Cognitech Informatics Journal of Reflections
COGNITECH
Vol. 1, No. 1, January 2026 pp. 25-36
Journal Page is available at https://ejournal.lppmunsaka.ac.id/index.php/cognitech

Keamanan Siber dalam Dunia IoT: Tinjauan Sistematis Literatur

Sigit Nurcahyono[1], Haerullah[2]
[1]Universitas Salakanagara
[2]Universitas Mulia
Email: sigit.nurcahyono@unsaka.ac.id, haerullah@universitasmulia.ac.id

ABSTRAK

Perkembangan pesat Internet of Things (IoT) telah membawa transformasi signifikan dalam berbagai sektor, namun sekaligus meningkatkan kompleksitas dan risiko keamanan siber. Keterbatasan sumber daya perangkat, tingginya tingkat interkonektivitas, serta integrasi teknologi canggih seperti kecerdasan buatan (AI), machine learning (ML), blockchain, dan jaringan 5G menjadikan ekosistem IoT rentan terhadap berbagai ancaman siber, termasuk pelanggaran privasi, malware, dan serangan penolakan layanan. Penelitian ini bertujuan untuk menganalisis secara komprehensif lanskap keamanan siber dalam dunia IoT melalui tinjauan sistematis literatur. Metode yang digunakan mengacu pada pedoman Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) dengan menelusuri basis data Scopus, Web of Science, ScienceDirect, dan PubMed. Dari 470 artikel yang teridentifikasi, hanya 10 studi yang memenuhi kriteria inklusi dan dianalisis secara mendalam. Hasil kajian menunjukkan bahwa tantangan utama keamanan IoT meliputi keragaman perangkat, lemahnya mekanisme autentikasi, kurangnya pembaruan keamanan, serta rendahnya kesadaran pengguna. Berbagai solusi yang diusulkan dalam literatur mencakup pendekatan keamanan holistik, penerapan prinsip *security-by-design*, pemanfaatan AI dan ML untuk deteksi ancaman, serta penguatan kebijakan dan kolaborasi lintas pemangku kepentingan. Meskipun demikian, efektivitas solusi yang ada masih menghadapi keterbatasan teknis dan ekonomi. Penelitian ini menegaskan pentingnya pendekatan multidimensional dan berkelanjutan untuk membangun ekosistem IoT yang aman, resilien, dan terpercaya di era digital.
Kata kunci: keamanan siber, Internet of Things, IoT, tinjauan sistematis, PRISMA, keamanan data.

ABSTRACT

The rapid development of the Internet of Things (IoT) has brought significant transformation to various sectors, but at the same time has increased complexity and cybersecurity risks. Limited device resources, high levels of interconnectivity, and the integration of advanced technologies such as artificial intelligence (AI), machine learning (ML), blockchain, and 5G networks make the IoT ecosystem vulnerable to various cyber threats, including privacy breaches, malware, and denial-of-service attacks. This study aims to comprehensively analyze the cybersecurity landscape in the IoT world through a systematic review of the literature. The method used refers to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines by searching the Scopus, Web of Science, ScienceDirect, and PubMed databases. Of the 470 articles identified, only 10 studies met the inclusion criteria and were analyzed in depth. The results of the study show that the main challenges of IoT security include device diversity, weak authentication mechanisms, lack of security updates, and low user awareness. Various solutions proposed in the literature include a holistic security approach, the application of the *security-by-design* principle, the use of AI and ML for threat detection, and the strengthening of policies and cross-stakeholder collaboration. However, the effectiveness of existing solutions still faces technical and economic limitations. This study emphasizes the importance of a multidimensional and sustainable approach to building a secure, resilient, and trustworthy IoT ecosystem in the digital age.
Keywords: cybersecurity, Internet of Things, IoT, systematic review, PRISMA, data security

PENDAHULUAN

Dalam era digital yang terus berkembang, Internet of Things telah menjadi kekuatan transformatif, menghubungkan berbagai perangkat fisik ke internet dan memungkinkan pertukaran data yang luas (Bakti et al., 2023). Integrasi ini telah membuka peluang baru untuk otomatisasi, efisiensi, dan inovasi di berbagai sektor, mulai dari rumah tangga hingga industri

Vol. 1, No. 1, January 2026, pp. 25-36
https://doi.org/10.56861/cognitech.v1i1.10

(Pati, 2024). Namun, ekspansi pesat IoT juga menghadirkan tantangan keamanan siber yang signifikan, mengingat perangkat IoT seringkali memiliki keterbatasan sumber daya dan kerentanan yang dapat dieksploitasi oleh pelaku kejahatan siber (Pati, 2024). Keamanan siber menjadi krusial dalam ekosistem IoT untuk melindungi data sensitif, menjaga integritas sistem, dan mencegah potensi serangan yang dapat mengganggu operasional dan membahayakan keselamatan pengguna (Pati, 2024). Perkembangan IoT mengoptimalkan kehidupan manusia dengan bantuan sensor dan kecerdasan buatan yang menggunakan jaringan internet untuk menjalankan perintah serta menghubungkan manusia dengan perangkat (Megawati, 2021).

Keamanan siber dalam konteks IoT melibatkan serangkaian strategi, teknologi, dan praktik untuk melindungi perangkat IoT, jaringan, dan data dari ancaman siber (Islami, 2018). Pendekatan ini mencakup identifikasi dan mitigasi kerentanan, implementasi kontrol akses yang kuat, enkripsi data, pemantauan keamanan, dan respons terhadap insiden keamanan. Kompleksitas ekosistem IoT, yang melibatkan berbagai jenis perangkat, protokol komunikasi, dan platform, memerlukan pendekatan keamanan yang komprehensif dan adaptif. Arsitektur IoT yang mendasar terdiri dari tiga elemen utama: perangkat fisik yang dilengkapi dengan modul IoT, media penghubung ke internet seperti modem dan router nirkabel, serta pusat data cloud yang berfungsi sebagai tempat penyimpanan aplikasi dan database (Sandi & Fatma, 2023).

Keamanan pada perangkat IoT ini menjadi prioritas utama karena perannya dalam mengirimkan data melalui jaringan tanpa intervensi manusia atau komputer (Turyadi, 2021). Tinjauan sistematis literatur ini bertujuan untuk menganalisis lanskap keamanan siber dalam dunia IoT, mengidentifikasi tren penelitian terkini, tantangan yang dihadapi, dan solusi yang diusulkan. Dengan memahami ancaman dan kerentanan yang ada, serta strategi mitigasi yang efektif, kita dapat membangun ekosistem IoT yang lebih aman dan terpercaya. Keamanan data pribadi menjadi hal yang sangat penting di era digital ini, oleh karena itu integrasi antara teknologi dan kesadaran pengguna akan sangat berperan penting dalam menjaga keamanan data (Yamin et al., 2024). Indonesia sendiri masih memiliki tantangan yang besar terkait dengan keamanan siber. Berdasarkan data dari National Cyber Security Index pada tahun 2022, Indonesia menempati peringkat ke-3 terendah di antara negara-negara G20 dengan skor indeks keamanan siber sebesar 38,96 dari 100 (Yamin et al., 2024).

