bagaimana *machine learning* dapat meningkatkan deteksi intrusi jaringan dengan mengidentifikasi pola serangan secara *real-time*. Selain itu, studi lain oleh Sharmeen et al. (2022) menunjukkan bahwa AI dapat digunakan untuk menganalisis *malware* dan memprediksi serangan siber berdasarkan tren historis. Meskipun demikian, di Indonesia, adopsi teknologi AI dalam keamanan sistem informasi masih dalam tahap awal. Faktor seperti keterbatasan infrastruktur, kurangnya sumber daya manusia yang terampil, serta pemahaman yang terbatas mengenai manfaat AI dalam keamanan siber menjadi tantangan utama yang menghambat penerapan teknologi ini secara luas.

Penelitian ini bertujuan untuk mengidentifikasi pendekatan keamanan sistem informasi yang saat ini diterapkan di Indonesia, mengevaluasi perkembangan dan inovasi di bidang tersebut, serta meneliti bagaimana AI dapat diintegrasikan untuk meningkatkan efektivitas sistem keamanan informasi. Untuk mencapai tujuan tersebut, penelitian ini akan menjawab beberapa pertanyaan utama berikut:

1. Bagaimana kondisi terkini keamanan sistem informasi di Indonesia?
2. Bagaimana peran AI dalam meningkatkan keamanan sistem informasi dibandingkan dengan metode non-AI?
3. Apa saja tantangan utama yang dihadapi Indonesia dalam mengadopsi teknologi AI untuk keamanan sistem informasi?
4. Apa saja solusi dan rekomendasi untuk meningkatkan pemanfaatan AI dalam keamanan siber di Indonesia?

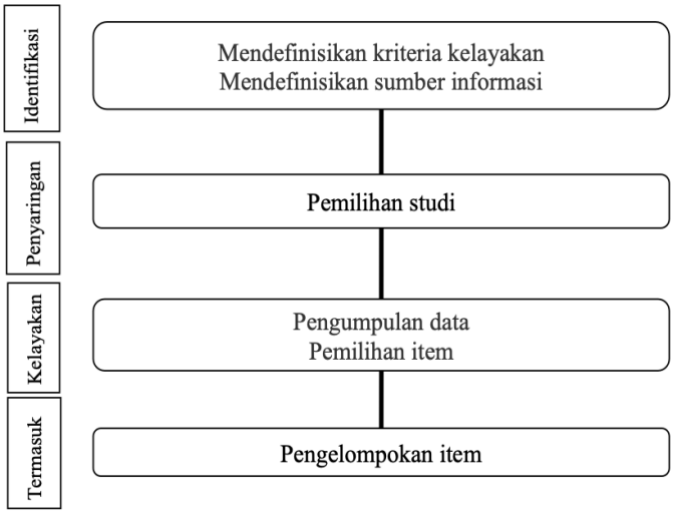
Selain itu, penelitian ini akan membahas perbandingan antara metode keamanan berbasis AI dan metode tradisional (non-AI) dalam keamanan siber. Beberapa aspek utama yang akan dianalisis meliputi:

- **Kecepatan dan akurasi deteksi ancaman:** AI memiliki kemampuan untuk menganalisis data dalam jumlah besar dan mendeteksi pola anomali dengan lebih cepat dibandingkan metode konvensional.
- **Kemampuan adaptasi terhadap ancaman baru:** Sistem berbasis AI dapat terus belajar dan beradaptasi dengan ancaman yang berkembang, sementara metode tradisional lebih statis dan membutuhkan pembaruan manual.
- **Efisiensi dalam mitigasi serangan:** AI dapat mengotomatisasi *respons* terhadap serangan siber, mengurangi intervensi manusia, dan meminimalkan kesalahan manusia (*human error*).
- **Keamanan data dan privasi:** Implementasi AI dalam keamanan siber juga memunculkan tantangan baru, seperti risiko bias dalam algoritma dan kemungkinan penyalahgunaan data.

Penelitian ini akan menggunakan studi literatur dari berbagai jurnal internasional untuk mengidentifikasi aplikasi AI dalam keamanan sistem informasi yang telah terbukti efektif di berbagai negara. Melalui analisis ini, diharapkan dapat diperoleh wawasan baru mengenai bagaimana AI dapat diintegrasikan secara optimal dalam sistem keamanan informasi di Indonesia. Temuan dari penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan keamanan siber di Indonesia serta menjadi referensi bagi penelitian lanjutan di bidang ini.

METODE

Penyusunan review ini disusun berdasarkan pedoman PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-analyses*)[2]. Langkah-langkah yang digunakan seperti pada Gambar 1.



Gambar 1. Tahapan Penelitian

Pencarian sistematis dilakukkan pada bulan September 2024 untuk menangkap studi yang ditulis dalam bahasa Indonesia dan Inggris ditemukan dalam *Google Scholar* dan Scopus Strategi pencarian dirangkum dalam Tabel 1. Hasil penelitian ini dimasukkan jika:

1) Penelitian asli yang ditulis mulai dari tahun 2020 dengan jumlah minimal sebanyak 25 dan termasuk dalam jurnal SINTA 2.
2) Penelitian yang berkaitan dengan Artificial Intelligence (AI) dan sistem keamanan Informasi.

Dalam pemilihan *paper* diperlukan kriteria yang jelas untuk memastikan bahwa studi yang digunakan relevan dan memiliki kualitas yang sesuai dengan tujuan penelitian. Kriteria ini terdiri dari kriteria inklusi, yang menentukan studi yang dapat dimasukkan dalam analisis, serta kriteria eksklusi, yang menetapkan batasan terhadap studi yang tidak memenuhi syarat. Berikut adalah kriteria yang digunakan dalam penelitian ini:

Tabel 1. Kriteria Pemilihan *Paper*

Kriteria	Deskripsi
Kriteria Inklusi	
Penelitian yang membahas keamanan informasi berbasis AI atau Non-AI	*Paper* yang secara eksplisit membahas metode AI dan Non-AI dalam keamanan siber.
Artikel yang dipublikasikan dalam 4 tahun terakhir	*Paper* yang masih relevan dengan perkembangan teknologi terbaru.
Paper yang tersedia dalam bahasa Inggris dan bahasa Indonesia	Studi yang dapat diakses dan dipahami oleh komunitas akademik lebih luas.
Artikel yang mencakup pendahuluan, metode, hasil, dan diskusi	*Paper* yang memiliki struktur penelitian lengkap untuk dianalisis.
Studi yang dipublikasikan dalam jurnal atau konferensi bereputasi	*Paper* yang memiliki kredibilitas tinggi berdasarkan sumber publikasi.

Kriteria	Deskripsi
Kriteria Eksklusi	
Paper yang hanya berupa komentar singkat atau editorial	Artikel yang tidak memiliki metodologi dan hasil penelitian yang jelas.
Studi yang tidak relevan dengan keamanan informasi	*Paper* yang tidak membahas aspek keamanan siber baik AI maupun Non-AI.
Artikel yang tidak memiliki akses penuh (hanya abstrak)	*Paper* yang tidak memungkinkan analisis lebih dalam karena keterbatasan akses.
Paper yang ditulis dalam bahasa selain Inggris dan Indonesia	Artikel yang sulit untuk diverifikasi dan dianalisis karena kendala bahasa.
Penelitian yang sudah terbit sangat lama (>4 tahun)	Studi yang sudah terbit terlalu lama tidak lagi relevan dengan perkembangan teknologi terbaru.

