Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT

[1]Ade Irawan, [2]Wildan Hamzah Nur Fadholi , [3]Zahwa Erikamaretha, [4]Fried Sinlae
[1,2,3,4] Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara, Jakarta
[1]202110715026@mhs.ubharajaya.ac.id, [2]202110715081@mhs.ubharajaya.ac.id, [3]202110715219@mhs.ubharajaya.ac.id, fried.sinlae@dsn.ubharajaya.ac.id

Abstract - The aim of this research is to analyze the challenges and strategies of cybersecurity management in Indonesia based on IoT. The research utilizes a literature review method to address the research questions posed. Data collection is conducted through various academic databases using common search engines such as Google Scholar. The data collection timeframe is between 2019 and 2024 to capture the latest literature on IoT-based risk management. The research findings indicate that information security is a major concern for businesses worldwide, with information security management being a significant challenge. Factors influencing a country's cybersecurity performance include the availability of expertise, structured decision-making processes, infrastructure management, specialized security solutions, OT/TI convergence, rapid incident response, and staff training. Cybersecurity strategies should be holistic and proactive, involving threat recognition, user training, policy development, early monitoring and detection, data encryption, access management, data backup, and collaboration with other security institutions. Cybersecurity systems should adopt an integrated approach to address challenges in the era of the Fourth Industrial Revolution, focusing on knowledge, technology, economics, social, and political aspects. Preparation for the Fourth Industrial Revolution requires solutions to secure supply chain systems, data exchanges, and production system reliability. IoT security management requires careful monitoring and control, as well as the integration of new technologies such as AI and blockchain to combat increasingly sophisticated attacks. Education and user awareness efforts are also crucial in reducing system vulnerabilities.

Keywords — Security Management, IoT, Challenges, and Strategies

Abstrak*— Tujuan penelitian ini menganalisis tantangan dan strategi manajemen keamanan siber di Indonesian berbasis IoT. Penelitian ini menggunakan metode literature review untuk menjawab pertanyaan penelitian yang diajukan. Pengumpulan data dilakukan melalui berbagai basis data akademik menggunakan mesin pencari umum seperti Google Scholar. Rentang waktu pengumpulan data adalah antara 2019 hingga 2024 untuk menangkap literatur terbaru tentang manajemen risiko berbasis IoT. Hasil penelitian menunjukan bahwa keamanan informasi menjadi perhatian utama bagi bisnis di seluruh dunia, dengan manajemen keamanan informasi menjadi tantangan penting. Faktor-faktor yang mempengaruhi performa keamanan siber suatu negara meliputi ketersediaan tenaga ahli, proses pengambilan keputusan yang terstruktur, manajemen infrastruktur, solusi keamanan yang dirancang khusus, konvergensi OT/TI, respons insiden cepat, dan pelatihan staf. Strategi keamanan siber harus holistik dan proaktif, melibatkan pengenalan ancaman, pelatihan pengguna, pengembangan kebijakan, pemantauan dan deteksi dini, enkripsi data, manajemen akses, pencadangan data, dan kolaborasi dengan lembaga keamanan lainnya. Sistem keamanan siber harus membangun pendekatan terpadu untuk menghadapi tantangan di era Revolusi Industri 4.0, dengan fokus pada aspek pengetahuan, teknologi, ekonomi, sosial, dan politik. Persiapan menghadapi revolusi industri 4.0 menuntut solusi yang dapat mengamankan sistem suplai pusat, pertukaran data, dan keandalan sistem produksi. Manajemen keamanan IoT memerlukan pemantauan dan kontrol yang cermat, serta integrasi teknologi baru seperti AI dan blockchain untuk melawan serangan yang semakin canggih. Upaya edukasi dan kesadaran pengguna juga penting dalam mengurangi kerentanan sistem.

