Technologia Journal: Jurnal Informatika
e-ISSN : 3046-9163
Vol.1.No.2,Tahun 2024
DOI : https://doi.org/10.62872/v2tffe44

Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT)

Desi Ratna Sari
Universitas Jambi, Indonesia
e-mail: **nfdhlh14@gmail.com**

ABSTRAK

Analisis keamanan sistem informasi dalam era Internet of Things (IoT) mengungkapkan kompleksitas dan tantangan yang terkait dengan memastikan integritas dan keamanan infrastruktur yang semakin terhubung. Metode penelitian yang digunakan dalam penelitian ini merupakan penelitian kualitatif, Data terkait keamanan sistem informasi dalam konteks IoT akan dikumpulkan dari berbagai sumber, termasuk literatur ilmiah, laporan riset, dan dokumentasi teknis dan dianalisis literatur yang mendalam. Ancaman serius seperti malware, ransomware, dan serangan denial of service (DoS) memerlukan pendekatan proaktif dan holistik dalam menghadapinya. Kurangnya standar keamanan yang konsisten, kerentanan interoperabilitas perangkat, dan kurangnya kesadaran keamanan pengguna akhir menjadi fokus utama dalam upaya meningkatkan keamanan dalam lingkungan IoT. Diperlukan kerja sama antara industri, pemerintah, dan pemangku kepentingan lainnya untuk mengembangkan standar keamanan yang kuat, meningkatkan kesadaran keamanan pengguna, dan mengatasi tantangan interoperabilitas. Melalui langkah-langkah ini, diharapkan dapat menciptakan lingkungan IoT yang lebih aman dan terjamin, menjaga integritas data serta keamanan infrastruktur di era yang semakin terhubung dan kompleks

Kata kunci: IoT; Keamanan Sistem Informasi

PENDAHULUAN

Pada era digital yang terus berkembang, Internet of Things (IoT) telah menjadi pilar utama dalam transformasi teknologi (Megawati, 2021). Konsep ini mendasari integrasi dan konektivitas antara berbagai perangkat elektronik, sensor, dan sistem komputer melalui jaringan internet (Antara, 2024). IoT memungkinkan objek-objek yang dulu pasif menjadi 'cerdas', mampu berkomunikasi, memantau lingkungan sekitar, dan merespons secara otomatis tanpa campur tangan manusia. Salah satu aspek utama dari IoT adalah kemampuannya untuk menghasilkan dan mengumpulkan data secara terus-menerus. Melalui sensor-sensor yang tertanam pada perangkat, IoT menghasilkan aliran data yang mencakup informasi tentang kondisi fisik, lokasi, dan aktivitas dari berbagai objek yang terhubung (Santo, 2022). Data ini kemudian dapat dianalisis untuk mendapatkan wawasan yang berharga, memungkinkan pengambilan keputusan yang lebih cerdas dan efisien.

Pada era digital yang terus berkembang, Internet of Things (IoT) telah menjadi salah satu konsep yang mengubah paradigma dalam pengelolaan dan interaksi antara perangkat-perangkat yang terhubung melalui jaringan internet

(Aulia, 2023). IoT memungkinkan perangkat-perangkat elektronik, sensor, perangkat mobile, dan berbagai jenis perangkat lainnya untuk saling berkomunikasi dan bertukar data secara otomatis tanpa perlu campur tangan manusia. Konsep ini membawa kemungkinan besar dalam mengoptimalkan berbagai aspek kehidupan sehari-hari dan industri (Amane, 2023). Dalam konteks rumah pintar, IoT memungkinkan integrasi yang mulus antara berbagai perangkat elektronik dan sistem keamanan. Misalnya, lampu, perangkat pendingin udara, kunci pintu pintar, peralatan dapur seperti oven atau kulkas, dan bahkan sistem keamanan seperti kamera pengawas atau sensor gerak dapat terhubung ke jaringan internet melalui teknologi IoT. Dengan adanya konektivitas ini, pengguna dapat mengendalikan dan mengotomatisasi berbagai fungsi rumah mereka dari jarak jauh melalui aplikasi seluler atau perangkat lain yang terhubung ke internet. Sebagai contoh, pengguna dapat menyalakan atau mematikan lampu, menyesuaikan suhu ruangan, mengunci atau membuka pintu, memeriksa isi kulkas, dan bahkan memantau keamanan rumah secara real-time dari mana saja.