Tabel 2 mencerminkan alur proses pencarian penyaringan dengan PRISMA:

Tabel 2. ***Search Strategy***

Base Data	***Keywords***
Scopus	(((*Cybersecurity*))) *OR* (*cyberattacks*) *OR* (*attacks*) *OR* (*Ransomware*) *AND* (*explainable AI*) *AND* (*machine*) *AND* (*preventattion*)))
Google *Scholar*	(((*Networks security*))) *OR* (sistem keamanan) *OR* (keamanan jaringan) *OR* (ISO/IEC 27005:2018) *AND* (*penetration data*) *OR* (deteksi serangan data) *OR* (seteksi serangan), *AND* (enkrispsi data), *AND* (*malware detection*) *OR* (deteksi malware), *AND* (steganografi)))

Semua duplikat dihapus secara otomatis dan manual, lalu di filter dalam tahapan judul jurnal, metode, kelebihan dan kekurangan sehingga menghasilkan studi terpilih yang di tulis disini. Pemilihan studi kualitas dan ekstrasi data, menghapus duplikat dan menyaring judul. Penelitian tentang AI dilakukan dengan metode PRISMA. Ekstrasi data menggunakan tabel Microsoft Excel. Hasil pemilihan artikel sesuai prosedur, jumlah studi yang diambil untuk tinjauan sistematis dan kualitas studi dipilih cukup baik. Penilaian lengkap dapat dilihat pada Tabel 2.

Teknik pengumpulan data yang dilakukkan dengan manual, menggunakan instrumen tabel ekstrasi data yang terdiri dari, nomor, penulis, tahun, nama jurnal, tipe artikel, topik, metode, hasil pembahasan, dan kesimpulan. Informasi yang diambil dari setiap artikel terdiri dari 1) penjelasan tentang keamanan jaringan atau sistem informasi; 2) ancaman atau serangan keamanan; 3) teknologi keamanan yang ada sebagai perlindungan.

HASIL DAN PEMBAHASAN

A. Seleksi *Paper*

Seleksi *paper* seperti pada Tabel 3 dimulai dengan menentukan topik penelitian yang spesifik seperti keamanan informasi berbasis kecerdasan buatan atau manajemen resiko dalam keamanan siber. Setelah ditentukan, kata kunci utama kemudian dibuat seperti "*cybersecurity AI*", "*network security risk management*", "*blockchain information security*" dan istilah yang terkait lainnya.

Kemudian, google scholar dipilih sebagai pencarian awal karena jangkauannya yang luas dan kemampuan untuk memberikan hasil yang bervariasi dari berbagai publikasi ilmiah baik jurnal maupun konferensi. Untuk memastikan bahwa informasi yang ditemukan tetap relevan dengan teknologi dan kemajuan terbaru dalam keamanan data, filter pencarian diatur untuk

menampilkan hasil publikasi dalam 4 tahun terakhir. Dari pencarian melalui google scholar ini, puluhan bahkan ratusan *paper* ditemukan. Dengan mengacu pada kata kunci yang telah dibuat, membaca judul serta abstrak, *paper* yang mencantumkan metode berbasis kecerdasan buatan, metodologi khusus dalam manajemen keamanan, atau teknologi yang inovatif dalam penanganan risiko tersaring menjadi sekitar 40-50 *paper*.

Langkah selanjutnya adalah mempersempit pencarian di Scopus. Scopus memiliki fitur yang lebih mendalam untuk menilai kualitas publikasi. Pencarian dalam Scopus sama seperti sebelumnya yaitu menggunakan kata kunci yang telah dibuat. Prioritas dalam Scopus ini adalah *paper* yang memiliki banyak kutipan atau muncul dalam jurnal yang bereputasi. Selanjutnya, dilakukan seleksi yang lebih mendalam dengan membaca pendahuluan dan kesimpulan. *Paper* yang menyajikan temuan baru atau membahas keamanan informasi baik berbasis AI maupun non-AI yang tetap menjadi pertimbangkan. Seleksi juga dilakukan pada *paper* yang dianggap memiliki topi atau metode yang serupa dieliminasi agar terdapat keberagaman metode dan sudut pandang.

Dari hasil seleksi-seleksi yang telah dilakukan, tersisa 30 *paper* yang dianggap paling relevan dan memiliki kualitas tinggi. *Paper* tersebut kemudian dianalisis seperti pada Tabel 4 berikut ini.

Tabel 3. Langkah Seleksi *Paper*

Langkah	Deskripsi
1. Menentukan topik penelitian	Menetapkan fokus penelitian, seperti keamanan informasi berbasis AI atau manajemen risiko keamanan siber.
2. Membuat kata kunci	Menyusun kata kunci utama seperti "*cybersecurity AI", "network security risk management",* dan *"blockchain information security".*
3. Pencarian di Google Scholar	Melakukan pencarian awal dengan filter 4 tahun terakhir untuk mendapatkan publikasi terbaru.
4. Seleksi berdasarkan Judul dan Abstrak	Memilih *paper* yang mencantumkan metode berbasis AI, manajemen keamanan, atau inovasi dalam mitigasi risiko.
5. Penyaringan di Scopus	Mempersempit pencarian di Scopus dengan mempertimbangkan kutipan tinggi dan jurnal bereputasi.
6. Evalusi Pendahuluan dan Kesimpulan	Membaca pendahuluan dan kesimpulan untuk menilai relevansi temuan serta perbandingan AI dan non-AI.
7. Eliminasi *Paper* yang Redundan	Menghapus *paper* yang memiliki metode atau topik serupa untuk memastikan keberagaman sudut pandang.
8. Finalisasi *Paper*	Memilih 30 *paper* terbaik untuk dianalisis lebih lanjut dalam penelitian.

Tabel 4. Analisis Jurnal

Penulis	Nama Jurnal	Topik	Metode	Hasil Pembahasan	Kesimpulan
Ansari et al., 2022	The Impact and Limitations of Artificial Intelligence in Cybersecurity	AI, Keamanan Siber	Kualitatif	AI: *Deep Learning, Simulation Modelling, Social Network Analysis, Machine Translation, Machine Learning, Robotics, Internet of things, Graph Analytics, Audio Analytics, Visualization, Virtual Personal Assistant, Natural Learning Processing.* Keamanan Siber: *Spear Phishing, Phishing, SQL Injection, Ransomware, Malware, DNS Attacks, Denial Of Service Attacks.*	AI (*Artificial Intelligence*) telah memberi dampak jelas bagi keamanan siber.
Capuano et al., 2022	Explainable Artifical Intelligence in CyberSecurity: A Survey	Keamanan siber, pradigma keamanan	Deskriptif	Tantangan keamanan siber:1. diperlukan banyak formalisme. XAI merupakan target multidivisi yang tidak dapaat dicapai oleh pendekatan teoritis, dan perlu peningkatan formalisme. 2. human in the loop. membangun sisber yang dapat dipahami manusia 3. kemampuan menjelaskan, dimana kemampuan tersebut harus transparan	Keamanan siber merupakan tempat AI menganalisis kumpulan data dan melacak keamanan, ancaman, dan perilaku kejahatan.
Kaur et al., 2023	Artificial intelligence for cybersecurity: literature review and future research directions	Deteksi, perlindungan, Pemulihan , Pembelajaran Cyberattacks	Deskriptif	klasifikasi komperhensif potensi AI untuk meningkatkan keamanan siber. identifikasi peluang mengenai metode AI, representasi data, pengembangan keamanan siber AI di era transformasi digital dan poikrisis saat ini	Banyak teknik AI diterapkan dalam domin keamananan siber dan keamanannya melalui teknoligi. literatur yang dianalisis yaitu 1. taksonomi AI yang disajikan dalam keadaaan siber 2. frekuensi publikasi menurut tahun 3. frekuensi publikasi menutut wilayah geogradis, 4. jenis kontribusi kemanaan 5. jenis teknik AI yang digunakan