Serangan siber telah menjadi tantangan tersendiri bagi para pemangku kebijakan di Indonesia di era informasi ini (Islami, 2018). Pada tahun 2018, tercatat adanya 232.447.974 serangan siber yang menargetkan jaringan di Indonesia (Ishak, 2023). Serangan siber dapat menimbulkan gangguan yang signifikan pada perusahaan dan bahkan rumah sakit, seperti yang terjadi pada serangan Ransomware WannaCry pada Mei 2017 yang berdampak pada lebih dari 150 negara, termasuk Indonesia (Islami, 2018).

Ancaman dan Serangan pada Perangkat IoT Perangkat IoT seringkali menjadi target serangan siber karena kerentanan yang melekat pada desain dan implementasinya. Keterbatasan sumber daya komputasi dan memori pada perangkat IoT seringkali menghambat implementasi fitur keamanan yang kuat, seperti enkripsi dan otentikasi. Selain itu, siklus hidup perangkat IoT yang panjang dan kurangnya pembaruan keamanan secara teratur dapat menyebabkan kerentanan yang tidak teratasi, yang dapat dieksploitasi oleh penyerang (Pati, 2024). Serangan terhadap perangkat IoT dapat bervariasi, mulai dari pencurian data dan pengambilalihan perangkat hingga serangan penolakan layanan yang dapat mengganggu operasional jaringan. Kompleksitas arsitektur IoT dapat menciptakan berbagai kerentanan keamanan, termasuk yang terkait dengan komunikasi nirkabel, penyimpanan data, dan antarmuka pengguna (Herdiana et al., 2021).

Beberapa jenis serangan umum pada perangkat IoT meliputi serangan injeksi kode, serangan man-in-the-middle, dan serangan brute-force. Serangan injeksi kode memanfaatkan kerentanan dalam perangkat lunak untuk menyisipkan kode berbahaya yang dapat mengeksekusi perintah yang tidak sah. Serangan man-in-the-middle memungkinkan penyerang untuk mencegat dan memanipulasi komunikasi antara perangkat IoT dan server, mencuri data sensitif atau mengubah perilaku perangkat. Serangan brute-force mencoba menebak kata sandi atau kunci

enkripsi dengan mencoba semua kombinasi yang mungkin. Ancaman siber telah menjadi semakin nyata di Indonesia, dengan peningkatan signifikan dalam kasus kejahatan siber yang memengaruhi jutaan pengguna dan menyebabkan kerugian finansial yang besar serta dampak psikologis yang mendalam (Putri et al., 2024).

Pada tahun 2020, Indonesia mengalami sekitar 495 juta serangan siber, dan jumlah ini meningkat menjadi 741 juta pada periode Januari hingga Juli 2021 (Prabaswari et al., 2022). Serangan siber ini dapat berupa berbagai jenis ancaman, termasuk malware, ransomware, phishing, dan serangan DDoS. Motivasi di balik serangan siber ini bervariasi, mulai dari keuntungan finansial hingga spionase dan sabotase. Perangkat IoT yang terhubung ke internet dapat dengan mudah terinfeksi oleh malware dan digunakan sebagai bagian dari botnet untuk meluncurkan serangan DDoS.

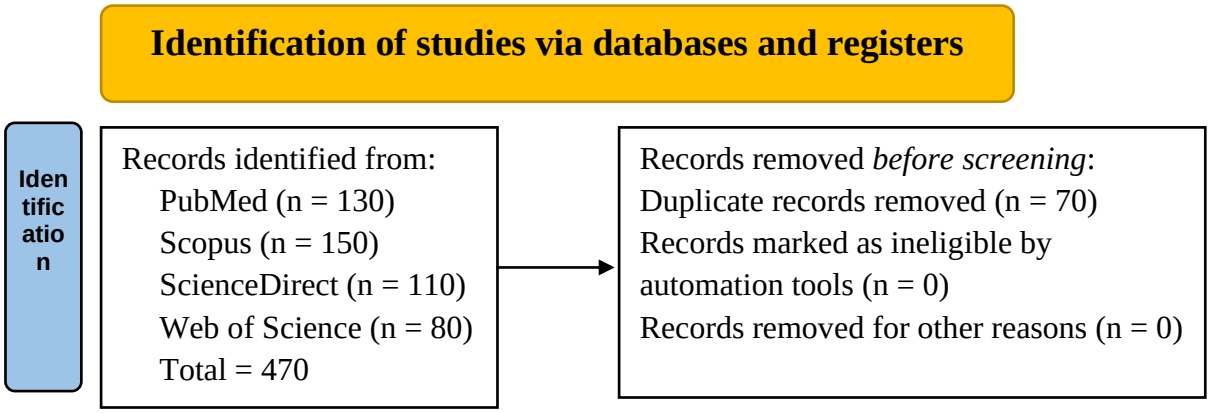
Kurangnya kesadaran keamanan siber di kalangan pengguna dan organisasi juga menjadi faktor yang berkontribusi terhadap meningkatnya insiden keamanan siber. Banyak pengguna tidak menyadari risiko yang terkait dengan penggunaan perangkat IoT yang tidak aman atau tidak mengambil langkah-langkah yang memadai untuk melindungi diri mereka sendiri dari serangan siber. Selain itu, kurangnya koordinasi dan kolaborasi antara pemangku kepentingan keamanan siber, seperti pemerintah, industri, dan akademisi, dapat menghambat upaya pencegahan dan penanggulangan kejahatan siber (Ishak, 2023).