Selain itu, IoT juga memungkinkan adanya interaksi antara berbagai perangkat di dalam rumah. Misalnya, ketika sensor gerak mendeteksi aktivitas di ruangan, lampu dapat menyala secara otomatis atau sistem keamanan dapat memberikan notifikasi kepada pemilik rumah. Ini tidak hanya meningkatkan kenyamanan pengguna, tetapi juga meningkatkan keamanan rumah dengan memberikan pemantauan dan kontrol yang lebih baik.

Selain itu, beberapa perangkat IoT juga dilengkapi dengan kemampuan untuk belajar dan beradaptasi dengan kebiasaan pengguna. Misalnya, sistem pendingin udara pintar dapat belajar preferensi suhu penghuni rumah dan mengatur suhu secara otomatis untuk menciptakan lingkungan yang nyaman sesuai dengan keinginan pengguna. Secara keseluruhan, integrasi IoT dalam rumah pintar memberikan tingkat kenyamanan, efisiensi, dan keamanan yang lebih tinggi bagi penghuninya (Mukin, 2023). Dengan kemampuan untuk mengontrol dan memantau berbagai aspek rumah dari jarak jauh, IoT membantu menciptakan lingkungan hunian yang cerdas dan responsif terhadap kebutuhan penghuninya (Erwin, 2023). Di sektor industri, IoT digunakan untuk memantau dan mengelola proses produksi secara efisien. Sensor-sensor yang terpasang pada peralatan dan mesin memungkinkan pengumpulan data secara real-time tentang kinerja peralatan, kondisi lingkungan, dan parameter produksi lainnya. Data ini kemudian dianalisis untuk mengidentifikasi pola, memprediksi kerusakan, dan mengoptimalkan kinerja proses produksi secara keseluruhan (Prawiyogi, 2023).

Selain itu, IoT juga berperan penting dalam pengembangan kota cerdas (smart cities). Konsep ini mencakup penerapan teknologi IoT untuk memantau dan mengelola infrastruktur kota, seperti sistem transportasi, pencahayaan jalan, manajemen limbah, dan layanan publik lainnya (Marine, 2018). Dengan menggunakan data yang dikumpulkan melalui sensor-sensor yang terintegrasi, kota cerdas dapat meningkatkan efisiensi penggunaan sumber daya dan memberikan layanan yang lebih baik kepada warganya.

Di sektor industri, implementasi Internet of Things (IoT) telah membawa perubahan revolusioner dalam pengelolaan proses produksi (Yusuf, 2023). Sensor-sensor yang terpasang pada peralatan dan mesin memungkinkan pengumpulan data secara real-time tentang berbagai aspek kinerja, mulai dari suhu dan tekanan hingga kecepatan dan efisiensi operasional. Data yang dikumpulkan ini memberikan pemahaman yang mendalam tentang kondisi peralatan dan lingkungan produksi secara keseluruhan. Dengan menganalisis data tersebut, perusahaan dapat mengidentifikasi pola-pola tertentu, mendeteksi anomali, dan bahkan memprediksi kerusakan potensial pada peralatan. Hal ini memungkinkan perusahaan untuk mengambil tindakan preventif dengan melakukan perawatan yang diperlukan sebelum terjadinya kerusakan yang tidak diinginkan, sehingga mengurangi waktu henti produksi dan biaya perbaikan yang tidak terduga.