Kata Kunci— Manajemen Keamanan, IoT, Tantangan dan Strategi

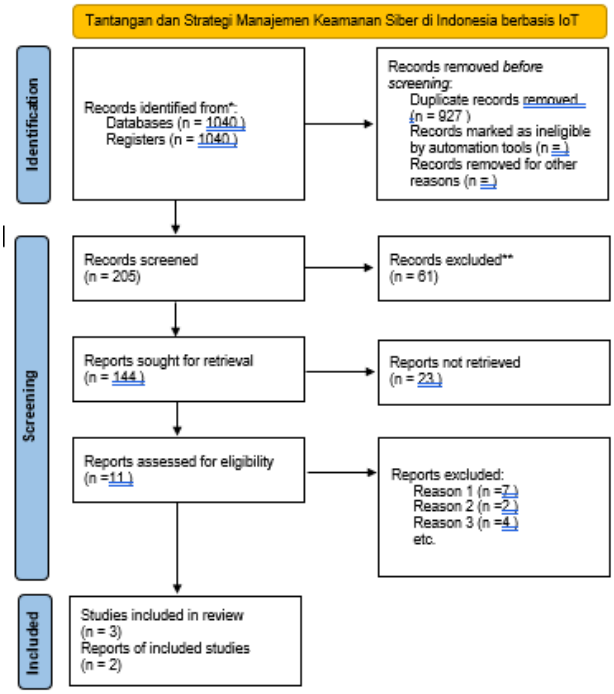
I. Pendahuluan

Keamanan sistem informasi menjadi pokok bahasan yang sangat penting dalam era digital saat ini. Ancaman seperti serangan malware, phishing, dan ancaman dari dalam organisasi semakin kompleks dan seringkali memerlukan pendekatan yang menyeluruh. Strategi-strategi yang penting dalam konteks ini mencakup enkripsi data, pemantauan keamanan secara real-time, dan pelatihan karyawan tentang keselamatan[1]. Keamanan informasi atau keamanan cyber merujuk pada upaya menjaga kerahasiaan, integritas, dan ketersediaan informasi di dunia maya[2]. Dunia maya merujuk pada lingkungan kompleks yang terbentuk dari interaksi antara manusia, perangkat lunak, dan layanan internet melalui penggunaan berbagai perangkat teknologi serta berbagai koneksi jaringan, dalam sebuah lingkungan yang informal.

Keamanan cyber adalah praktik untuk melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya. Ini juga dikenal sebagai keamanan teknologi informasi atau keamanan informasi elektronik[3]. Keamanan siber sebagai praktik untuk melindungi berbagai sistem, jaringan, dan program dari serangan digital[4]. Dengan demikian, keamanan siber atau keamanan informasi bertujuan untuk melindungi informasi di dunia maya dari berbagai serangan. Peran keamanan siber semakin penting seiring dengan peningkatan penggunaan komputer seperti desktop, laptop, ponsel pintar, server, dan perangkat Internet of Things (IoT), serta penggunaan jaringan komputer seperti Internet dalam kehidupan sehari-hari. Keamanan informasi memainkan peran kunci dalam manajemen perusahaan, karena menangani kerahasiaan,

privasi, integritas, dan ketersediaan salah satu sumber daya terpenting[5].

Menurut Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN), sejak 1 Januari hingga 12 April 2020, telah tercatat 88.414.296 serangan siber. Pada bulan Januari, terdapat 25.224.811 serangan yang terpantau, diikuti oleh 29.188.645 serangan pada bulan Februari, kemudian 26.423.989 serangan pada bulan Maret, dan sampai dengan 12 April 2020, telah terjadi 7.576.851 serangan. Puncak jumlah serangan terjadi pada tanggal 12 Maret 2020, dengan mencapai 3.344.470 serangan, dan setelah itu jumlah serangan mengalami penurunan yang



cukup signifikan saat diberlakukan kebijakan work from home (WFH) di berbagai tempat[6].

IoT (*Internet of Things)* memperluas internet yang berkelanjutan dengan memungkinkan pertukaran data, kendali jarak jauh, dan penerimaan sensor pada berbagai hal seperti makanan, elektronik, dan peralatan melalui sensor tertanam yang terhubung ke jaringan lokal dan seluruh dunia[7]. IoT telah mengotomatiskan tugas-tugas rutin di rumah, memungkinkan orang untuk memantau dan mengontrol perangkat dari jarak jauh, meningkatkan kenyamanan dan efisiensi. Dalam skala industri, IoT memungkinkan organisasi melacak aset, memantau peralatan, dan menciptakan konektivitas keseluruhan antara objek dan sistem. Produsen menggunakan sensor jaringan pada peralatan produksi untuk mengumpulkan data operasional dan mendeteksi masalah, sementara perusahaan logistik melacak truk pengiriman secara real-time.