METODOLOGI

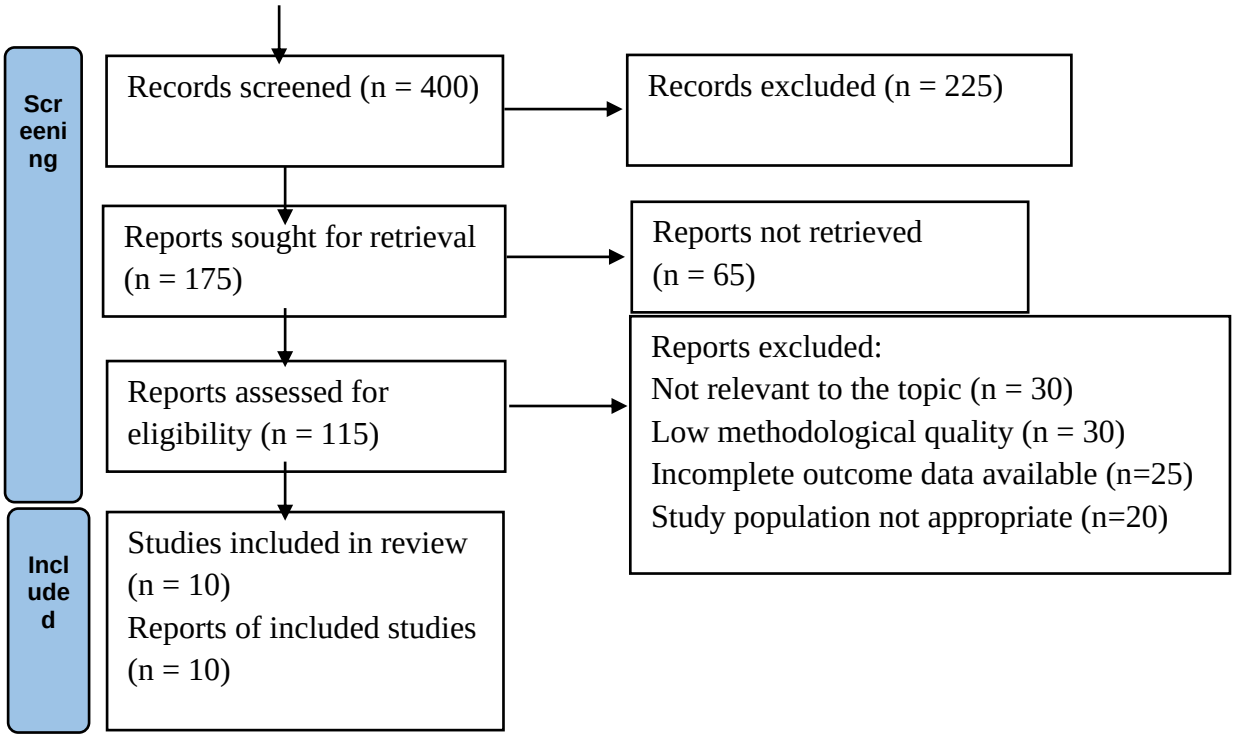
Dalam menganalisis lanskap keamanan siber pada ekosistem IoT, metodologi penelitian yang diterapkan melibatkan pendekatan sistematis untuk mengumpulkan, meninjau, dan mensintesis literatur yang relevan. Langkah pertama adalah identifikasi kata kunci dan istilah pencarian yang relevan dengan topik penelitian, seperti "keamanan IoT", "kerentanan IoT", "serangan IoT", "mitigasi keamanan IoT", dan "analisis risiko IoT". Pencarian literatur dilakukan pada basis data akademik dan mesin pencari seperti Scopus, Web of Science, IEEE Xplore, dan Google Scholar. Kriteria inklusi dan eksklusi ditetapkan untuk memastikan bahwa hanya artikel yang relevan dan berkualitas yang dimasukkan dalam tinjauan. Artikel yang dipilih harus fokus pada aspek keamanan siber dalam konteks IoT, diterbitkan dalam jurnal atau konferensi terkemuka, dan menggunakan metode penelitian yang valid. Setelah pengumpulan literatur, dilakukan proses penyaringan untuk menghilangkan artikel yang tidak relevan atau duplikat.

Artikel yang tersisa kemudian dievaluasi berdasarkan kualitas metodologis dan relevansi konten. Data yang diekstraksi dari artikel yang dipilih mencakup informasi tentang jenis serangan IoT, kerentanan yang dieksploitasi, teknik mitigasi yang diusulkan, dan hasil evaluasi kinerja. Data yang diekstraksi kemudian dianalisis secara kualitatif dan kuantitatif untuk mengidentifikasi tren, pola, dan kesenjangan dalam literatur. Selain itu, dilakukan analisis terhadap studi kasus dan laporan insiden keamanan IoT untuk mendapatkan wawasan praktis tentang tantangan dan solusi keamanan yang diterapkan dalam dunia nyata. Hasil analisis kemudian disintesis dan diinterpretasikan untuk memberikan gambaran komprehensif tentang lanskap keamanan siber dalam dunia IoT.

Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Diagram Flow



Vol. 1, No. 1, January 2026, pp. 25-36
https://doi.org/10.56861/cognitech.v1i1.10



Berdasarkan diagram alur PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), proses seleksi literatur dalam tinjauan sistematis ini dilakukan melalui beberapa tahapan yang ketat dan terstruktur. Pada tahap identifikasi, sebanyak 470 dokumen berhasil ditemukan dari empat basis data utama, yaitu PubMed (n = 130), Scopus (n = 150), ScienceDirect (n = 110), dan Web of Science (n = 80). Setelah dilakukan pemeriksaan awal, sebanyak 70 dokumen dihapus karena merupakan duplikasi, sementara tidak ada dokumen yang ditolak oleh alat otomatis maupun alasan lainnya. Dengan demikian, 400 dokumen dilanjutkan ke tahap penyaringan berikutnya.

Pada tahap penyaringan, peneliti meninjau dokumen berdasarkan judul dan abstrak, sehingga 225 dokumen dinyatakan tidak memenuhi kriteria awal dan dieliminasi. Dari hasil penyaringan tersebut, 175 dokumen dianggap potensial dan dicari versi full-text-nya untuk dianalisis lebih lanjut. Namun, sebanyak 65 dokumen tidak berhasil diperoleh, menyisakan 115 dokumen yang berhasil dikumpulkan dan dinilai kelayakannya. Penilaian ini mencakup berbagai aspek penting seperti relevansi terhadap topik, kualitas metodologi, kelengkapan data hasil, dan kesesuaian populasi studi.

Hasil dari tahap penilaian kelayakan menunjukkan bahwa 80 dokumen harus dikeluarkan karena berbagai alasan, antara lain ketidaksesuaian dengan topik penelitian (n = 30), kualitas metodologi yang rendah (n = 30), ketersediaan data hasil yang tidak lengkap (n = 25), serta ketidaksesuaian populasi studi (n = 20). Akhirnya, hanya 10 studi yang dinilai layak dan memenuhi seluruh kriteria inklusi, sehingga dimasukkan ke dalam tinjauan sistematis. Proses ini menunjukkan pendekatan yang komprehensif dan ketat dalam menyaring literatur, guna memastikan bahwa hanya bukti-bukti yang paling relevan dan bermutu tinggi yang dijadikan dasar dalam analisis lebih lanjut.