Selain itu, data yang dikumpulkan juga digunakan untuk mengoptimalkan kinerja proses produksi secara keseluruhan. Dengan pemahaman yang lebih baik tentang parameter-produksi kunci dan faktor-faktor yang memengaruhinya, perusahaan dapat melakukan penyesuaian secara real-time untuk meningkatkan efisiensi, mengurangi limbah, dan meningkatkan kualitas produk. Dengan demikian, implementasi IoT dalam sektor industri membawa dampak yang signifikan dalam meningkatkan produktivitas, efisiensi, dan keandalan proses produksi (Atmajaya, 2024). Dengan kemampuan untuk memantau dan mengelola operasi secara real-time, perusahaan dapat mengambil keputusan yang lebih tepat waktu dan berbasis data, yang pada gilirannya menghasilkan

Keberhasilan implementasi IoT membawa sejumlah tantangan yang perlu diatasi. Salah satunya adalah masalah keamanan, yang semakin menjadi perhatian karena jumlah perangkat yang terhubung terus meningkat. Dengan banyaknya titik akses ke jaringan, IoT memberikan peluang bagi penyerang siber untuk mencoba masuk dan menyusup ke dalam sistem, mencuri data sensitif, atau bahkan mengganggu operasi yang penting. Untuk mengatasi tantangan ini, perusahaan dan pengembang teknologi IoT perlu mengadopsi praktik keamanan yang ketat, mulai dari enkripsi data hingga otentikasi yang kuat untuk setiap perangkat yang terhubung.

Berdasarkan latarbelakang tersebut maka peneliti tertarik untuk melakukan penelitian mengenai Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT).

METODOLOGI

Metode penelitian yang diajukan untuk menganalisis keamanan sistem informasi dalam era Internet of Things (IoT) melibatkan serangkaian langkah sistematis. yaitu, pengumpulan data menjadi titik awal dalam proses ini. Data terkait keamanan sistem informasi dalam konteks IoT akan dikumpulkan dari berbagai sumber, termasuk literatur ilmiah, laporan riset, dan dokumentasi teknis. Langkah selanjutnya adalah analisis literatur yang mendalam, yang melibatkan tinjauan dan sintesis terhadap artikel jurnal, buku, dan publikasi

terkait lainnya untuk memahami tren, temuan, dan pendekatan terbaru (Febriani, 2023). Selain itu, studi kasus tentang implementasi keamanan sistem informasi dalam lingkungan IoT pada beberapa organisasi atau proyek akan dilakukan untuk memberikan wawasan yang lebih mendalam tentang strategi yang digunakan dan hasil yang dicapai. Data yang terkumpul kemudian akan dianalisis secara kualitatif untuk mengidentifikasi pola, tren, dan tema yang muncul, serta untuk mengevaluasi keefektifan berbagai teknik dan metode keamanan yang digunakan. Berdasarkan hasil analisis, solusi-solusi potensial akan diidentifikasi, dan rekomendasi akan disusun untuk meningkatkan keamanan sistem informasi dalam era IoT. Ini mungkin mencakup implementasi alat-alat keamanan yang spesifik, pengembangan kebijakan keamanan, atau investasi dalam teknologi yang lebih aman. Melalui pendekatan ini, diharapkan akan diperoleh pemahaman yang lebih baik tentang tantangan keamanan yang dihadapi dalam lingkungan IoT dan solusi-solusi yang dapat diimplementasikan untuk melindungi infrastruktur informasi yang terhubung secara luas dan kompleks.