Beaman et al., 2021	Ransomware: react advances, analysi, challenges and future research directions	Ransomware, keamanan siber, antivirus, malware, pencegahan dan deteksi ransomware	Kuantitatif	Poin solusi penanggulangan ransomware: 1. Analisis dinamis: efektif tapu bisa dihandiri. 2. Generalisasi terbatas: tidak berlaku untuk semua varian. 3. Pencefahan &pencadangan membatasi kerusakan, tetaoi memberani. 4. Pembelajaran mesin: deteksi pola butuh data serangan. 5. RaaS mempercepat serangan. 6.Antivirus terbatas: kurang efektif untuk varian. Perlindungan folder: efektif namun sulit diatur.	Teknik deteksi ransomware sebagian besar berputar pada honeypot,analisis lalulintas jarindan, dan pendekatan berbasis pembelajaran bisanis. teknis pencegahan pada kontrol akses, pencadangan data dan kunci, ser
Jain et al., 2021	Online social networks security and privacy: comprehensive review analysis	social networks, cyberbullying, cyber grooming	Kualitatif	Ada berbagai masalah keamanan dan privasi terkait informasi yang dibagikan pengguna, terutama konten pribadi. Penyerang dapat menyalahgunakannya, terutama jika anak-anak menjadi sasaran. Makalah ini meninjau ancaman keamanan dan privasi di jejaring sosial, serangan OSN pada aplikasi web, serta solusi dan pendekatan defensif. Selain itu, dibahas tantangan dan pedoman untuk meningkatkan kepercayaan di jejaring sosial.	Analisis Dinamis: Efektif, bisa dihindari. 2. Generalisasi: Tidak semua varian. 3. Kontrol Akses & Cadangan: Batasi kerusakan, beban tinggi. 4. Pembelajaran Mesin: Deteksi pola umum, butuh serangan aktif. 5. RaaS: Mudah serang, naik frekuensi. 6. Antivirus: Efektif lama, kurang di varian baru.7. Perlindungan Folder: Efektif, perlu atur manual.
Kuzlu et al., 2021	Role of Artificial intelligence in the internet of things (IoT) cybersecurity	Artificial Intelligence, Internet of Things (IoT), Cybersecurity	Kualitatif	Solusi keamanan siber mencakup perangkat keras tahan gangguan, pembaruan, enkripsi, autentikasi dua faktor, dan deteksi anomali. Botnet ditangani dengan antivirus dan penghindaran tautan mencurigakan, serangan DoS dengan antivirus, brickerbot dengan autentikasi, fuzzing dengan sanitasi input, dan peracunan data dengan deteksi outlier.	Penerapan AI dalam keamanan siber dan tantangan yang dihadapi, serta menyoroti risiko baru dari IoT dan AI dalam jaringan besar seperti kota pintar. Tujuannya adalah untuk memberikan pemahaman dan alat untuk melindungi sistem IoT dari ancaman siber
Ismayanti & Rantelinggi, 2024	Simulasi Penggunaan Blockchain pada keamanan jaringan internet of things menggunakan pin	blockchain, internet of things (IoT), simulasi, keamanan, smart contract	Kualitatif	Implementasi blockchain berlangsung dengan menggunakan controller untuk mengontrol semua pin yang terdapat pada emulator. Sehingga pada saat pin dinyalakan atau dimatikan akan menampilkan riwayat transaksi pada setiap terminal.	Blockchain pada IoT meningkatkan keamanan transaksi dengan enkripsi data anonim yang hanya dapat diakses oleh pengirim dan penerima, melindungi informasi dari ancaman.

	emulator model publik blockchain				
Umar et al., 2024	Security Analysis of Learning Management System Using Penetration Testing with ISSAF Framework	Security, LMS, Pentest, Kali Linux	Deskriptif kuantitatif	Pemindaian menemukan kerentanan tinggi seperti Cross Site Scripting (DOM), risiko sedang pada JS Library dan X-Frame-Options, serta risiko rendah seperti Anti-CSRF Token dan Cookie tanpa HttpOnly/SameSite, dan isu informasional seperti Sensitive URL.	Dari penelitian yang dilakukan dengan tidak adanya anti-clickjacking X-Frame - Option, clickjacking merupakan teknik serangan agar target dapat melakukan klik pada area tertentu yang menguntungkan bagi hacker
Sulistiadi & Salman, 2023	Ransomware Attacks Threat Modeling Using Bayesian Network	Ransomware, Risk Assessment, Threat Modeling, Bayesian Network, EPSS	Kuantitatif	Model ancaman ransomware berbasis Bayesian Network menganalisis risiko serangan dengan probabilitas tertinggi 0.046534. EPSS lebih akurat daripada CVSS, memudahkan identifikasi dan mitigasi.	1. Fokus: Hanya "likelihood". 2. Kekurangan: Perlu gabungan "likelihood" & impact. 3. Impact: Dampak serangan pada aset. 4. Saran: Tambahkan faktor "impact". 5. Manfaat: Tingkatkan akurasi penilaian risiko.
Rafrastara et al., 2023	Performance Improvement of random forest algorithm for malware detection on imbalanced dataset using random under-samplinf method	Random forest, imbalanced dataset, random under-sampling, malware, classification.	Kuantitatif	Deteksi malware semakin sulit, sehingga pembelajaran mesin menjadi fokus utama. Penelitian ini menguji algoritma Random Forest yang dioptimalkan, dengan hasil recall 98,3%, lebih tinggi dari kNN (96,6%), Naïve Bayes (91,4%), dan Regresi Logistik (96,1%).	Random Under Sampling dan Random Forest efektif untuk deteksi malware.
Emmanuel & Maulany, 2023	Penilaian Resiko SIstem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing aHouse	Penilaian risiko ABASE IPH mengidentifikasi 5 aset, 4 container, dan 13 area concern, dengan 7 membutuhkan mitigasi, berdasarkan ISO/IEC 27001:2013.	Kualitatif	Penilaian risiko ABASE IPH mengidentifikasi 5 aset, 4 container, dan 13 area concern, dengan 7 membutuhkan mitigasi. Suricata diinstal di VPS untuk deteksi serangan, unggul dibanding Snort dalam memblokir Syn Flood, Port Scanning, dan Ping of Death.	Penilaian risiko ABASE IPH mengidentifikasi 5 aset, 4 container, dan 13 area concern, dengan 7 membutuhkan mitigasi. Rencana kontrol risiko mengacu pada ISO/IEC 27001:2013. Suricata unggul dibanding Snort dalam deteksi serangan jaringan, dengan kecepatan dan analisis lebih baik.