Revolusi IoT telah meningkatkan risiko keamanan siber secara signifikan, sehingga membutuhkan strategi manajemen yang proaktif[8]. Dengan lebih dari 30 miliar perangkat yang diprediksi pada tahun 2025, teknologi ini menghadirkan banyak rute serangan dan kerentanan. Bisnis harus beradaptasi dengan perkembangan global dengan memadukan metode produksi tradisional dengan teknologi canggih[9]. Mengatasi cakupan jaringan, kerentanan perangkat, dan deteksi waktu nyata sangatlah penting. Menerapkan platform pemantauan terpadu, mendorong standar keamanan tingkat perangkat, dan memanfaatkan teknologi otomatis seperti AI dan pembelajaran mesin sangat penting untuk melawan ancaman yang baru lahir di era yang sangat terhubung ini. Tujuan penelitian ini menganalisis tantangan dan strategi manajemen keamanan siber di Indonesian berbasis IoT

II. Metode Penelitian

Penelitian ini menggunakan metode *literature review* dengan tujuan untuk memberikan jawaban atas pertanyaan penelitian yang diuraikan dalam pendahuluan. Pengumpulan data berbagai basis data akademik mesin pencari umum, seperti Google Scholar, digunakan untuk mengumpulkan sumber yang relevan. Data dikumpulkan dengan rentang waktu antara 2019-2024, agar dapat menangkap literatur yang baru diterbitkan, serta jurnal yang diterbitkan pada awal perkembangan manajemen keamanan cyber berbasis IoT inti, tren serangan, dan kerentanan perangkat. Metodologi yang diadopsi dalam tinjauan sistematis digambarkan dalam prisma pada Gambar 1.

Gambar 1: Diagram Alir Literature Review untuk Manajemen Resiko berbasis IoT

Berdasarkan diagram alir di atas, catatan awal yang ditemukan dari semua basis data terdaftar dalam fase identifikasi. Ini adalah nomor catatan mentah yang belum disaring dan diurutkan. Jumlah total dari masing-masing basis data online adalah kombinasi dari pencarian semua istilah pencarian untuk tinjauan sistematis. Setiap istilah pencarian dari tinjauan sistematis ini yang mencakup "manajemen resiko" dan "IoT", " diterapkan secara seragam pada setiap basis data online. Catatan-catatan ini kemudian diperiksa untuk duplikasi selama tahap identifikasi lebih lanjut.

Pada tahap ini, perangkat lunak EndNote digunakan dan menjadi alat yang sangat berguna dalam menghapus catatan-catatan yang diduplikasi. Dapat dilihat dari diagram alir bahwa ada beberapa perubahan dalam jumlah catatan, meskipun tidak ada duplikasi karena menunjukkan jumlah catatan yang sama. Selama tahap penyaringan, semua catatan digabungkan menjadi satu folder di EndNote.

Peneliti melakukan penghapusan duplikasi manual dari catatan-catatan karena disebutkan bahwa beberapa catatan yang diduplikasi mungkin tidak terdeteksi dalam fungsi temukan duplikat EndNote. Hal ini disebabkan oleh referensi yang mungkin tidak diperbarui untuk mendeteksi catatan yang sama. Pada tahap ini, kriteria inklusi dan eksklusi diterapkan bersama dengan kriteria penyaringan. Terlihat adanya penurunan yang signifikan dalam jumlah catatan setelah proses ini selesai dilakukan. Kriteria penyaringan diterapkan untuk mencari catatan yang tidak memenuhi syarat. Catatan-catatan yang tidak

dapat diakses atau tanpa penulis disaring, dan jumlah catatan tersebut kemudian dikurangi sebanyak 5 dari total catatan. Total baru dari catatan-catatan sekarang dianggap memenuhi syarat untuk diakses. Jumlah catatan akhir ini juga menunjukkan jumlah akhir literatur terkait manajemen resiko berbasis IoT.