HASIL DAN PEMBAHASAN

Analisis keamanan sistem informasi dalam lingkungan Internet of Things (IoT) berhasil mengidentifikasi berbagai jenis ancaman yang mengintai, yang dapat memengaruhi keberlangsungan operasi dan keamanan infrastruktur IoT (Darumaya, 2023). Ancaman-ancaman tersebut mencakup serangan siber seperti malware, ransomware, dan serangan denial of service (DoS), yang masing-masing memiliki dampak dan karakteristik yang unik. Keamanan sistem informasi dalam era Internet of Things (IoT) menjadi semakin kritis seiring dengan berkembangnya konektivitas yang semakin luas dan kompleks (Susanto, 2023). Dalam lingkungan yang terhubung secara digital ini, berbagai perangkat dari berbagai sektor, mulai dari rumah tangga hingga industri, saling berinteraksi dan bertukar data secara terus-menerus. Namun, hal ini juga membuka pintu lebar bagi serangan siber yang dapat mengancam keamanan dan privasi informasi. Ancaman-ancaman seperti malware, ransomware, dan serangan denial of service (DoS) menjadi semakin kompleks dan merusak, mengancam integritas dan ketersediaan sistem IoT (Pardosi, 2024). Tantangan lainnya termasuk kurangnya standar keamanan yang konsisten, kerentanan yang terkait dengan interoperabilitas perangkat, dan kurangnya kesadaran keamanan dari pengguna akhir (Wibowo, 2023). Oleh karena itu, diperlukan upaya yang terkoordinasi dari berbagai pihak, termasuk produsen, penyedia layanan, pengguna akhir, dan regulator, untuk mengembangkan strategi keamanan yang kokoh dan efektif dalam menghadapi ancaman di era IoT ini. Hal ini mencakup penerapan standar keamanan yang kuat, pemantauan lalu lintas jaringan yang terus-menerus, peningkatan kesadaran keamanan pengguna, serta kolaborasi dalam mengatasi tantangan interoperabilitas dan kurangnya standar keamanan yang konsisten. Dengan langkah-langkah ini, diharapkan dapat menciptakan lingkungan IoT yang lebih aman dan andal, menjaga integritas data serta keamanan infrastruktur dalam era yang semakin

terhubung dan canggih ini.

Malware, sebagai ancaman serius bagi sistem Internet of Things (IoT), dapat memiliki konsekuensi yang merugikan dan meresahkan bagi pengguna dan organisasi yang terhubung. Melalui infiltrasi ke dalam perangkat IoT (Aslan, 2020), perangkat lunak berbahaya ini dapat menyebabkan kerugian finansial yang signifikan bagi perusahaan atau individu. Dengan mengambil alih kontrol perangkat, malware dapat memanipulasi fungsi-fungsi utama perangkat IoT, mengganggu operasi normalnya, dan bahkan mengancam keselamatan pengguna. Sebagai contoh, dalam konteks rumah pintar, malware dapat menyebabkan gangguan pada sistem keamanan pintu atau sensor kebakaran, meningkatkan risiko terjadinya intrusi atau kebakaran yang tidak terdeteksi. Selain itu, ancaman malware juga bisa berujung pada pencurian data sensitif. Dengan mengakses informasi yang disimpan di perangkat IoT, seperti data pengguna atau informasi keuangan, penyerang dapat menggunakannya untuk tujuan yang merugikan, seperti pencurian identitas atau penipuan keuangan.

Tentu saja, kerusakan fungsionalitas perangkat IoT juga merupakan hasil yang mungkin dari serangan malware. Perangkat yang terinfeksi dapat mengalami penurunan kinerja atau bahkan kerusakan permanen, yang membutuhkan biaya perbaikan atau penggantian yang signifikan (Kelrey, 2019). Dalam menghadapi ancaman malware ini, penting bagi organisasi dan individu untuk mengambil langkah-langkah pencegahan yang tepat, seperti memperbarui perangkat lunak secara teratur, mengamankan jaringan dengan firewall dan enkripsi, serta membatasi akses perangkat IoT hanya kepada pihak yang berwenang (Susanto, 2023). Dengan tindakan pencegahan yang tepat, dapat mengurangi risiko terhadap serangan malware dan melindungi infrastruktur IoT dari potensi kerusakan dan penyalahgunaan yang merugikan.