HASIL PENELITIAN

No	Judul Artikel	Temuan Utama

1	A Dynamic Cybersecurity Framework for Energy-Efficient Internet of Things (Sandhyakumari et al., 2025)	Keamanan siber IoT menghadirkan tantangan karena perangkat yang beragam dengan kerentanannya masing-masing. Penting untuk memastikan privasi data dan integritas rantai pasokan, serta mematuhi regulasi seperti GDPR dan HIPAA.
2	A Comprehensive Study on Cybersecurity Challenges and Opportunities in the IoT Worlds (Lone et al., 2023)	Makalah ini membahas tantangan dan peluang keamanan siber akibat integrasi IoT, dengan fokus pada masalah keamanan terkait AI, machine learning, blockchain, dan 5G, serta pentingnya menjaga segitiga keamanan CIA.
3	Assessing the Cybersecurity Risks Associated with the Internet of Things (IoT) Devices (Akintayo et al., 2024)	Penelitian ini menyoroti masalah keamanan siber pada IoT, seperti kejahatan dunia maya dan pelanggaran privasi, serta pentingnya AI untuk meningkatkan keamanan, meskipun masih banyak serangan yang belum teratasi dengan solusi saat ini.
4	Cybersecurity Risks and Countermeasures in the Threat Landscape of IoT Devices (Patel et al., 2024)	Makalah ini menyimpulkan bahwa interkonektivitas perangkat IoT meningkatkan risiko keamanan siber, memerlukan tindakan pencegahan yang kuat, pelatihan pengguna, undang-undang, dan kemajuan teknologi keamanan untuk menciptakan lingkungan digital yang aman.
5	Cybersecurity in the Internet of Things (IoT) Era: Safeguarding Connected Systems and Data (Butsianto et al., 2024)	Artikel ini menekankan pentingnya pendekatan keamanan siber holistik yang menggabungkan teknologi, kebijakan, dan kesadaran pengguna untuk melindungi ekosistem IoT, dengan penekanan pada kolaborasi antara pemangku kepentingan untuk meningkatkan ketahanan sistem.
6	A Comprehensive Analysis of Cybersecurity Threats based IoTs (Shukur & Shukur, 2023)	Studi ini menyoroti kerentanannya sistem IoT terhadap ancaman dunia maya, terutama terkait privasi dan kejahatan. Ditekankan pentingnya penelitian berkelanjutan, integrasi AI, dan kolaborasi multidisiplin untuk meningkatkan keamanan IoT.
7	Cybersecurity in the Age of IoT: Business Strategies for Managing Emerging Threats (Nishat Margia et al., 2024)	Studi ini mengidentifikasi kerentanan besar dalam IoT dan menekankan perlunya solusi keamanan komprehensif. Integrasi AI dan ML untuk pemantauan serta kerangka kerja keamanan kolaboratif dapat meningkatkan postur keamanan IoT.
8	Improving Cybersecurity in Business Settings: The Challenges and Solutions of Internet of Things (Rao et al., 2024)	Makalah ini menyimpulkan bahwa meningkatnya perangkat IoT memperluas permukaan serangan, memerlukan langkah-langkah keamanan siber yang lebih canggih, seperti otentikasi multi-elemen, pembaruan firmware, penilaian risiko, dan pelatihan kesadaran untuk melindungi informasi sensitif.
9	Cyber Security in the Age of the Internet of Things, Constraints, and Solutions (Dickson & Okechukwu, 2023)	Penelitian ini menekankan pentingnya filosofi "security-by-design" dalam pengembangan perangkat IoT untuk mengurangi risiko. Studi ini memberikan rekomendasi dan wawasan untuk mengatasi tantangan keamanan siber dalam ekosistem IoT yang luas.
10	Cybersecurity Risk Analysis in the IoT: A Systematic Review (AlSalem et al., 2023)	Studi ini menyoroti masalah privasi dan kejahatan dunia maya dalam keamanan IoT, dengan AI sebagai solusi potensial. Namun, solusi yang ada masih kurang efektif, memerlukan penelitian lebih lanjut dan penilaian dampak

Vol. 1, No. 1, January 2026, pp. 25-36
https://doi.org/10.56861/cognitech.v1i1.10

		ekonomi.

Dalam konteks pesatnya adopsi Internet of Things (IoT) di berbagai sektor, isu keamanan dan kerentanannya menjadi perhatian utama yang mendorong lahirnya berbagai penelitian. Kompleksitas sistem IoT yang terdiri dari perangkat dengan karakteristik dan fungsi berbeda-beda menciptakan tantangan besar dalam menjaga integritas, privasi, dan keamanan data yang dipertukarkan. Tak hanya ancaman teknis, tekanan terhadap kepatuhan regulatif seperti GDPR dan HIPAA turut memperumit lanskap ini, terutama ketika teknologi mutakhir seperti AI, blockchain, dan 5G mulai diintegrasikan ke dalam infrastruktur IoT. Untuk memahami dan menghadapi tantangan tersebut secara menyeluruh, para peneliti mengembangkan berbagai pendekatan, mulai dari strategi holistik hingga penerapan kecerdasan buatan, serta mengusulkan kerangka keamanan yang terintegrasi dengan kebijakan bisnis dan peran aktif semua pemangku kepentingan. Lima kategori tematik berikut merangkum dinamika dan strategi yang diusulkan dalam literatur terkait keamanan IoT, yang secara kolektif memberikan kontribusi penting dalam upaya mitigasi ancaman siber di era digital.

1. Tantangan dan Kerentanan Keamanan pada IoT
   Penelitian pertama yang masuk dalam kategori ini adalah karya Sandhyakumari et al. (2025), yang menyoroti tantangan besar dalam mengamankan perangkat IoT yang sangat beragam, dengan masing-masing perangkat memiliki kerentanannya sendiri. Hal ini diperparah oleh tuntutan untuk mematuhi regulasi seperti GDPR dan HIPAA yang menambah lapisan kompleksitas dalam menjaga privasi dan integritas data. Sementara itu, Lone et al. (2023) lebih mendalami tantangan yang muncul dari integrasi teknologi canggih seperti AI, blockchain, dan 5G dalam IoT, yang memunculkan potensi ancaman baru. Akintayo et al. (2024) juga menyoroti masalah privasi dan kejahatan dunia maya yang sering terjadi di perangkat IoT, meskipun penelitian ini juga menunjukkan bahwa AI berperan penting dalam mengatasi beberapa masalah ini. Karya-karya ini saling menguatkan bahwa sistem IoT memiliki kerentanannya sendiri, yang perlu dipahami secara holistik untuk memitigasi potensi ancaman.
2. Pendekatan Holistik dalam Keamanan IoT
   Beberapa penelitian menekankan pentingnya pendekatan holistik dalam melindungi sistem IoT. Butsianto et al. (2024) menyoroti perlunya pendekatan yang menggabungkan teknologi, kebijakan, dan kesadaran pengguna dalam menjaga keamanan sistem IoT. Hal serupa juga diungkapkan oleh Patel et al. (2024), yang menyatakan bahwa penguatan tindakan pencegahan, pelatihan pengguna, dan kemajuan teknologi keamanan sangat dibutuhkan untuk menciptakan ekosistem digital yang aman. Dalam konteks ini, Nishat Margia et al. (2024) menekankan integrasi AI dan machine learning untuk memantau dan merespons ancaman secara lebih cepat dan efektif, menciptakan kerangka kerja yang kolaboratif dalam menjaga keamanan. Temuan ini menyarankan bahwa kolaborasi antara pemangku kepentingan, seperti pengembang, regulator, dan pengguna, adalah kunci dalam menciptakan sistem IoT yang aman dan tahan terhadap ancaman siber.
3. Peran AI dan Machine Learning dalam Mitigasi Risiko Keamanan IoT
   Beberapa penelitian juga mengidentifikasi potensi besar AI dan machine learning (ML) dalam meningkatkan keamanan IoT. Misalnya, Shukur & Shukur (2023) dan AlSalem et al. (2023) menyoroti peran AI dalam mendeteksi dan merespons ancaman siber di lingkungan IoT. Teknologi ini dapat digunakan untuk meningkatkan deteksi ancaman dan mengurangi risiko kejahatan dunia maya serta pelanggaran privasi. Namun, meskipun potensi AI besar, penelitian ini mengungkapkan bahwa solusi yang ada saat ini masih belum efektif sepenuhnya dan membutuhkan penelitian lebih lanjut untuk mengevaluasi dampaknya secara ekonomi. Hasil-hasil ini menunjukkan bahwa meskipun AI menawarkan peluang besar untuk

meningkatkan keamanan, tantangan besar tetap ada dalam hal implementasi dan pengembangannya.