III. Hasil dan Pembahasan

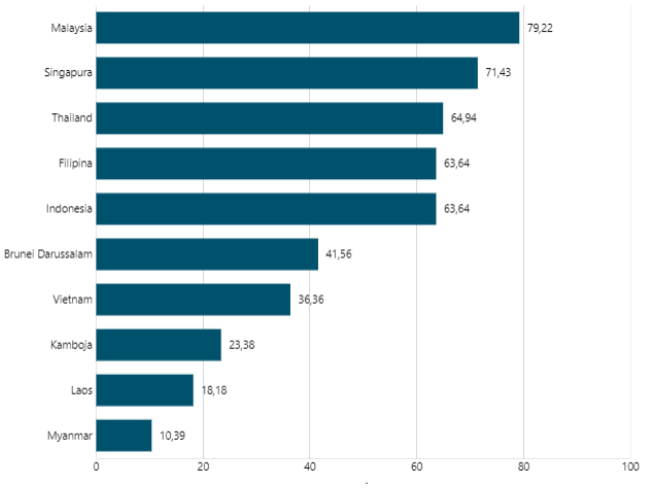
Tantangan dan Strategi Keamanan Cyber di Indonesia

Keamanan informasi menjadi perhatian utama bagi bisnis di seluruh dunia karena operasi yang berada dalam pasar global, ketergantungan yang tinggi pada teknologi informasi, serta kehadiran online dan digital yang menyeluruh. Manajemen keamanan informasi menjadi tantangan penting bagi perusahaan-perusahaan ini, yang berusaha untuk mencegah terjadinya ancaman keamanan dan privasi terhadap sistem informasi dan infrastruktur jaringan[5].

Perkembangan teknologi yang pesat telah membawa tantangan baru dalam bidang keamanan siber. Semakin banyaknya perangkat yang terhubung ke internet meningkatkan kerentanan terhadap serangan, baik oleh individu, kelompok terorganisir, maupun negara. Kekurangan tenaga ahli keamanan siber menjadi masalah serius, sementara teknik serangan yang semakin canggih mempersulit upaya perlindungan. Kerentanan pada sistem dan aplikasi juga sering dimanfaatkan oleh penyerang. Ancaman keamanan siber terus berkembang dan memerlukan respons yang cepat dan adaptif. Namun, tantangan dalam memperkuat keamanan siber meliputi kurangnya ketersediaan pakar teknologi, munculnya penyedia layanan telekomunikasi baru, dan kurangnya peraturan internasional yang mengatur perilaku negara. Oleh karena itu, perlindungan terhadap keamanan siber menjadi semakin penting dalam menghadapi ancaman dan risiko yang terus berkembang di dunia maya[1].

Keamanan siber memegang peran yang sangat penting dalam melindungi keamanan data karena sangat penting untuk menjaga informasi di dalam media penyimpanan serta memastikan data yang dikirim tetap aman. Keamanan siber merupakan perlindungan terhadap struktur siber dari ancaman siber. Ini melibatkan perlindungan ganda terhadap data dan struktur dari akses yang tidak sah melalui kerahasiaan, integritas, otentikasi, non-penolakan, dan ketersediaan data untuk melindungi dari serangan siber. Dengan pendekatan yang terlindungi, sistem menyediakan pemulihan fakta dengan menggabungkan kemampuan keamanan, deteksi, dan respons[10].

Menurut Laporan National Cyber Security Index (NCSI), skor indeks keamanan siber Indonesia pada tahun 2022 adalah sebesar 38,96 poin dari 100. Angka ini menempatkan Indonesia di peringkat ke-3 terendah di antara negara-negara G20. Secara global, Indonesia menduduki peringkat ke-83 dari 160 negara dalam daftar yang disajikan dalam laporan tersebut. Menurut Laporan National Cyber Security Index (NCSI), skor indeks keamanan siber Indonesia pada tahun 2023 sebagai berikut:



Gambar. 2. Skor Indeks Keamanan Siber Indonesia

Berdasarkan laporan National Cyber Security Index (NCSI), Indonesia berhasil masuk lima besar negara dengan keamanan siber terbaik di kelompok Association of Southeast Asian Nations (ASEAN) pada tahun 2023. Indonesia memperoleh penilaian sebesar 63,64 poin dari skor maksimal 100 poin. Secara global, Indonesia menempati peringkat ke-49 dari 176 negara yang disertakan dalam laporan tersebut. Bobot skor penilaian Indonesia setara dengan Filipina. Sementara itu, Malaysia diakui sebagai negara dengan keamanan siber terbaik di Asia Tenggara dengan meraih skor 79,22 poin. Malaysia juga menempati peringkat ke-22 secara global. Singapura menduduki posisi kedua di Asia Tenggara dengan skor keamanan siber sebesar 71,43 poin, diikuti oleh Thailand dengan skor 64,94 poin. Beberapa negara lain di Asia Tenggara berada di bawah peringkat Indonesia, termasuk Brunei Darussalam, Vietnam, Kamboja, Laos, dan Myanmar yang meraih skor keamanan siber kurang dari 50 poin.

NCSI membuat penilaian ini berdasarkan sejumlah indikator, termasuk aturan hukum negara terkait keamanan siber, ketersediaan lembaga pemerintah di bidang keamanan siber, kerja sama pemerintah terkait keamanan siber, serta bukti-bukti publik seperti situs resmi pemerintah atau program lain yang terkait.

Faktor-faktor yang mempengaruhi performa keamanan siber suatu negara mencakup beberapa aspek penting. Pertama, ketersediaan departemen spesialisasi teknologi operasional khusus menjadi kunci, di mana perusahaan industri memerlukan tim keamanan OT yang berkualitas untuk melindungi jaringan industri. Kedua, proses pengambilan keputusan yang terstruktur dengan jelas diperlukan agar visibilitas proses industri memadai dan implementasi proyek baru tidak terhambat. Selain itu, strategi manajemen infrastruktur legasi menjadi perhatian penting, di mana kehati-hatian dalam membangun sistem kontrol untuk jaringan industri yang sudah usang diperlukan. Selanjutnya, penting untuk memperkenalkan solusi keamanan yang dirancang khusus untuk ekosistem industri, karena solusi standar tidak cukup untuk melindungi proses industri. Selain itu, strategi konvergensi OT/TI dengan mempertimbangkan IIoT

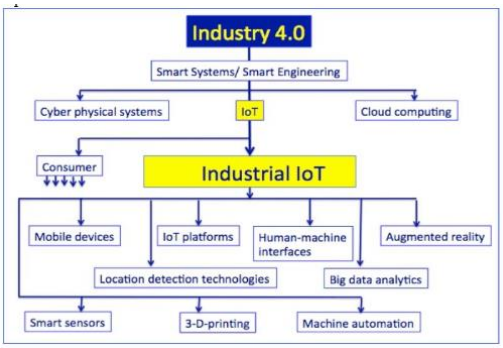
diperlukan untuk mengintegrasikan teknologi operasional dan informasi dengan aman. Respon insiden secara cepat juga penting, dengan regulasi respons cepat yang matang dan tim yang mampu mengidentifikasi serta menangani masalah dengan cepat. Terakhir, pelatihan staf tentang dasar-dasar keamanan dan memantau kepatuhan terhadap peraturan internal menjadi kunci untuk mengurangi dampak insiden terkait keamanan. Dengan memperhatikan semua aspek ini, suatu negara dapat meningkatkan kinerja keamanan siber secara keseluruhan[11].

Strategi keamanan siber merupakan serangkaian tindakan, kebijakan, dan praktik yang dirancang untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari serangan siber serta ancaman keamanan lainnya. Strategi ini bersifat holistik dan mencakup berbagai pendekatan untuk membendung ancaman dan merespons potensi serangan. Beberapa strategi yang umum digunakan meliputi pengenalan ancaman (threat intelligence) untuk mengumpulkan informasi tentang potensi ancaman dunia maya, pelatihan dan kesadaran pengguna tentang praktik keamanan terbaik, pengembangan kebijakan keamanan yang jelas dan ketat, pemantauan dan deteksi dini menggunakan alat-alat yang tepat, pembaruan perangkat lunak secara berkala, enkripsi data untuk melindungi informasi sensitif, manajemen akses dengan prinsip hak istimewa paling rendah, pencadangan data secara teratur, kolaborasi dan kemitraan dengan lembaga keamanan siber lainnya untuk berbagi intelijen ancaman siber. Dengan menerapkan strategi keamanan siber yang holistik dan proaktif, perusahaan dapat mengurangi risiko serangan siber dan meminimalkan dampak serangan yang terjadi[1].