Ransomware telah menjadi ancaman yang semakin umum di era Internet of Things (IoT), menghadirkan risiko yang signifikan bagi organisasi dan individu yang terhubung dalam lingkungan yang semakin terhubung (Irawan, 2024). Dalam serangan ransomware, perangkat IoT yang terinfeksi dapat mengalami pengenkripsian data yang penting, yang menghalangi akses pengguna ke informasi atau fungsionalitas perangkat tersebut. Penyerang kemudian meminta tebusan atau pembayaran untuk mengembalikan akses atau memberikan kunci dekripsi yang diperlukan untuk mendapatkan kembali akses ke data yang terkunci.

Serangan Denial of Service (DoS) merupakan ancaman serius bagi ketersediaan layanan dalam lingkungan Internet of Things (IoT) (Najib, 2020). Dalam serangan ini, penyerang mencoba mengganggu ketersediaan layanan dengan membanjiri perangkat atau jaringan dengan permintaan yang tidak sah, sehingga menyebabkan gangguan atau penurunan kinerja yang signifikan. Dalam konteks IoT, serangan DoS dapat memiliki dampak yang luas dan serius. Operasi bisnis, sistem kesehatan, atau infrastruktur kritis lainnya yang terhubung dalam lingkungan IoT rentan terhadap serangan (Anggono, 2023). Misalnya, dalam lingkungan industri, serangan DoS yang berhasil dapat menyebabkan penurunan kinerja pada sistem otomatisasi produksi atau

perangkat IoT yang mengontrol infrastruktur penting. Hal ini dapat mengakibatkan gangguan dalam rantai pasokan, kerugian finansial, dan bahkan risiko kecelakaan atau kegagalan sistem.

Pemahaman yang mendalam tentang berbagai ancaman yang mengintai infrastruktur IoT menjadi kunci dalam pengembangan strategi keamanan yang efektif. Organisasi perlu mengambil langkah-langkah pencegahan yang proaktif untuk melindungi diri dari serangan siber yang semakin kompleks dan merusak (Hoshmand, 2023). Salah satu langkah pencegahan yang penting adalah penerapan perangkat lunak keamanan yang mutakhir, yang dapat membantu mendeteksi, mencegah, dan merespons serangan dengan cepat dan efektif. Tantangan keamanan khusus yang diidentifikasi selama analisis keamanan sistem informasi dalam era Internet of Things (IoT) menjadi perhatian utama untuk diperangi guna memastikan integritas dan keamanan infrastruktur yang semakin terhubung

Kurangnya standar keamanan yang konsisten menjadi tantangan utama dalam menjaga keamanan sistem informasi dalam lingkungan Internet of Things (IoT). Dalam ekosistem IoT yang beragam, dengan banyaknya produsen dan penyedia layanan yang berbeda (Yudistriansyah, 2019), seringkali terdapat keragaman dalam menerapkan standar keamanan. Hal ini mengakibatkan ketidakseragaman dalam implementasi keamanan antar-perangkat, yang pada gilirannya meningkatkan kerentanan sistem terhadap serangan siber. Keragaman ini dapat berasal dari perbedaan dalam pendekatan desain, implementasi perangkat keras dan lunak, serta kebijakan keamanan yang diterapkan oleh produsen IoT. Dalam beberapa kasus, produsen mungkin lebih fokus pada kinerja atau fitur daripada keamanan, menghasilkan perangkat yang rentan terhadap serangan. Selain itu, perbedaan dalam pembaruan perangkat lunak dan dukungan jangka panjang juga dapat menyebabkan perangkat tetap rentan terhadap kerentanan yang telah diketahui.