4. Kerangka Keamanan dan Strategi Bisnis dalam IoT
   Sebagian penelitian berfokus pada bagaimana kerangka kerja keamanan dapat diterapkan dalam konteks bisnis. Misalnya, Rao et al. (2024) menjelaskan bahwa otentikasi multi-elemen, pembaruan firmware, dan pelatihan kesadaran sangat penting dalam memperkuat sistem IoT di lingkungan bisnis. Dickson & Okechukwu (2023) juga memberikan wawasan tentang pentingnya filosofi "security-by-design" dalam pengembangan perangkat IoT, yang dapat mengurangi risiko keamanan sejak tahap perancangan. Pendekatan ini semakin relevan dalam bisnis yang bergantung pada teknologi IoT untuk operasional mereka, di mana perencanaan yang cermat dan implementasi kebijakan yang tepat sangat diperlukan untuk melindungi data dan sistem yang terhubung.
5. Solusi dan Upaya Mitigasi Ancaman Keamanan IoT
   Penelitian yang berfokus pada solusi dan upaya mitigasi ancaman juga sangat relevan untuk meningkatkan keamanan IoT. Dalam penelitian oleh Patel et al. (2024) dan Butsianto et al. (2024), pentingnya tindakan pencegahan yang kuat, kebijakan yang tepat, serta peran kesadaran pengguna dalam mencegah serangan dunia maya sangat ditekankan. Selain itu, pentingnya kolaborasi antar berbagai pihak, termasuk pemerintah, organisasi, dan individu, juga disebutkan sebagai elemen yang diperlukan untuk memperkuat ketahanan sistem IoT terhadap ancaman. Penelitian ini memberikan gambaran yang jelas bahwa solusi keamanan yang efektif harus menyeluruh dan melibatkan berbagai aspek, dari teknologi hingga kesadaran sosial.

PEMBAHASAN PENELITIAN

Penelitian yang dilakukan oleh Sandhyakumari et al. (2025) menggarisbawahi kompleksitas tantangan keamanan siber dalam konteks Internet of Things (IoT), terutama ketika dihadapkan pada kebutuhan efisiensi energi dan kepatuhan terhadap regulasi seperti GDPR dan HIPAA. Dengan ekosistem perangkat IoT yang beragam dan sering kali memiliki tingkat keamanan yang tidak seragam, penelitian ini menekankan pentingnya kerangka kerja dinamis yang mampu menjaga privasi data serta menjamin integritas rantai pasokan. Solusi yang diusulkan mencakup pemanfaatan teknologi enkripsi yang hemat energi dan protokol komunikasi yang adaptif, sehingga tidak hanya mengurangi kerentanan sistem, tetapi juga memastikan bahwa konsumsi daya tetap dalam batas yang dapat diterima untuk perangkat IoT skala kecil. Penelitian ini menunjukkan bahwa sinergi antara kebijakan keamanan dan efisiensi operasional sangat diperlukan dalam mendesain sistem IoT yang aman dan berkelanjutan.

Makalah yang ditulis oleh Lone et al. (2023) menyoroti tantangan keamanan siber yang muncul akibat integrasi IoT dengan teknologi canggih seperti kecerdasan buatan (AI), machine learning (ML), blockchain, dan jaringan 5G. Dengan pendekatan komprehensif, penelitian ini mengidentifikasi bahwa perlu ada perhatian serius terhadap segitiga keamanan CIA Confidentiality, Integrity, dan Availability yang sangat rentan akibat konektivitas tinggi antarperangkat. Lone et al. menekankan bahwa penguatan aspek-aspek tersebut harus diiringi dengan pengembangan kerangka regulasi yang sesuai serta peningkatan kesadaran pengguna dalam menerapkan praktik keamanan dasar. Artikel ini juga menyatakan bahwa meskipun teknologi pendukung seperti AI menawarkan solusi untuk mendeteksi dan merespons ancaman secara real-time, kompleksitas yang timbul dari interaksi antar teknologi justru memperbesar permukaan serangan jika tidak dikelola secara holistik.

Penelitian yang dilakukan oleh Akintayo et al. (2024) memberikan fokus pada risiko keamanan siber yang ditimbulkan oleh perangkat IoT, terutama dalam hal pelanggaran privasi dan meningkatnya kejahatan dunia maya. Penulis mencatat bahwa meskipun AI memiliki potensi untuk memperkuat sistem pertahanan IoT, masih banyak celah yang belum dapat ditangani secara efektif oleh solusi yang ada saat ini. Studi ini secara kritis menilai kemampuan sistem

Vol. 1, No. 1, January 2026, pp. 25-36
https://doi.org/10.56861/cognitech.v1i1.10

deteksi anomali berbasis AI dan menemukan bahwa akurasi serta keandalan deteksi masih dipengaruhi oleh kurangnya data pelatihan yang representatif dan perubahan pola serangan yang dinamis. Dengan demikian, Akintayo et al. menyarankan pendekatan keamanan berlapis dan perlunya kolaborasi antara penyedia teknologi dan regulator dalam menetapkan standar minimum keamanan untuk perangkat IoT, agar bisa menciptakan ekosistem digital yang lebih terlindungi.

Makalah dari Patel et al. (2024) membahas secara mendalam bagaimana interkonektivitas antar perangkat IoT meningkatkan risiko terhadap serangan siber. Penelitian ini menyatakan bahwa selain solusi teknologi, keberhasilan perlindungan terhadap sistem IoT sangat bergantung pada pelatihan pengguna, pembentukan kerangka hukum yang tegas, dan kemajuan teknologi keamanan. Patel et al. menekankan bahwa hanya dengan kombinasi strategi ini yakni kesadaran pengguna yang tinggi, penegakan hukum yang kuat, dan inovasi teknologi berkelanjutan maka ekosistem IoT dapat menjadi lebih aman. Studi ini juga memberikan perhatian khusus pada pentingnya deteksi dini dan respons cepat terhadap serangan, serta perlunya audit keamanan secara berkala sebagai bagian dari praktik manajemen risiko yang proaktif dalam menghadapi lanskap ancaman siber yang terus berkembang.

Artikel yang ditulis oleh Butsianto et al. (2024) menegaskan perlunya pendekatan keamanan siber yang holistik dalam era IoT. Penulis berargumen bahwa perlindungan sistem yang saling terhubung tidak hanya mengandalkan solusi teknologi semata, tetapi juga membutuhkan sinergi antara kebijakan yang tepat dan peningkatan kesadaran pengguna. Dalam konteks ini, kolaborasi antara pemangku kepentingan termasuk pengembang teknologi, pemerintah, penyedia layanan, dan pengguna akhir dianggap sebagai faktor kunci dalam menciptakan sistem yang tangguh terhadap serangan siber. Pendekatan interdisipliner menjadi penting, di mana kebijakan yang disusun berbasis pemahaman teknis dan sosial mampu menjembatani kesenjangan antara teknologi dan regulasi. Artikel ini juga merekomendasikan integrasi sistem audit otomatis dan kebijakan keamanan berbasis risiko sebagai langkah strategis untuk memperkuat ketahanan infrastruktur digital.