Rivaldi & Marpaung, 2023	Penerapan sistem keamanan jaringan menggunakan intrusion prevention system berbasis suricata		Kuantitatif	Penilaian risiko ABASE IPH mengidentifikasi 5 aset, 4 container, dan 13 area concern, dengan 7 membutuhkan mitigasi. Suricata diinstal di VPS untuk deteksi serangan, unggul dibanding Snort dalam memblokir Syn Flood, Port Scanning, dan Ping of Death.	Penilaian risiko ABASE IPH mengidentifikasi 5 aset, 4 container, dan 13 area concern, dengan 7 membutuhkan mitigasi. Rencana kontrol risiko mengacu pada ISO/IEC 27001:2013. Suricata unggul dibanding Snort dalam deteksi serangan jaringan, dengan kecepatan dan analisis lebih baik.
Tri Julianto et al., 2024	Improving Algorithm Performance using Feature Extraction for Ethereum Forecasting	lgorithms, ethereum, eature extraction, forecasting	Kuantitatif	Penelitian ini menunjukkan bahwa Ekstraksi Fitur meningkatkan kinerja algoritma, khususnya Jaringan Syaraf Tiruan, Pembelajaran Mendalam, dan Mesin Vektor Pendukung, dengan penerapan PCA dan ICA. Hasil terbaik ditunjukkan oleh Jaringan Syaraf Tiruan menggunakan ICA, dengan nilai RMSE optimal sebesar 38,102 ± 31,093 (rata-rata mikro: 48,600 ± 0,000).	ICA meningkatkan kinerja model. Penelitian ini terbatas pada Feature Extraction, tiga algoritma (Neural Network, Deep Learning, SVM), dan dataset Ethereum; penelitian selanjutnya dapat mencoba Feature Selection, lebih banyak algoritma, dan menambah mata uang kripto lain.
Pratiwi & Ermaya, 2024	Implementation of Blockchain technology on accounting information system for transacction security and data reliability	Blockchain, Accounting Information Systems, Security, Data Reliability	Kualitatif deskriptif	1. Blockchain adalah teknologi buku besar digital terdistribusi dengan desentralisasi, transparansi, dan keamanan tinggi. 2. Cocok untuk transaksi dan pelaporan perusahaan besar. 3. Keamanan terjamin melalui desentralisasi dan kriptografi, butuh literasi digital tinggi. 4. Blockchain menghasilkan data terpercaya dan tahan manipulasi. 5. Tantangan: skalabilitas, biaya, dan rendahnya literasi digital di Indonesia..	Blockchain merevolusi teknologi informasi dengan keamanan, transparansi, dan desentralisasi yang tinggi, terutama dalam akuntansi. Teknologi ini menjanjikan peningkatan efisiensi dan integritas data. Namun, implementasinya di Indonesia masih terbatas karena tantangan seperti biaya tinggi, rendahnya pemahaman publik, dan kesulitan migrasi sistem.
Arif Indra Irawan et al., 2024	*Implementation of QR Code Attendance Security System Using RSA and Hash Algorithms*	Sistem Autenikasi, Kode QR, RSA, Hash	Kuantitatif	Pengujian kinerja aplikasi Android menunjukkan bahwa QR terenkripsi RSA 1.024 bit lebih lambat 0,36 detik dibanding tanpa enkripsi, namun lebih cepat 0,42 detik dibanding RSA 2.048 bit. RSA 2.048 bit mengonsumsi 57,4 mJ lebih banyak dibanding RSA 1.024 bit, dan 88,5 mJ lebih banyak dibanding tanpa enkripsi.	Sistem autentikasi QR dengan RSA dan hash mencegah pemalsuan, menjaga integritas data. Kinerja diuji dengan waktu eksekusi, jarak pembacaan, dan perangkat Android. RSA efektif mencegah presensi ilegal, dengan keterlambatan 12 detik dan konsumsi energi 0,09 J per jam. Algoritma AES disarankan untuk mempercepat proses.

Darmi et al., 2024	Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks	IT Governance; Information System Security; COBIT 2019	Kuantitatif	UUniversitas XYZ memiliki kapabilitas APO12 dan BAI10 di Level 2, dengan target Level 4. APO12 mencapai 75% dan BAI10 72% di Level 3. Gap 2 level perlu diatasi, sementara tantangan implementasi COBIT 2019 mencakup perubahan kepemimpinan dan lingkungan bisnis.	Identifikasi manajemen di Universitas XYZ menunjukkan kapabilitas APO12 dan BAI10 di Level 2, dengan gap menuju Level 4. Untuk peningkatan, perlu memperbarui skenario risiko, menyiapkan kontrol deteksi, dan menyepakati cakupan konfigurasi secara terstruktur.
Umam & Muslih, 2023	Enkripsi Data Teks DenganAES dan Steganografi DWT	Advanced Encryption Standard, Steganografi, Transformasi Kosinus Diskrit	Kuantitatif	Audit enkripsi di Dinas Kominfo Lampung Selatan menunjukkan AES menghasilkan ciphertext dan waktu proses. Citra stego menggunakan format *jpg lebih baik dari *bmp dalam MSE dan PSNR, dengan resolusi tinggi meningkatkan kualitas. Penambahan karakter menurunkan kualitas citra, dengan waktu komputasi rata-rata 0,6-0,8 detik.	Implementasi AES 128 Bit berhasil enkripsi dan dekripsi pesan, sementara steganografi DWT menyembunyikan pesan dalam citra digital dengan kualitas MSE 0,16-0,26 dB dan PSNR 46,27-52,2 dB. Pengembangan dapat mencakup metode steganografi lain dan media audio/video.
Fachrurozy et al., 2023	Embedded Wids Kismet Sebagai Perangkat Deteksi Serangan Data Link Layer Wi-Fi Access Point	Confusion Matrix, Kismet, Raspberry Pi,WIDS, Wi-Fi.	Kuantitatif	Pengujian deteksi serangan Wi-Fi menggunakan Kismet di Raspberry Pi mengidentifikasi Deauthentication Flood, Evil Twin, WPS Bruteforce, dan KRACK. Akurasi deteksi tertinggi untuk Evil Twin (99,39%) dan KRACK (99,83%), dengan WPS Bruteforce terendah (96,42%).	IImplementasi WIDS Kismet di Raspberry Pi 4 berhasil deteksi serangan, dengan efektivitas tertinggi pada Evil Twin (recall 100%) dan terendah pada WPS Bruteforce (1,77%). Sistem ini 10 kali lebih murah dari Cisco Meraki. Penelitian selanjutnya dapat mengeksplorasi perangkat, ELK stack, penyimpanan, dan antena Wi-Fi terbaru.
Hartinah et al., 2023	Deteksi Malware Ransmware Berdasarkan Panggilan API dengan Metode Ekstrasi Fitur N-gram dan TF-IDF	Ransomware, Panggilan API, Machine Learning, Binary Classification, N-gram, TF-IDF	Kuantitatif	1. Environment: Menggunakan PC core i7, RAM 16 GB, OS Linux 18.04, dan Cuckoo Sandbox. 2. Ekstraksi Fitur: N-gram 1,2 (unigram dan bigram) dengan TF-IDF dan batas 800 fitur. 3. Evaluasi Model: Akurasi 94% pada data latih, 83% pada varian baru. 4. Error Rate: Tertinggi 10% pada data latih, 30% pada data baru. 5. Interpretasi: SVM dan eli5 mengidentifikasi 26 fitur API kunci untuk deteksi ransomware yang akurat.	Penelitian ini mengembangkan model deteksi ransomware menggunakan fitur panggilan API, dengan akurasi 94% pada data latih dan 83% pada data uji dengan varian baru. Model ini efektif mendeteksi ancaman berkat 26 fitur API yang konsisten di berbagai varian ransomware.