Kerentanan yang terkait dengan interoperabilitas perangkat merupakan tantangan penting dalam menjaga keamanan sistem informasi dalam lingkungan Internet of Things (IoT). Dalam konteks IoT, di mana berbagai perangkat dari produsen yang berbeda perlu berkomunikasi dan berinteraksi satu sama lain, ketidakcocokan atau kekurangan dalam interoperabilitas dapat menciptakan celah keamanan yang signifikan (Widarti, 2024). Salah satu contoh utama adalah ketika perangkat IoT tidak mampu memvalidasi atau mengenkripsi data yang dikirim atau diterima dari perangkat lain. Ini dapat menyebabkan data sensitif yang diungkapkan atau dipertukarkan melalui jaringan IoT menjadi rentan terhadap pencurian atau manipulasi oleh pihak yang tidak sah. Selain itu, kurangnya standar interoperabilitas yang solid juga dapat membuka jalan bagi serangan seperti spoofing atau man-in-the-middle, di mana penyerang dapat menipu perangkat IoT untuk berkomunikasi dengan perangkat palsu atau mencuri data yang melewati jaringan.

Kurangnya kesadaran keamanan dari pengguna akhir menjadi perhatian serius dalam menjaga keamanan sistem informasi dalam era Internet of Things (IoT). Banyak pengguna akhir tidak menyadari potensi risiko keamanan yang

terkait dengan perangkat IoT yang mereka gunakan, sehingga rentan terhadap serangan siber. Ketidakpahaman tentang praktik keamanan cyber yang baik dapat menyebabkan penggunaan perangkat yang rentan terhadap serangan, memperbesar risiko kerentanan sistem secara keseluruhan (Rosmayati, 2024). Meningkatkan keamanan sistem informasi dalam era Internet of Things (IoT) memerlukan upaya bersama dari berbagai pihak untuk menghadapi tantangan yang kompleks dan berkembang (Yusuf, 2023). Salah satu pendekatan utama adalah dengan mengembangkan standar keamanan yang konsisten dan komprehensif untuk diterapkan secara luas dalam infrastruktur IoT. Hal ini melibatkan kerja sama antara produsen perangkat IoT, penyedia layanan, regulator, dan pemangku kepentingan lainnya untuk merancang dan menerapkan kerangka kerja keamanan yang kokoh. Kesadaran keamanan pengguna akhir juga perlu ditingkatkan melalui pendidikan dan pelatihan yang terarah, sehingga mereka dapat mengidentifikasi dan menghindari potensi risiko keamanan saat menggunakan perangkat IoT. Kolaborasi lintas-sektor juga diperlukan untuk mengatasi tantangan interoperabilitas perangkat dan memastikan bahwa implementasi interoperabilitas dilakukan dengan aman dan terukur (Pinuji, 2021). Dengan langkah-langkah ini, diharapkan dapat menciptakan lingkungan IoT yang lebih aman dan andal, menjaga integritas data serta keamanan infrastruktur dalam era yang semakin terhubung dan kompleks ini.

Pentingnya pendidikan dan kesadaran keamanan di antara pengguna akhir sangatlah penting (Muhtar, 2024). Pengguna perlu diberikan pemahaman yang cukup tentang ancaman keamanan yang mungkin dihadapi saat menggunakan perangkat IoT, serta langkah-langkah yang dapat mereka ambil untuk melindungi diri mereka sendiri dan sistem mereka dari serangan siber. Ini termasuk praktik-praktik seperti menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, membatasi akses ke perangkat IoT hanya untuk pihak yang sah, dan memahami tanda-tanda serangan atau kebocoran keamanan yang mungkin terjadi. Selain itu, penyedia layanan dan produsen perangkat IoT juga memiliki tanggung jawab untuk meningkatkan kesadaran keamanan pengguna akhir. Mereka dapat menyediakan pedoman penggunaan yang jelas dan mudah dimengerti, menyelenggarakan pelatihan keamanan secara teratur, dan mengirimkan pemberitahuan tentang kerentanan keamanan dan pembaruan perangkat lunak yang tersedia kepada pengguna mereka. Dengan meningkatkan kesadaran keamanan di antara pengguna akhir, dapat mengurangi risiko serangan siber terhadap perangkat IoT dan infrastruktur yang terhubung. Ini akan membantu menciptakan lingkungan IoT yang lebih aman dan terjamin bagi semua pengguna, serta memastikan bahwa data dan informasi yang sensitif tetap dilindungi dari ancaman cyber.