Studi yang dilakukan oleh Shukur dan Shukur (2023) memperjelas bahwa ancaman terhadap sistem IoT sangat nyata dan sering kali menyasar aspek privasi pengguna serta sistem yang rentan terhadap eksploitasi. Dalam kajiannya, penulis menyoroti kebutuhan mendesak untuk penelitian berkelanjutan guna mengidentifikasi kerentanan baru serta menyempurnakan model keamanan yang ada. Selain itu, integrasi kecerdasan buatan dianggap krusial untuk meningkatkan ketahanan sistem dalam menghadapi serangan yang semakin canggih. Studi ini juga menekankan pentingnya pendekatan multidisiplin, yang menggabungkan keahlian dari bidang teknik, ilmu komputer, hukum, dan kebijakan publik dalam merancang sistem pertahanan yang responsif dan adaptif. Dengan begitu, keamanan siber dalam sistem IoT tidak hanya menjadi isu teknis, tetapi juga sosial dan kebijakan.

Penelitian yang dilakukan oleh Nishat Margia et al. (2024) menyelidiki strategi bisnis yang dapat digunakan untuk mengelola ancaman siber dalam lanskap IoT yang terus berkembang. Temuan mereka menunjukkan bahwa kerentanan pada perangkat IoT tidak hanya berdampak pada sistem teknis, tetapi juga menimbulkan risiko besar terhadap keberlangsungan bisnis. Oleh karena itu, integrasi AI dan machine learning untuk keperluan pemantauan dinamis sangat disarankan. Selain itu, dibutuhkan kerangka kerja keamanan kolaboratif yang dapat menghubungkan sistem keamanan internal organisasi dengan mitra eksternal guna menciptakan respons kolektif terhadap serangan. Artikel ini menggarisbawahi bahwa keamanan IoT tidak hanya menjadi tanggung jawab individu, tetapi harus dilihat sebagai bagian dari strategi perusahaan secara keseluruhan.

Makalah yang disusun oleh Rao et al. (2024) menjelaskan bagaimana pertumbuhan eksponensial perangkat IoT memperluas permukaan serangan, sehingga memerlukan peningkatan langkah-langkah keamanan secara signifikan. Studi ini mengusulkan implementasi mekanisme otentikasi multi-elemen, pembaruan firmware secara berkala, serta penilaian risiko

berbasis konteks sebagai elemen penting dalam perlindungan data. Rao et al. juga menggarisbawahi pentingnya pelatihan kesadaran bagi karyawan, karena faktor manusia tetap menjadi titik lemah utama dalam sistem keamanan siber. Penelitian ini menunjukkan bahwa pendekatan keamanan yang reaktif sudah tidak lagi memadai; sebaliknya, pendekatan proaktif dan prediktif berbasis teknologi serta edukasi menjadi kunci dalam mengatasi ancaman keamanan di era konektivitas tinggi.

Penelitian yang dilakukan oleh Dickson dan Okechukwu (2023) mengangkat pentingnya prinsip "security-by-design" dalam pengembangan perangkat dan sistem IoT sebagai langkah preventif utama. Studi ini mengungkap bahwa banyak kerentanan terjadi karena keamanan sering kali diperlakukan sebagai tambahan, bukan sebagai komponen inti dalam desain awal sistem. Oleh sebab itu, penulis merekomendasikan agar pengembang dan produsen perangkat mengadopsi filosofi ini secara menyeluruh untuk mengurangi risiko sejak tahap perancangan. Artikel ini juga membahas bagaimana pendekatan desain yang berfokus pada keamanan dapat memperkecil kebutuhan akan tambalan keamanan di masa depan, yang sering kali kompleks dan mahal. Selain itu, artikel ini memberikan sejumlah rekomendasi kebijakan dan wawasan praktis untuk meningkatkan ketahanan infrastruktur IoT secara menyeluruh.

Akhirnya, studi yang dilakukan oleh AlSalem et al. (2023) menyajikan tinjauan sistematis mengenai berbagai ancaman siber terhadap perangkat IoT dan menekankan bahwa privasi serta kejahatan dunia maya merupakan isu utama yang belum sepenuhnya teratasi. Penulis mencatat bahwa meskipun AI telah digunakan sebagai solusi untuk mengidentifikasi dan merespons ancaman, efektivitasnya masih terbatas dan sangat tergantung pada ketersediaan data pelatihan yang memadai. Artikel ini merekomendasikan perlunya penelitian lebih lanjut untuk mengevaluasi dampak ekonomi dari serangan siber terhadap sistem IoT serta pengembangan metode baru yang dapat mengantisipasi pola serangan yang semakin kompleks. Dengan pendekatan berbasis bukti, studi ini menawarkan arah baru untuk penguatan kebijakan keamanan IoT dan inovasi teknologi yang lebih adaptif di masa depan.

Penelitian dalam kategori ini menyoroti kompleksitas keamanan pada sistem IoT yang ditandai oleh keragaman perangkat, integrasi teknologi baru, dan regulasi yang ketat. Sandhyakumari et al. (2025) menjelaskan bahwa setiap perangkat IoT memiliki karakteristik unik dan kerentanan tersendiri, sehingga menciptakan tantangan besar dalam menjaga keamanan secara menyeluruh. Kewajiban untuk mematuhi peraturan privasi seperti GDPR dan HIPAA memperumit proses ini, karena memerlukan perlindungan data yang lebih ketat di seluruh lapisan sistem. Lone et al. (2023) memperluas diskusi ini dengan menunjukkan bagaimana penggabungan teknologi seperti AI, blockchain, dan 5G menciptakan permukaan serangan yang lebih luas dan kompleks. Senada dengan itu, Akintayo et al. (2024) memperkuat urgensi isu dengan menyoroti tingginya tingkat pelanggaran privasi dan kejahatan siber di perangkat IoT, meskipun juga menunjukkan potensi AI sebagai alat mitigasi. Secara keseluruhan, temuan dalam kategori ini menegaskan bahwa kerentanan keamanan IoT merupakan isu multidimensional yang harus dipahami secara menyeluruh, baik dari aspek teknis maupun regulatif.

Kebutuhan akan pendekatan yang komprehensif menjadi benang merah dalam penelitian yang tergolong dalam kategori ini. Butsianto et al. (2024) menyatakan bahwa pengamanan IoT tidak dapat hanya bergantung pada teknologi, melainkan harus melibatkan sinergi antara inovasi teknis, regulasi kebijakan, dan peningkatan kesadaran pengguna. Hal ini didukung oleh Patel et al. (2024), yang menekankan pentingnya pelatihan pengguna dan penguatan kebijakan pencegahan untuk menciptakan ekosistem IoT yang aman. Sementara itu, Nishat Margia et al. (2024) menawarkan perspektif yang lebih teknis dengan menyoroti pemanfaatan AI dan machine learning sebagai alat deteksi ancaman yang adaptif dan responsif secara real-time. Ketiganya menyiratkan bahwa strategi keamanan IoT tidak bisa bersifat parsial, melainkan harus dibangun melalui kerangka kerja kolaboratif yang mencakup semua pemangku kepentingan. Pendekatan holistik ini dinilai lebih mampu menjawab tantangan kompleks dalam dunia siber yang terus berkembang.