D. Y. D. Pratiwi & Adrian, 2024	Deteksi dan Mitigasi Serangan Distributed Denial of Service Pada Defined Network	distributed denial of service; iptables; snort; software defined network	Kuantitatif	Implementasi Snort dan Iptables efektif dalam mendeteksi dan mencegah DDoS, meskipun penelitian terbatas pada tiga jenis tools. Pengembangan lebih lanjut diharapkan untuk meningkatkan efektivitas sistem.	Snort pada SDN mendeteksi serangan DDoS dengan akurasi 95% (slowhttptest), 90% (slowloris), dan 100% (LOIC), dengan waktu deteksi rata-rata 0,72 detik. Iptables memblokir serangan dalam 0,91 detik hingga 1,89 detik, menjaga ketersediaan SDN. Penelitian terbatas pada tiga jenis serangan.
Ernawati et al., 2024	Case Study In Network Security System Using Random Port Knocking Method On The Principles Of Availability, Confidentiality And Integrity	Availability Confidentiality Integrity Network Security Random Port Knocking	Kuantitatif	Metode RPK dalam keamanan jaringan menunjukkan kinerja baik dengan ketersediaan 99,97%, kerahasiaan 100%, dan waktu *respons* rata-rata 0,22 detik. RPK efektif mencegah pemindaian port dan serangan brute force, serta dapat mengamankan proses login dengan otomatis mengubah port dan memblokir IP. Penelitian ini menambahkan prinsip ketersediaan dan integritas, berbeda dengan studi sebelumnya yang hanya fokus pada kerahasiaan.	RPK efektif dengan ketersediaan 99,97%, kerahasiaan 100%, *respons* 0,22 detik, dan akurasi pemblokiran 100%. Mencegah serangan brute force dan port scanning, namun kurang pada ketersediaan dan integritas. Pengujian terbatas pada tiga parameter, perlu penambahan autentikasi dan kontrol akses. Disarankan untuk menambahkan port HTTP, FTP, dan pertimbangkan serangan seperti DoS, Man in the Middle, dan DNS Poisoning.
Arifin et al., 2023	Audit Keamanan Sistem Informasi Euclid Menggunakan Framework Cobit 5 pada PT. XYZ	audit, capability level, COBIT 5, DSS05, sistem informasi	Kuantitatif	EuClid adalah aplikasi PT. XYZ untuk pengajuan proposal dan pengelolaan administrasi. Masalah utama mencakup laporan hilang, risiko peretasan, dan kesulitan akses. Proses pengajuan melibatkan staf hingga manajemen. COBIT 5.0 PAM menunjukkan kematangan IT di level 1 dengan pencapaian 62,5%, dan keamanan belum dikelola dengan baik.	Audit keamanan Sistem Informasi EuClid di PT. XYZ dengan framework COBIT 5 pada domain DSS05 menunjukkan pencapaian nilai antara 59,63% hingga 65,36%, dengan peringkat Largely Achieved. Beberapa kriteria masih belum terpenuhi. Strategi untuk mencapai level 1 meliputi pelatihan keamanan informasi, penentuan pihak terlibat, dan evaluasi hasil kerja.
Ridwan et al., 2020	Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat	teganografi, Discrete Cosine Transform, DCT, Kriptografi, AES-192, Advanced Encryption Standard.	Kuantitatif	Sistem memiliki dua tampilan utama: **Embed** untuk menyisipkan file rahasia ke dalam file cover menggunakan AES-192 dan DCT, dan **Extract** untuk mengembalikan file asli dari stego image. Uji coba dengan berbagai file cover menunjukkan PSNR 48,44 dB dan MSE 1,39, memastikan kualitas citra baik dan ukuran file hasil Extract identik dengan aslinya.	Penelitian aplikasi keamanan dokumen digital dengan steganografi DCT dan AES-192 menunjukkan bahwa waktu proses embed dan extract tergantung pada ukuran file. Aplikasi ini meningkatkan keamanan, namun perlu perbaikan dalam kecepatan proses, algoritma steganografi, dan dukungan untuk file video dan audio.

Isnaini et al., 2023	Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa	isk analysis, ISO 27005:2019, Simpel Desa.	Kualitatif	Risiko yang didapatkan dari aplikasi Simpel Desa yang paling tinggi yaitu ketika ancaman risiko yang terjadi server down.	Analisis risiko aplikasi Simpel Desa di Kantor Desa Cingebul, berdasarkan ISO 27005:2019, mengidentifikasi 17 risiko, dengan rekomendasi penanganan mencakup perlindungan peralatan, pemeliharaan, keamanan kabel, instalasi perangkat lunak, dan pencadangan informasi. Penelitian selanjutnya disarankan untuk analisis risiko lebih spesifik di pusat aplikasi.
Hikam et al., 2024	Analisis manajemen risiko informasi menggunakan iso/iec 27005:2018 (studi kasus: PT XYZ)	ISO/IEC 27002:2022, ISO/IEC 27005:2018, Risk Assesment, ISMS	Kualitatif	PT XYZ menganalisis risiko keamanan informasi berdasarkan ISO 27005:2019, mengidentifikasi aset penting, dan mengelompokkan ancaman berdasarkan dampaknya. Risiko dievaluasi untuk menentukan prioritas penanganan dan pengendalian yang diperlukan, fokus pada perlindungan aset untuk mengurangi dampak negatif.	Penelitian mengidentifikasi 6 risiko pada aset utama yang perlu dikendalikan: 2 pada hardware, 1 pada network, dan 3 pada software. Rekomendasi akan diberikan untuk mengurangi kemungkinan ancaman dan dampaknya.
Ocha Safira et al., 2023	Analisis Manajemen Bandwith dan Keamanan Jaringan Menggunakan Metode Hierarchical Token Bucket dan Port Knocking Pada Router Mikrotik	Hierarchical Token Bucket, Bandwidth, Port Knocking	Kuantitatif (*sniffing dan port knocking*)	Penelitian ini mengevaluasi metode Hierarchical Token Bucket (HTB) yang berhasil mengendalikan bandwidth, dengan rata-rata download 9.0 Mbps dan upload 9.6 Mbps. Port blocking dan port knocking efektif memblokir port 443. Pengujian QoS menunjukkan delay 0,007 ms, jitter 0,0008 ms, throughput 73,059 kbps, dan tanpa packet loss, menegaskan efektivitas manajemen bandwidth dan keamanan jaringan.	Penelitian ini menunjukkan bahwa metode Hierarchical Token Bucket (HTB) mengelola bandwidth dengan rata-rata download 9.00 Mbps dan upload 9.06 Mbps. Port blocking dan port knocking efektif dalam mengatur penggunaan bandwidth dan keamanan jaringan, termasuk untuk IP Public Perumdam Tirta Satria.
Panggabean & Soewito, 2023	Analisis keamanan infrastruktur jaringan berdasarkan Cyber kill chain framework	Infrastructure Security Analysis, Security Gaps, Cyber Kill Chain Framework	Kuantitatif	Beberapa masalah telah berhasil dideteksi dengan baik, namun celah keamanan masih ada, sebagaimana terlihat dari pengujian yang dilakukan dan kurangnya respon sistem keamanan perusahaan.	Pendekatan Cyber Kill Chain Framework menunjukkan bahwa pengelolaan keamanan infrastruktur perusahaan masih memiliki celah. Beberapa masalah terdeteksi, tetapi respon sistem keamanan kurang memadai. Penelitian ini terbatas pada pengujian yang belum kompleks, dan perusahaan belum siap menghadapi skenario serangan.