KESIMPULAN

Analisis keamanan sistem informasi dalam era Internet of Things (IoT) mengungkapkan kompleksitas dan tantangan yang terkait dengan memastikan integritas dan keamanan infrastruktur yang semakin terhubung.

Ancaman serius seperti malware, ransomware, dan serangan denial of service (DoS) memerlukan pendekatan proaktif dan holistik dalam menghadapinya. Kurangnya standar keamanan yang konsisten, kerentanan interoperabilitas perangkat, dan kurangnya kesadaran keamanan pengguna akhir menjadi fokus utama dalam upaya meningkatkan keamanan dalam lingkungan IoT. Diperlukan kerja sama antara industri, pemerintah, dan pemangku kepentingan lainnya untuk mengembangkan standar keamanan yang kuat, meningkatkan kesadaran keamanan pengguna, dan mengatasi tantangan interoperabilitas. Melalui langkah-langkah ini, diharapkan dapat menciptakan lingkungan IoT yang lebih aman dan terjamin, menjaga integritas data serta keamanan infrastruktur di era yang semakin terhubung dan kompleks.

DAFTAR PUSTAKA

Amane, A. P. O., Sos, S., Febriana, R. W., Kom, S., Kom, M., Artiyasa, I. M., ... & Hut, S. (2023). Pemanfaatan dan Penerapan Internet Of Things (Iot) Di Berbagai Bidang. PT. Sonpedia Publishing Indonesia.

Anggono, S. U., Siswanto, E., & Fajri, L. R. H. A. (2023). User Interface Berbasis Web Pada Perangkat Internet Of Things. Teknik: Jurnal Ilmu Teknik dan Informatika, 3(1), 35-54. https://doi.org/10.51903/teknik.v3i1.326

Antara, K. T. (2024). Pengaruh IoT pada Transformasi Jaringan Multimedia: Literatur Review. Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 7(1), 173-181. https://doi.org/10.55338/jikomsi.v7i1.2736

Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE access, 8, 6249-6271.

Atmaja, R., Rosalina, N., & Wardoyo, A. (2024). Penerapan Teknologi Cerdas Dalam Bidang Industri Jaringan. Jurnal Fakultas Teknik Kuningan, 5(1), 38-42.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. JUSTINFO| Jurnal Sistem Informasi dan Teknologi Informasi, 1(1), 9-20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. Jurnal Keamanan Nasional, 9(2), 299-324. https://ejurnal.ubharajaya.ac.id/index.php/kamnas/article/view/1418

Erwin, E., Datya, A. I., Nurohim, N., Sepriano, S., Waryono, W., Adhicandra, I., ... & Purnawati, N. W. (2023). Pengantar & Penerapan Internet Of Things: Konsep Dasar & Penerapan IoT di berbagai Sektor. PT. Sonpedia Publishing Indonesia.

Febriani, Gri Sella., Sanjiwani, Ni Made Putri Intan., Dewi, I Gusti Ayu Melistyari. Pentingnya Kemampuan Berkomunikasi Secara Efektif Dalam Supervisi Hotel.

Majority Science Journal. Vol. 1, No. 3 (2023). https://doi.org/10.61942/msj.v1i3.25

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. Jurnal Sains dan Teknologi, 5(2), 679-686. https://ejournal.sisfokomtek.org/index.php/saintek/article/view/2347

Irawan, A., Fadholi, W. H. N., Erikamaretha, Z., & Sinlae, F. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. JOURNAL ZETROEM, 6(1), 114-119. https://doi.org/10.36526/ztr.v6i1.3376

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. Cyber Security dan Forensik Digital, 2(2), 77-81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Marine, Y., & Saluky, S. (2018). Penerapan IoT untuk Kota Cerdas. ITEJ (Information Technology Engineering Journals), 3(1), 36-47. https://doi.org/10.24235/itej.v3i1.24