Artificial intelligence (AI) dan machine learning (ML) telah diidentifikasi sebagai komponen penting dalam meningkatkan ketahanan sistem IoT terhadap ancaman siber. Shukur & Shukur (2023) dan AlSalem et al. (2023) menyoroti kemampuan AI dalam mendeteksi anomali dan memprediksi serangan siber secara proaktif, yang menjadikannya alat yang strategis dalam sistem pertahanan IoT. Teknologi ini memungkinkan respons yang lebih cepat dan efisien terhadap potensi pelanggaran, sehingga memperkecil dampak dari serangan. Namun, penelitian juga menunjukkan bahwa efektivitas AI belum mencapai tingkat optimal, karena masih terdapat tantangan dalam akurasi deteksi, biaya implementasi, serta evaluasi dampak ekonominya. Hal ini menunjukkan bahwa meskipun AI dan ML menjanjikan sebagai solusi keamanan, pengembangannya masih memerlukan investasi riset lanjutan dan pengujian yang sistematis dalam konteks nyata.

Dalam kategori ini, perhatian difokuskan pada integrasi kerangka keamanan ke dalam strategi bisnis berbasis IoT. Rao et al. (2024) menunjukkan bahwa praktik seperti otentikasi multi-elemen, pembaruan perangkat lunak secara berkala, dan pelatihan kesadaran keamanan merupakan bagian penting dalam menciptakan sistem yang tangguh terhadap ancaman. Di sisi lain, Dickson & Okechukwu (2023) memperkenalkan konsep *security-by-design*, yakni pendekatan pengembangan perangkat IoT dengan prinsip keamanan yang tertanam sejak tahap awal perancangan. Pendekatan ini tidak hanya mencegah kerentanan teknis, tetapi juga membangun budaya organisasi yang sadar terhadap pentingnya keamanan data. Dalam lingkungan bisnis yang makin bergantung pada konektivitas IoT, kerangka kerja ini menjadi fondasi penting dalam menjaga integritas sistem dan mencegah kebocoran data yang merugikan.

Upaya mitigasi terhadap ancaman keamanan menjadi tema utama dalam kategori terakhir ini. Patel et al. (2024) dan Butsianto et al. (2024) menekankan pentingnya solusi keamanan yang menyeluruh, mencakup tindakan pencegahan teknis, kebijakan perlindungan, serta edukasi pengguna. Peran kesadaran pengguna menjadi kunci karena banyak serangan siber berhasil akibat kelalaian atau ketidaktahuan individu. Selain itu, kolaborasi lintas sektor juga dipandang sebagai langkah penting, di mana pemerintah, perusahaan, dan masyarakat sipil harus bersinergi dalam membangun ekosistem keamanan yang kuat dan resilien. Penelitian ini menunjukkan bahwa tidak ada satu solusi tunggal untuk menghadapi ancaman IoT, melainkan dibutuhkan pendekatan sistemik dan koordinatif yang mencakup berbagai aspek: teknis, sosial, dan kelembagaan.

KESIMPULAN

Berdasarkan kajian literatur yang mendalam, dapat disimpulkan bahwa keamanan dalam sistem Internet of Things (IoT) merupakan isu kompleks yang menuntut pendekatan multidimensional. Keragaman perangkat, integrasi teknologi canggih, dan tuntutan kepatuhan regulatif menciptakan tantangan besar dalam menjaga privasi, integritas, dan keamanan data. Penelitian-penelitian yang dianalisis menunjukkan bahwa pemahaman holistik terhadap kerentanan IoT sangat krusial, terutama dalam menghadapi ancaman yang terus berkembang. Pendekatan kolaboratif yang mengintegrasikan teknologi seperti AI dan machine learning, strategi bisnis, kebijakan keamanan, serta partisipasi aktif dari semua pemangku kepentingan menjadi kunci dalam menciptakan sistem yang aman dan adaptif. Meskipun berbagai solusi telah diusulkan, efektivitas implementasinya masih memerlukan pengujian lanjutan, terutama dalam aspek teknis dan ekonomis. Dengan demikian, kontribusi kolektif dari riset ini tidak hanya memperkaya pemahaman terhadap lanskap ancaman IoT, tetapi juga memberikan arah strategis bagi pengembangan kebijakan dan teknologi keamanan yang berkelanjutan di era digital.

IMPLIKASI PENELITIAN

Temuan dari kumpulan penelitian ini memiliki sejumlah implikasi strategis yang signifikan bagi pengembangan, pengelolaan, dan pengamanan sistem Internet of Things (IoT). Pertama, kompleksitas dan kerentanan sistem IoT menuntut adanya pendekatan keamanan yang

tidak hanya berfokus pada aspek teknis, tetapi juga memperhitungkan regulasi dan kebutuhan efisiensi operasional. Hal ini mengharuskan perancang sistem dan pembuat kebijakan untuk mengembangkan kerangka kerja yang fleksibel, dinamis, dan adaptif terhadap perubahan teknologi serta tuntutan hukum seperti GDPR dan HIPAA.

Kedua, integrasi teknologi canggih seperti AI, ML, blockchain, dan 5G dalam infrastruktur IoT memperluas permukaan serangan dan menimbulkan tantangan keamanan baru. Oleh karena itu, dibutuhkan regulasi yang mampu mengikuti perkembangan teknologi dan meningkatkan literasi keamanan di kalangan pengguna untuk meminimalkan risiko dari sisi manusia.

Ketiga, penerapan teknologi AI dan ML sebagai alat mitigasi ancaman terbukti menjanjikan, namun masih menghadapi keterbatasan praktis, seperti kurangnya data pelatihan representatif dan kebutuhan evaluasi dampak ekonomi. Ini menunjukkan perlunya investasi riset lanjutan dan kolaborasi multidisiplin untuk mengembangkan model AI yang lebih akurat, efisien, dan dapat diandalkan dalam konteks dunia nyata.

Keempat, integrasi aspek keamanan ke dalam strategi bisnis melalui konsep *security-by-design*, otentikasi multi-elemen, dan audit berkala harus menjadi bagian tak terpisahkan dari tata kelola organisasi. Hal ini penting untuk menjaga keberlangsungan operasional dan membangun kepercayaan konsumen terhadap sistem IoT.

Kelima, pendekatan holistik dan kolaboratif yang melibatkan seluruh pemangku kepentingan dari pemerintah, pengembang teknologi, penyedia layanan, hingga pengguna akhir menjadi kunci untuk menciptakan ekosistem digital yang aman, inklusif, dan resilien terhadap ancaman siber. Edukasi pengguna dan kesadaran publik terhadap praktik keamanan dasar perlu diperkuat sebagai lapisan pertahanan utama terhadap serangan berbasis human-error.