B. Perbandingan Metode

Dari hasil analisis seperti yang tampak pada tabel 2 diatas, kemudian di klasifikasikan berdasarkan metode untuk melihat keunggulan dari masing-masing metode yang digunakan seperti pada tabel 3 berikut ini:

Tabel 5. Perbandingan Jurnal

NO	JURNAL	METODE	KELEBIHAN	KEKURANGAN
		AI		
1	Ansari et al., 2022 – Analisis Dampak AI dalam Keamanan Siber	Menggunakan analisis teoritis terkait aplikasi AI dalam deteksi ancaman.	Menyediakan pemahaman holistik tentang kekuatan AI dalam mendeteksi ancaman lebih cepat.	Tidak menawarkan studi kasus atau data eksperimen langsung.
2	Ramanpreet et al., 2023 – Literature Review AI untuk Keamanan Siber	Ulasan literatur tentang peran AI, serta identifikasi gap dan peluang penelitian.	Memberikan gambaran menyeluruh dan mengidentifikasi arah penelitian AI ke depan.	Pendekatan ini tidak menyediakan solusi praktis untuk diimplementasikan langsung.
3	Rafrastara et al., 2023 – Peningkatan Algoritma Random Forest untuk Deteksi Malware	Random under-sampling pada dataset yang tidak seimbang untuk meningkatkan kinerja deteksi malware.	Meningkatkan akurasi algoritma Random Forest pada dataset yang bias.	Metode ini memerlukan tuning yang hati-hati untuk mencegah hilangnya data penting.
4	Murat et al., 2020 – Peran AI dalam Keamanan IoT	Penggunaan AI untuk deteksi anomali dalam perangkat IoT.	Mendukung otomatisasi dan deteksi cepat pada jaringan IoT.	Membutuhkan dataset IoT yang besar dan beragam untuk akurasi yang lebih tinggi.
		BLOCKCHAIN		
1	Ismayanti, C.A., dan Rantelinggi, P.H., 2024 – Simulasi Blockchain untuk IoT	Simulasi penggunaan blockchain publik untuk keamanan jaringan IoT.	Memberikan keamanan tambahan dalam transfer data IoT, yang krusial untuk sistem terbuka.	Penggunaan blockchain publik masih membutuhkan daya komputasi tinggi dan memerlukan enkripsi tambahan.
2	Pratiwi, A.E., dan Ermaya H.N.L., 2024 – Blockchain untuk Sistem Informasi Akuntansi	Implementasi blockchain dalam sistem informasi akuntansi untuk keamanan transaksi.	Memastikan keamanan dan keandalan data akuntansi, sehingga cocok untuk aplikasi finansial.	Memerlukan infrastruktur yang kompatibel dengan teknologi blockchain.

RANSOMWARE				
1	Craig et al., 2021 – Tantangan dalam Penanganan Ransomware	Analisis perkembangan ransomware dan tantangan dalam deteksi dan reaksi.	Identifikasi pola serangan ransomware membantu dalam persiapan langkah pencegahan.	Tidak ada solusi praktis untuk mendeteksi atau mencegah serangan yang sedang berlangsung.
2	Sulistiadi dan Salman, 2023 – Pemodelan Ancaman Menggunakan Bayesian Network	Penggunaan jaringan Bayesian untuk pemodelan ancaman ransomware.	Metode ini memberikan visualisasi probabilitas serangan, memudahkan dalam pengambilan keputusan.	Membutuhkan data historis serangan untuk akurasi model yang lebih tinggi.
3	Hatinah et al., 2023 – Deteksi Malware Ransomware dengan Ekstraksi Fitur N-gram	Analisis API call ransomware menggunakan teknik N-gram dan TF-IDF.	Efektif dalam mendeteksi pola ransomware spesifik berdasarkan API calls.	Tidak optimal untuk malware yang sering bervariasi dalam pola panggilan API.
IoT				
1	Ismayanti, C.A., dan Rantelinggi, P.H., 2024 – Blockchain untuk Keamanan Jaringan IoT	Implementasi blockchain publik sebagai sistem keamanan untuk IoT.	Blockchain menambah lapisan keamanan untuk transfer data IoT, khususnya dalam jaringan publik.	Masalah efisiensi performa karena ketergantungan pada daya komputasi tinggi.
2	Umar et al., 2024 – Analisis Keamanan LMS menggunakan Penetration Testing ISSAF	Pengujian penetrasi pada Learning Management System (LMS) menggunakan ISSAF.	Metode ini mampu mengidentifikasi kelemahan spesifik dalam LMS.	Membutuhkan tim keamanan yang berpengalaman untuk pelaksanaan.
PENILAIAN RISIKO DAN KEAMANAN INFORMASI				
1	Emmanuel, P.N., dan Maulany, R., 2023 – Penilaian Risiko Sistem Informasi dengan Metode OCTAVE Allegro	OCTAVE Allegro, yang digunakan untuk menilai risiko keamanan informasi pada sebuah sistem penerbitan.	Memberikan pendekatan sistematis dan menyeluruh dalam mengidentifikasi serta menilai risiko; mudah disesuaikan dengan berbagai jenis organisasi.	Memerlukan waktu dan sumber daya yang signifikan untuk pelaksanaan.
2	Darmi, Y. et al., 2024 – Evaluasi Tata Kelola Keamanan Sistem Informasi	Evaluasi tata kelola untuk meminimalkan risiko teknologi informasi.	Memberikan pendekatan holistik untuk menilai kepatuhan keamanan informasi.	Memerlukan standar yang tepat sebagai acuan untuk mencapai hasil optimal.
3	Wasilah et al., 2024 – Evaluasi Keamanan Informasi dengan Indeks KAMI 4.3	Pengukuran tingkat keamanan informasi menggunakan Indeks KAMI.	Memberikan panduan yang dapat disesuaikan sesuai kebutuhan keamanan organisasi.	Indeks KAMI mungkin memerlukan adaptasi agar sesuai dengan standar internasional.
INTRUSION PREVENTION SYSTEM (IPS) & EARLY WARNING SYSTEM				
1	Rivaldi, O. dan Marpaung, N.L., 2023 – Intrusion Prevention System Berbasis Suricata	Suricata sebagai Intrusion Prevention System (IPS) untuk mencegah ancaman jaringan.	Dapat mendeteksi dan mencegah intrusi secara *real-time*; *open-source* sehingga lebih fleksibel.	Memerlukan pemeliharaan dan pengaturan yang cukup mendalam.

2	Wijaya, I. K.K.A., dan Siagian, R.C., 2021 – Early Warning System Menggunakan Media Sosial	Sistem peringatan dini berbasis analisis data dari media sosial untuk mendeteksi bencana.	Memanfaatkan data yang tersedia secara publik; dapat memberikan peringatan dalam waktu nyata.	Akurasi tergantung pada ketersediaan data dan mungkin terpengaruh oleh misinformasi.
ENKRIPSI DAN STEGANOGRAFI UNTUK KEAMANAN DATA				
1	Irwan, A.I. et al., 2024 - Sistem Keamanan Berbasis Kode QR dengan RSA dan Hash	Menggunakan algoritma RSA dan hash untuk autentikasi berbasis kode QR.	Memberikan tingkat keamanan yang tinggi; RSA memastikan enkripsi kuat.	Kode QR rentan terhadap serangan fisik dan membutuhkan verifikasi tambahan.
2	Umam, C., dan Muslih, 2023 – Enkripsi dengan AES dan Steganografi DWT	Menggunakan kombinasi enkripsi AES dan streganografi DWT untuk menyembunyikan data.	Menyediakan lapisan keamanan ganda; data tersembunyi di dalam media lain.	Dapat memperlambat proses karena adanya dua lapisan enkripsi.
3	Ridwan et al., 2020 – Steganografi DCT untuk Keamanan Dokumen Digital	Menggunakan steganografi berbasis Discrete Cosine Transform	Efektif dalam menyembunyikan data dalam gambar digital.	Tidak sepenuhnya aman terhadap serangan yang menargetkan manipulasi gambar.
MENDETEKSI DAN MENGURANGI SERANGAN CYBER				
1	Pratiwi, D.Y.D., dan Adrian, R., 2024 – Deteksi dan Mitigasi Serangan DDoS	Sistem mendeteksi dan meredakan serangan DDoS pada jaringan.	Memungkinkan mitigasi serangan sebelum mengganggu layanan.	Deteksi yang efektif membutuhkan pengaturan jaringan yang rumit.
2	Ernawati, T. et al., 2023 – Keamanan Jaringan dengan Random Port Knocking	Penggunaan port knocking acak untuk mengamankan jaringan dari akses yang tidak diizinkan.	Sulit bagi penyerang untuk memprediksi port yang akan digunakan	Membutuhkan pemeliharaan konstan dan terkadang menyulitkan pengguna yang sah.
FRAMEWORK DAN STANDAR UNTUK AUDIT DAN MANAJEMEN RISIKO KEAMANAN INFORMASI				
1	Arifin, N. et al., 2023 – Audit Keamanan dengan Framework COBIT 5	Audit sistem informasi menggunakan framework COBIT 5.	Standar industri yang diterima secara luas; menyediakan kerangka kerja yang lengkap.	Memerlukan pemahaman mendalam tentang framework untuk implementasi yang efektif.
2	Isnaini et al., 2023 – Analisis Risiko dengan ISO 27005:2019	Pendekatan manajemen risiko ISO 27005:2019.	Standar yang diakui secara internasional; fokus pada analisis risiko.	Proses yang panjang; membutuhkan sumber daya dan tenaga ahli.
3	Hikam et al., 2022 – Manajemen Risiko Informasi dengan ISO/IEC 27005:2018	Standar ISO/IEC 27005:2018 dalam manajemen risiko.	Memberikan pendekatan menyeluruh dalam mengelola risiko keamanan informasi.	Proses ini memerlukan waktu dan sumber daya yang cukup besar.