Megawati, S. (2021). Pengembangan sistem teknologi internet of things yang perlu dikembangkan negara indonesia. JIEET (Journal of Information Engineering and Educational Technology), 5(1), 19-26. https://doi.org/10.26740/jieet.v5n1.p19-26

Muhtar, St. Murniati., Amir, Andi Subhan., Amir, Nosakros. Utilizing Social Media For Public Health Advocacy And Awareness In Digital Health Communication. Majority Science Journal (MSJ). Vol. 2No. 1, February 2024. https://doi.org/10.61942/msj.v2i1.96

Mukin, Y. D., & Noviyanti, P. (2023). Simulasi Jaringan Smart Home dengan Sistem Berbasis IoT. Jurnal Komunikasi, Sains dan Teknologi, 2(1), 159-168. https://doi.org/10.61098/jkst.v2i1.34

Najib, W., & Sulistyo, S. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things. Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 9(4), 375-384.

Pardosi, V. B. A., Kom, S., Karim, A., Ti, M., Ilham, R., Kom, M., & Wijaya, A. (2024). Sistem Keamanan Komputer. Cv Rey Media Grafika.

Pinuji, S., Jayanti, N., & Wulandari, M. (2021). Informasi Geospasial Dan Pembangunan Pertanahan Berkelanjutan Dalam Mewujudkan Good Land Governance. Puslitbang ATR/BPN Press.

Prawiyogi, A. G., & Anwar, A. S. (2023). Perkembangan Internet of Things (IoT) pada Sektor Energi: Sistematik Literatur Review. Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 1(2), 187-197. https://doi.org/10.33050/mentari.v1i2.254

Rosmayati, S., & Maulana, A. (2024). Peluang Dan Tantangan Ekonomi Bisnis Dan Kesehatan Di Era Society 5.0. Coopetition: Jurnal Ilmiah Manajemen, 15(1), 113-130. https://doi.org/10.32670/coopetition.v15i1.4124

Santo Gitakarma, M., & Tjahyanti, L. P. A. S. (2022). Peranan Internet of Things dan Kecerdasan Buatan dalam Teknologi Saat Ini. KOMTEKS, 1(1).

Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. Journal of Business And Entrepreneurship, 11(1), 23-33. https://doi.org/10.46273/jobe.v11i1.365

Susanto, E., Prasetya, D. A., Arbatona, I., Marpaung, J. C., & Rahadian, S. H. (2023). Pengamanan objek vital, keamanan File, dan keamanan Cyber pada PT POS indonesia. Jurnal Mutiara Ilmu Akuntansi, 1(3), 163-174. https://doi.org/10.55606/jumia.v1i3.1516

Wibowo, A. (2023). Internet Of Things (Iot) Dalam Ekonomi Dan Bisnis Digital. Penerbit Yayasan Prima Agus Teknik, 1-94.

Widarti, E., Joosten, J., Pratiwi, P. Y., Pradnyana, G. A., Indradewi, I. G. A. A. D., Kamilah, N., & Sepriano, S. (2024). BUKU AJAR PENGANTAR SISTEM INFORMASI. PT. Sonpedia Publishing Indonesia.

Yudistriansyah, A., Suryanegara, M., Gunawan, D., Arifin, A., & Krisnadi, I. (2019). Evaluasi Maturity Level Keamanan dan Rekomendasi Perbaikan Keamanan Internet of Things (IOT) PT XYZ Berdasarkan Kerangka Kerja IOT Security Maturity Model. Universitas Indonesia, 1-2.

Yusuf, M., & Sodik, M. (2023). Penggunaan Teknologi Internet of Things (IoT) dalam Pengelolaan Fasilitas dan Infrastruktur Lembaga Pendidikan Islam. PROPHETIK: Jurnal Kajian Keislaman, 1(2), 65-82. https://doi.org/10.26533/prophetik.v1i2.3233