Sistem keamanan siber harus membangun pendekatan yang terpadu untuk melawan tantangan eksternal dan internal, serta menghadapi perubahan yang terjadi di era Revolusi Industri 4.0. Tantangan ini merambah ke aspek bisnis di berbagai bidang yang harus siap menghadapi perubahan global yang menggabungkan manufaktur tradisional dengan praktik industri yang didukung oleh teknologi. Terdapat lima tantangan besar yang akan dihadapi, yakni dalam aspek pengetahuan, teknologi, ekonomi, sosial, dan politik

Manajemen Keamanan berbasis IoT

Dalam persiapan menghadapi revolusi industri 4.0, seperti yang terlihat dengan meningkatnya adopsi Internet of Things (IoT) dan Industrial Internet of Things (IIoT), bisnis menghadapi risiko yang tak terhindarkan. Ini mendorong para pelaku bisnis untuk menuntut solusi dalam mengamankan sistem suplai pusat, pertukaran data yang aman, dan keandalan sistem produksi. Kementerian Perindustrian telah merancang "Making Indonesia 4.0" sebagai roadmap terintegrasi untuk mengimplementasikan sejumlah strategi dalam menghadapi era Industri 4.0. Para peneliti di Center for Indonesian Policy Studies (CIPS), seperti Imelda Freddy, menekankan bahwa Industri 4.0 memperkenalkan era smart factories, di mana mekanisme robot atau sistem fisik siber akan mengawasi proses fisik yang terjadi di dalam pabrik. Sistem tersebut memiliki kemampuan untuk membuat keputusan sendiri, sehingga dengan adanya perubahan tren industri seperti ini muncul kekhawatiran bahwa peluang pekerjaan akan berkurang karena diambil alih oleh robot dan mesin. Namun, peningkatan kapasitas pekerja dapat dilakukan melalui pelatihan, kursus, dan sertifikasi. Para pelaku industri harus ikut serta dalam upaya ini karena peningkatan kapasitas pekerja akan berdampak positif terhadap industri itu sendiri.



Gambar 3. Manajemen Cyber berbasi IoT

Jaringan IoT menghadirkan tantangan yang signifikan untuk manajemen keamanan karena cakupan jaringan yang luas, kerentanan perangkat yang melekat, dan kesulitan untuk mengatasi ancaman. Organisasi kesulitan untuk memantau dan mengontrol keamanan dalam jaringan yang kompleks, dengan sensor, kamera, dan pengontrol yang diretas menjadi pintu masuk bagi pelaku kejahatan. Deteksi, identifikasi, dan remediasi serangan merupakan hambatan yang terus-menerus, sehingga mendorong pertimbangan ulang strategi manajemen dalam pengaturan IoT.

Keamanan infrastruktur IoT merupakan lanskap yang kompleks dan terdistribusi, yang membutuhkan pemantauan dan kontrol yang cermat[12]. Ekosistem IoT perusahaan, yang meliputi platform cloud, server, titik akhir desktop, perangkat seluler, dan sensor yang terhubung, bisa jadi sulit untuk dikelola karena topologi yang tersebar. Kurangnya visibilitas ke semua titik akhir dan jalur transmisi memungkinkan kerentanan untuk menghindari kontrol keamanan. Penyerang dapat mengidentifikasi titik-titik buta dalam instalasi IoT perusahaan yang sangat besar, membuat organisasi terekspos pada pelanggaran jaringan. Menegakkan standar keamanan secara seragam juga sulit dilakukan karena penyebaran perangkat yang cepat.