Dari hasil klasifikasi 25 *paper* yang dipilih dapat diketahui bahwa terdapat 9 metode yang digunakan dalam penelitian mengenai sistem keamanan informasi yaitu AI, Blockchain, Ransomware, IoT, Penilaian Resiko dan Keamanan Informasi, Intrusion Prevention System (IPS) & Early Warning System, Enkrispi dan Steganografi untuk Keamanan Data, Mendeteksi dan Mengurangi Serangan Cyber, serta Framework dan Standar untuk Audit dan Manajemen Risiko Keamanan Informasi.

Berdasarkan hasil analisis terkait dengan penggunaan metode berbasis AI dengan non-AI terdapat 3 klasifikasi yaitu efektivitas dalam pendeteksian ancaman, kemampuan dalam penilaian dan manajemen risiko, efisiensi dalam penggunaan sumber daya dan waktu, serta keamanan dan keandalan data. Perbandingan antara metode berbasis AI dan Non-AI dalam keamanan siber diklasifikasikan sebagai berikut.

Tabel 6. Perbandingan Metode AI dan Non-AI

Aspek	Metode AI	Metode Non-AI
Efektivitas dalam Pendeteksian Ancaman	AI mampu mengenali pola serangan dan beradaptasi dengan ancaman baru secara cepat.	Bergantung pada aturan yang telah ditentukan sebelumnya, kurang fleksibel dalam menghadapi ancaman baru.
Kemampuan dalam Penilaian Manajemen Risiko	AI dapat menganalisis data besar dan memberikan rekomendasi otomatis.	Analisis manual membutuhkan waktu lebih lama dan bisa rentan terhadap *human error.*
Efisiensi dalam Penggunaan Sumber Daya dan Waktu	Automatisasi berbasis AI mengurangi kebutuhan tenaga manusia dan mempercepat proses keamanan.	Proses manual membutuhkan lebih banyak waktu dan tenaga manusia.
Keamanan dan Keandalan Data	AI dapat mengenkripsi dan mengelola data secara cerdas serta mendeteksi anomali.	Metode tradisional seperti firewall dan enkripsi konvensional kurang adaptif terhadap ancaman baru.

Efektivitas dalam Pendeteksian Ancaman

Metode menggunakan AI (seperti algoritma machine learning, jaringan saraf tiruan, atau deteksi pola berbasis AI) unggul dalam memproses data yang berjumlah besar dengan cepat dan dapat mendeteksi ancaman yang akan berkembang. Hal tersebut sesuai dengan penelitian yang dilakukan oleh (Rivaldi & Marpaung, 2023) dalam penerapan Intrusion Prevention System (IPS) berbasis Suricata. Dalam penelitian tersebut, Suricata mampu mendeteksi pola yang mencurigakan di jaringan dan memberi respon yang sesuai guna mencegah serangan.

Selain itu, AI juga dapat mendeteksi ancaman yang belum pernah ditemukan sebelumnya dengan analisa yang adaptif dan cepat secara otomatis. Sedangkan, dalam penelitian metode non-AI seperti dalam penelitian milik (Emmanuel & Maulany, 2023) dalam judul Penilaian Risiko menggunakan OCTAVE Allegro dan penelitian Evaluasi Keamanan Berbasis Standar seperti ISO 27005 (Isnaini et al., 2023) masih membutuhkan proses analisis manual, penerapan kebijakan, dan juga protokol yang telah disepakati dalam kata lain metode non-AI dinilai kurang fleksibel dalam menghadapi ancaman baru yang terus berkembang karena bergantung pada aturan dan pola ancaman yang sudah diketahui sebelumnya.

Penilaian dan Manajemen Risiko

Dalam penilaian dan manajemen risiko, metode AI memungkinkan untuk dapat mengidentifikasi pola ancaman seperti dalam penelitian penggunaan teknik ekstraksi figur n-gram dan TF-IDF untuk mendeteksi malware ransomware (Hartinah et al., 2023) Dengan menemukan pola tersebunyi dalam data, Metode AI dapat memprediksi pola yang tersembunyi dalam data dengan lebih tepat dan presisi. Sedangkan untuk metode non-AI seperti penelitian (Arifin et al., 2023) disusun untuk memberikan panduan secara tersruktur dalam penilaian dan pengelolaan resiko melalui metoe yang telah teruji.

Keamanan dan Keyakinan Data

Keamanan data menggunakan metode AI dapat diperkuat melalui penggunaan algoritma prediksi yang melacak serta mendeteksi pola ancaman seperti pada penelitian (Hartinah et al., 2023) yaitu metode berbasis fitur pada deteksi malware. Al dapat melakukan proteksi dini terhadap potensi adanya serangan dengan memberikan keamanan yang proaktif sebelum terjadi. Sedangkan, dalam metode non-AI seperti dalam penelitian penilaian keamanan menggunakan ISO/IEC 27005 (Hikam et al., 2024) menggunakan metode berbasis protokol dan standar konvensional, fokus terhadap pengendalian dan sistem yang jelas dalam menjaga keamanan data. Sehingga dapat memberikan kerangka kerja yang jelas dan terstandar dalam menjaga keamanan data. Tetapi, metode ini lebih lamban dalam menanggapi ancaman baru terutama yang tidak mencakup standar atau aturan yang sudah ada sebelumnya sehingga rentan terhadap serangan yang lebih canggih.

KESIMPULAN

Metode AI lebih efisien dan fleksibel daripada metode lain, terutama dalam menghadapi ancaman siber yang dinamis dan canggih. Dengan menggunakan AI, suatu organisasi dapat mendeteksi dan mencegah ancaman dalam waktu nyata. Namun, AI membutuhkan banyak sumber daya dan keahlian teknis, jadi metode AI membutuhkan banyak sumber daya dan keahlian teknis, sehingga metode AI tidak cocok untuk organisasi yang memproses data dalam volume yang besar.

Di sisi lain, metode non-AI lebih sederhana dan hemat biaya dalam penerapan awal dan lebih cocok untuk organisasi yang kecil atau menengah untuk memproses data. Standar yang ada dapat memastikan kepatuhan terhadap peraturan keamanan informasi, tetapi metode ini kurang peka terhadap ancaman baru dan berkembang.