SARAN

Berdasarkan temuan dan implikasi yang telah diuraikan, disarankan agar pengembangan dan penerapan sistem IoT dilakukan dengan pendekatan menyeluruh yang mengintegrasikan aspek teknis, regulatif, dan sosial. Para pengembang perangkat dan sistem IoT perlu mengadopsi prinsip *security-by-design* sejak tahap perancangan, guna memastikan bahwa keamanan menjadi elemen inti, bukan sekadar pelengkap. Pemerintah dan lembaga regulasi juga perlu memperbarui kebijakan yang mampu mengikuti dinamika teknologi secara responsif, dengan menetapkan standar minimum keamanan yang adaptif terhadap berbagai jenis perangkat dan skenario penggunaan. Selain itu, investasi dalam pengembangan teknologi kecerdasan buatan yang andal untuk mendeteksi dan merespons ancaman secara real-time perlu ditingkatkan, khususnya dengan fokus pada peningkatan akurasi, efisiensi energi, dan relevansi data pelatihan.

Tidak kalah penting, organisasi dan pelaku industri disarankan untuk membangun budaya keamanan siber melalui pelatihan rutin dan peningkatan literasi keamanan digital di kalangan pengguna dan karyawan. Kolaborasi lintas sektor antara pengembang teknologi, akademisi, regulator, dan masyarakat sipil harus diperkuat guna menciptakan ekosistem IoT yang resilien dan inklusif. Mengingat karakteristik ancaman siber yang terus berevolusi, diperlukan pula sistem audit dan evaluasi berkala untuk memastikan ketahanan sistem dalam jangka panjang. Dengan demikian, pengelolaan keamanan IoT tidak hanya bersifat reaktif terhadap insiden, tetapi juga proaktif dan berkelanjutan dalam membangun kepercayaan digital di era konektivitas tinggi.

DAFTAR PUSTAKA

Akintayo, T. A., Asolo, E., Nnamani, C. C., Felix, O. A., Osaro, C. C., & Atinuke, A. T. (2024). Assessing the Cybersecurity Risks Associated with the Internet of Things (IoT) Devices. Mikailalsys Journal of Advanced Engineering International, 1(3), 170–184. https://doi.org/10.58578/mjaei.v1i3.3862

AlSalem, T., Almaiah, M., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics, 12(18), 3958. https://doi.org/10.3390/electronics12183958

Bakti, V. K., Sutanto, A., & Basit, A. (2023). Sistem Monitoring Ruang Data Center Kombinasi Multi Sensor dengan Application Programming Interface (API) Tuya. Smart Comp Jurnalnya Orang Pintar Komputer, 12(3), 806. https://doi.org/10.30591/smartcomp.v12i3.5306

Butsianto, S., Nugraha, U., Anwar, M., Anwar, S., & Judijanto, L. (2024). Cybersecurity in the Internet of Things (IoT) Era: Safeguarding Connected Systems and Data. Global International Journal of Innovative Research, 1(3), 290–297. https://doi.org/10.59613/global.v1i3.39

Dickson, S. M., & Okechukwu, I. P. (2023). Cyber Security in the Age of the Internet of Things, Constraints, and Solutions. Journal of Digital Learning and Distance Education, 2(11), 829–837. https://doi.org/10.56778/jdlde.v2i11.233

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal ICT Information Communication & Technology, 20(1), 42. https://doi.org/10.36054/jict-ikmi.v20i1.305

Ishak, N. (2023). Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges? Audito Comparative Law Journal (ACLJ), 4(2), 108. https://doi.org/10.22219/aclj.v4i2.26098

Islami, M. J. (2018). TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX. Masyarakat Telematika Dan Informasi Jurnal Penelitian Teknologi Informasi Dan Komunikasi, 8(2), 137. https://doi.org/10.17933/mti.v8i2.108

Lone, A. N., Mustajab, S., & Alam, M. (2023). A Comprehensive Study on Cybersecurity Challenges and Opportunities in the IoT World. Security and Privacy, 6(6). https://doi.org/10.1002/spy2.318

Megawati, S. (2021). Pengembangan Sistem Teknologi Internet of Things Yang Perlu Dikembangkan Negara Indonesia. Journal of Information Engineering and Educational Technology, 5(1), 19. https://doi.org/10.26740/jieet.v5n1.p19-26

Nishat Margia, I., Hasan, S. K., Islam, M. A., Asha, A. I., & Priya, S. A. (2024). Cybersecurity in the Age of IoT: Business Strategies for Managing Emerging Threats. International Journal For Multidisciplinary Research, 6(5). https://doi.org/10.36948/ijfmr.2024.v06i05.28076

Patel, K. N., Ashok, P., Chirputkar, A., & Pillai, S. (2024). Cybersecurity Risks and Countermeasures in the Threat Landscape of IoT Devices. 2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS), 875–883. https://doi.org/10.1109/ICTACS62700.2024.10841210

Pati, M. (2024). ANALISA KEAKURATAN ALGORITMA NAÏVE BAYES, SUPPORT VECTOR MACHINE (SVM), DAN LOGISTIC REGRESSION UNTUK DETEKSI MALWARE PADA TRAFIK DATA IoT.

Prabaswari, P., Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. Matra Pembaruan, 6(1), 1. https://doi.org/10.21787/mp.6.1.2022.1-14

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). Jurnal Pengabdian Nasional (JPN) Indonesia, 6(1), 38. https://doi.org/10.35870/jpni.v6i1.1097

Rao, L., Keerthiraj, Mishra, M., Misra, A., Arora, A. S., & Vadi, V. R. (2024). Improving Cybersecurity in Business Settings: The Challenges and Solutions of Internet of Things.

In Recent Trends In Engineering and Science for Resource Optimization and Sustainable Development (pp. 431–435). CRC Press. https://doi.org/10.1201/9781003596721-91

Sandhyakumari, G., Bharathi, M., Madhurima, V., Tabassum, S., Neelima, K., & Kumar, N. A. (2025). A Dynamic Cybersecurity Framework for Energy-Efficient Internet of Things (pp. 165–190). https://doi.org/10.4018/979-8-3693-6859-6.ch008

Sandi, G. H., & Fatma, Y. (2023). PEMANFAATAN TEKNOLOGI INTERNET OF THINGS (IOT) PADA BIDANG PERTANIAN. JATI (Jurnal Mahasiswa Teknik Informatika), 7(1), 1. https://doi.org/10.36040/jati.v7i1.5892

Shukur, F., & Shukur, S. T. (2023). A Comprehensive Analysis of Cybersecurity Threats based IoTs. Journal of Applied Artificial Intelligence, 4(2), 12–21. https://doi.org/10.48185/jaai.v4i2.920

Turyadi, I. U. (2021). Analisa Dukungan Internet of Things (IoT) terhadap Peran Intelejen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur. Jurnal Teknologi Dan Manajemen Informatika, 7(1), 29. https://doi.org/10.26905/jtmi.v7i1.6040

Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2024). PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL: TANTANGAN DAN SOLUSI.