Lingkup IoT menghadirkan tantangan keamanan karena kurangnya keamanan yang tertanam dalam perangkat. Perangkat IoT konsumen memprioritaskan kenyamanan, penghematan biaya, dan fungsionalitas di atas kontrol akses yang ketat dan perlindungan data. Hal ini mengakibatkan kerentanan seperti kata sandi default yang tidak aman, lalu lintas yang tidak terenkripsi, dan tambalan keamanan yang hilang. Sistem-sistem ini, seperti bel pintu pintar, pengontrol gedung, perangkat medis, dan sistem kontrol industri, sangat rentan terhadap eksploitasi seperti serangan DDoS dan

pembajakan jarak jauh[13]. Tanpa standar keamanan dasar, miliaran titik akhir yang rentan ini menimbulkan risiko infrastruktur yang signifikan, sehingga memperluas permukaan serangan bagi organisasi.

Sistem IoT semakin rentan terhadap serangan siber karena keragaman perangkat dan teknik ancaman yang canggih. Serangan-serangan ini sulit dideteksi dan ditanggulangi karena kompleksitas interaksi di seluruh jaringan yang didukung IoT. Ancaman dapat menggunakan komunikasi enkripsi C2, *malware* polimorfik, injeksi SQL, dan serangan *spoofing* untuk mem-*bypass* deteksi tanda tangan[9]. Kompleksitas serangan-serangan ini membuat tim keamanan kebingungan dalam bereaksi terhadap sistem yang disusupi dan data sensitif. Strategi perlindungan di masa depan mencakup AI dan pembelajaran mesin untuk meningkatkan pengenalan pola dan model data grafik untuk mengungkap anomali. Namun, masalah biaya dan keahlian telah memperlambat adopsi, dan ancaman tersembunyi terus mengeksploitasi tantangan deteksi yang melekat di seluruh infrastruktur IoT.

Ekosistem IoT meningkatkan permukaan serangan siber, sehingga membutuhkan integrasi keamanan yang komprehensif di seluruh perangkat keras, perangkat lunak, protokol komunikasi, interkoneksi cloud, dan manajemen siklus hidup. Pengembang harus merekayasa kontrol akses yang ketat, enkripsi data, deteksi anomali, dan saluran pembaruan firmware, sementara tim hukum mengadvokasi kebijakan dan peraturan untuk mengurangi prevalensi kerentanan. Kolaborasi lintas departemen meningkatkan kesadaran situasional dan memastikan langkah-langkah keamanan tertanam dan terus diperkuat di seluruh jajaran teknologi IoT untuk memerangi risiko.

Keamanan IoT bergantung pada elemen manusia, yang tetap menjadi kerentanan yang signifikan[14]. Untuk memitigasi hal ini, organisasi harus menerapkan program edukasi yang komprehensif, meningkatkan kesadaran pengguna akan risiko siber IoT[15]. Ini termasuk pelatihan tentang kebersihan keamanan, taktik rekayasa sosial, prosedur akses fisik, dan penanganan data di seluruh titik kontak IoT. Latihan simulasi krisis langsung dan pembaruan pembelajaran mikro menjaga pemahaman keamanan tetap segar. Pendekatan ini meningkatkan ketahanan organisasi dalam lingkungan IoT yang berubah-ubah.

Teknologi dan inovasi IoT sangat penting dalam mengatasi beragam permukaan serangan ekosistem IoT. Alat tradisional seperti *firewall*, VPN, dan *anti-malware* tidak cukup untuk menghadapi ancaman yang berfokus pada IoT. Teknologi yang muncul seperti blockchain, mikrosegmentasi, dan jaringan penipuan menawarkan metode baru untuk verifikasi, kompartementalisasi, dan deteksi serangan dini. Teknologi – teknologi ini memperkuat ketahanan terhadap serangan multi-vektor kontemporer, meskipun biaya implementasi masih menjadi hambatan bagi adopsi secara luas.