DAFTAR PUSTAKA

[1] A. Liberati *et al.*, “The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: explanation and elaboration.,” *BMJ*, vol. 339, 2009, doi: 10.1136/bmj.b2700.

[2] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, “The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review,” *Ijarcce*, vol. 11, no. 9, pp. 81–90, 2022, doi: 10.17148/ijarcce.2022.11912.

[3] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, “Explainable Artificial Intelligence in CyberSecurity: A Survey,” *IEEE Access*, vol. 10, no. August, pp. 93575–93600, 2022, doi:

10.1109/ACCESS.2022.3204171.

[4] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, no. March, 2023, doi: 10.1016/j.inffus.2023.101804.

[5] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput. Secur.*, vol. 111, p. 102490, 2021, doi: 10.1016/j.cose.2021.102490.

[6] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2157–2177, 2021, doi: 10.1007/s40747-021-00409-7.

[7] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2157–2177, 2021, doi: 10.1007/s40747-021-00409-7.

[8] M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," *Discov. Internet Things*, vol. 1, no. 1, 2021, doi: 10.1007/s43926-020-00001-4.

[9] M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," *Discov. Internet Things*, vol. 1, no. 1, 2021, doi: 10.1007/s43926-020-00001-4.

[10] C. A. Ismayanti and P. H. Rantelinggi, "Simulasi Penggunaan Blockchain Pada Keamanan Jaringan Internet Of Things Menggunakan Pin Emulator: Model Public Blockchain," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 2, pp. 235–242, 2024, doi: 10.25126/jtiik.20241126108.

[11] R. Umar, I. Riadi, and S. A. Wicaksono, "Security Analysis of Learning Management System Using Penetration Testing with ISSAF Framework," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 12, no. 1, pp. 59–68, 2024, doi: 10.33558/piksel.v12i1.8331.

[12] Sulistiadi and M. Salman, "Ransomware Attacks Threat Modeling Using Bayesian Network," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 14, no. 1, pp. 43–56, 2023, doi: 10.31849/digitalzone.v14i1.13788.

[13] F. A. Rafrastara, C. Supriyanto, C. Paramita, Y. P. Astuti, and F. Ahmed, "Performance Improvement of Random Forest Algorithm for Malware Detection on Imbalanced Dataset using Random Under-Sampling Method," *J. Inform. J. Pengemb. IT*, vol. 8, no. 2, pp. 113–118, 2023, doi: 10.30591/jpit.v8i2.5207.

[14] P. N. Emmanuel and R. Maulany, "Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House," *Krea-Tif J. Tek. Inform.*, vol. 11, no. 1, pp. 37–52, 2023, doi: 10.32832/krea-tif.v11i1.14179.

[15] O. Rivaldi and N. L. Marpaung, "Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata," *INOVTEK Polbeng - Seri Inform.*, vol. 8, no. 1, p. 141, 2023, doi: 10.35314/isi.v8i1.3269.

[16] I. Tri Julianto, D. Kurniadi, R. Rohmanto, and F. Alisha Fauzia, "Improving Algorithm Performance using Feature Extraction for Ethereum Forecasting," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 8, no. 1, pp. 80–87, 2024, doi: 10.29207/resti.v8i1.4872.

[17] A. E. Pratiwi and H. N. L. Ermaya, "Implementation of Blockchain Technology on Accounting Information System For Transaction Security and Data Reliability," *JASa (Jurnal Akuntansi, Audit dan Sist. Inf. Akuntansi)*, vol. 8, no. 1, pp. 64–74, 2024, doi: 10.36555/jasa.v8i1.2419.

[18] Arif Indra Irawan, Iman Hedi Santoso, Istikmal, and Maya Rahayu, "Implementation of QR Code Attendance Security System Using RSA and Hash Algorithms," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 13, no. 1, pp. 53–59, 2024, doi: 10.22146/jnteti.v13i1.4395.

[19] Y. Darmi, S. Fernandez, M. Y. Fathoni, and S. Wijayanto, "Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 8, no. 1, pp. 40–51, 2024, doi: 10.29407/intensif.v8i1.21221.

[20] C. Umam and M. Muslih, "Enkripsi Data Teks Dengan AES dan Steganografi DWT," *InComTech J. Telekomun. dan Komput.*, vol. 13, no. 1, p. 28, 2023, doi: 10.22441/incomtech.v13i1.15059.

[21] R. Fachrurozy, M. Y. B. Setiadji, and D. F. Priambodo, "Embedded Wids Kismet Sebagai Perangkat Deteksi Serangan Data Link Layer Wi-Fi Access Point," *J. Inform. J. Pengemb. IT*, vol. 8, no. 1, pp. 22–33, 2023, doi: 10.30591/jpit.v8i1.4551.

[22] H. Hartinah, A. W. Paundu, and A. A. Ilham, "Deteksi Malware Ransomware Berdasarkan Panggilan API dengan Metode Ekstraksi Fitur N-gram dan TF-IDF," *J. Edukasi dan Penelit. Inform.*, vol. 9, no. 1, p. 50, 2023, doi: 10.26418/jp.v9i1.58721.

[23] D. Y. D. Pratiwi and R. Adrian, "Deteksi Dan Mitigasi Serangan Distributed Denial of Service Pada Software Defined Network," *J. Tek. Inform. dan Sist. Inf.*, vol. 10, no. 1, pp. 63–75, 2024, doi: 10.28932/jutisi.v10i1.6995.

[24] T. Ernawati, Idham Kholid, Dahlan, and D. Rohmayani, "Case Study in Network Security System Using Random Port Knocking Method on The Principles of Availability, Confidentiality and Integrity," *J. Online Inform.*, vol. 9, no. 1, pp. 41–51, 2024, doi: 10.15575/join.v9i1.1254.

[25] N. Arifin, E. Saputra, T. K. Ahsyar, and F. Mutakkin, "Audit Keamanan Sistem Informasi Euclid Menggunakan Framework Cobit 5 pada PT. XYZ," *INOVTEK Polbeng - Seri Inform.*, vol. 8, no. 1, p. 103, 2023, doi: 10.35314/isi.v8i1.3229.

[26] M. K. Ridwan, W. F. Pattipeilohy, and S. Sanwani, "Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 5, no. 2, pp. 177–182, 2020, doi: 10.33480/jitk.v5i2.1033.

[27] K. Isnaini, G. J. Nofita Sari, and A. P. Kuncoro, "Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa," *J. Eksplora Inform.*, vol. 13, no. 1, pp. 37–45, 2023, doi: 10.30864/eksplora.v13i1.696.

[28] M. L. B. Hikam, F. Dewi, and D. Praditya, "Analisis Manajemen Risiko Informasi

Menggunakan Iso/Iec 27005:2018 (Studi Kasus: Pt.Xyz)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 728–734, 2024, doi: 10.29100/jipi.v9i2.4709.

[29] N. Ocha Safira, E. Wahyudi, and F. Khair, "Analisis Manajemen Bandwidth dan Keamanan Jaringan Menggunakan Metode Hierarchical Token Bucket dan Port Knocking Pada Router Mikrotik," *InComTech J. Telekomun. dan Komput.*, vol. 13, no. 2, p. 113, 2023, doi: 10.22441/incomtech.v13i2.17214.

[30] U. H. Panggabean and B. Soewito, "Analisis Keamanan Infrastruktur Jaringan Berdasarkan Cyber Kill Chain Framework," *JUSIFO (Jurnal Sist. Informasi)*, vol. 9, no. 1, pp. 33–44, 2023, doi: 10.19109/jusifo.v9i1.17365.