IV. Kesimpulan

Hasil penelitian menunjukan bahwa keamanan informasi menjadi perhatian utama bagi bisnis di seluruh dunia, dengan manajemen keamanan informasi menjadi tantangan penting. Faktor-faktor yang mempengaruhi performa keamanan siber suatu negara meliputi ketersediaan tenaga ahli, proses pengambilan keputusan yang terstruktur, manajemen infrastruktur, solusi keamanan yang dirancang khusus, konvergensi OT/TI, respons insiden cepat, dan pelatihan staf. Strategi keamanan siber harus holistik dan proaktif, melibatkan pengenalan ancaman, pelatihan pengguna, pengembangan kebijakan, pemantauan dan deteksi dini, enkripsi data, manajemen akses, pencadangan data, dan kolaborasi dengan lembaga keamanan lainnya. Sistem keamanan siber harus membangun pendekatan terpadu untuk menghadapi tantangan di era Revolusi Industri 4.0, dengan fokus pada aspek pengetahuan, teknologi, ekonomi, sosial, dan politik. Persiapan menghadapi revolusi industri 4.0 menuntut solusi yang dapat mengamankan sistem suplai pusat, pertukaran data, dan keandalan sistem produksi. Manajemen keamanan IoT memerlukan pemantauan dan kontrol yang cermat, serta integrasi teknologi baru seperti AI dan blockchain untuk melawan serangan yang semakin canggih. Upaya edukasi dan kesadaran pengguna juga penting dalam mengurangi kerentanan sistem.

V. Daftar Pustaka

[1] Muslim, A. Sephira, M. H. Abrar, S. L. S. P. Angin, and H. Hidayatullah, "Analisis Keamanan Siber (Cyber Security) Dalam Era Digital 'Tantangan Dan Strategi Pengamanan,'" *J. Ilmu Komput. Revolusioner*, vol. 8, no. 2, Art. no. 2, Feb. 2024, Accessed: Apr. 02, 2024. [Online]. Available: https://com.ojs.co.id/index.php/jikr/article/view/116

[2] International Organization for Standardization, "ISO/IEC 27032:2012," ISO. Accessed: Apr. 02, 2024. [Online]. Available: https://www.iso.org/standard/44375.html

[3] Kaspersky, "What is Cyber Security?," www.kaspersky.com. Accessed: Apr. 02, 2024. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[4] Cisco, "What Is Cybersecurity?," Cisco. Accessed: Apr. 02, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[5] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *J. Cybersecurity Priv.*, vol. 1, no. 2, Art. no. 2, Jun. 2021, doi: 10.3390/jcp1020012.

[6] Badan Siber dan Sandi Negara, "Rekap Serangan Siber (Januari – April 2020) | www.bssn.go.id." Accessed: Apr. 02, 2024. [Online]. Available:

https://www.bssn.go.id/rekap-serangan-siber-januari-april-2020/
[7] T. AP, "Sejarah Dan Pemanfaatan Iot Di Era Industri 4.0," *Portaldata.org*, vol. 2, no. 4, pp. 1–8, 2022.
[8] S. Ariyaningsih, A. A. Andrianto, A. S. Kusuma, and R. A. Prastyanti, "Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia," *Justisia J. Ilmu Huk.*, vol. 1, no. 1, pp. 1–11, 2023.
[9] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.
[10] D. A. Sudarmadi and A. J. S. Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *J. Kaji. Strat. Ketahanan Nas.*, vol. 2, no. 2, pp. 157–178, 2019.
[11] Y. Daeng *et al.*, "Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, Art. no. 6, Nov. 2023, doi: 10.31004/innovative.v3i6.6376.
[12] F. Indah and A. Q. Sidabutar, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)," *J. Bid. Penelit. Inform.*, vol. 1, no. 1, p. 2, 2022.
[13] S. A. M. Babys, "Ancaman Perang Siber di Era Digital dan Solusi Keamanan Indonesia," *J. Oratio Directa*, vol. 3, no. 1, pp. 425–442, 2021.
[14] F. P. Nugroho, R. W. Abdullah, S. Wulandari, and Hanafi, "Keamanan Big Data di Era Digital di Indonesia," *J. Inf.*, vol. 5, no. 1, pp. 28–34, 2019.
[15] M. Subhan Abdullah and I. Heidiani Iksari, "Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan," *J. Ris. Inform. Dan Inov.*, vol. 1, no. 1, pp. 96–98, 2023.