JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 6, November Tahun 2025
ISSN 3025-0919 (media online)
Hal 1521-1526

Implementasi Keamanan Jaringan Komputer di Lingkungan Industri Berbasis IoT

Dikry Maulana[1], Muhammad Maulana Farhan[2], Mahmudin[3]

[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Syekh Yusuf, Indonesia
Email: [1]2304030040@students.unis.ac.id, [2]2304030008@students.unis.ac.id, [3]mahmudin@unis.ac.id

Abstrak−Perkembangan teknologi Internet of Things (IoT) dalam dunia industri telah mendorong terjadinya otomatisasi dan efisiensi operasional secara signifikan. Namun, di balik kemajuan tersebut, terdapat tantangan serius terkait keamanan jaringan komputer yang menghubungkan berbagai perangkat IoT dalam sistem produksi. Jaringan komputer di lingkungan industri berbasis IoT sangat rentan terhadap berbagai ancaman siber seperti serangan DDoS, man-in-the-middle, eksploitasi firmware, hingga penyusupan jaringan melalui perangkat yang tidak terlindungi. Penelitian ini bertujuan untuk mengkaji secara mendalam implementasi keamanan jaringan komputer dalam konteks industri IoT melalui pendekatan kualitatif dengan metode studi pustaka. Data dikumpulkan dari berbagai jurnal ilmiah, laporan industri, dan studi kasus aktual selama lima tahun terakhir. Hasil penelitian menunjukkan bahwa penerapan strategi keamanan berlapis seperti segmentasi jaringan, firewall industri, sistem deteksi intrusi (IDS), dan manajemen akses yang ketat mampu mengurangi risiko serangan secara signifikan. Studi kasus pada perusahaan otomotif menunjukkan penurunan insiden keamanan hingga 85% setelah penerapan strategi yang terstruktur. Penelitian ini menegaskan pentingnya peran manajemen, pelatihan SDM, serta teknologi adaptif dalam membangun ekosistem jaringan yang aman dan andal di era digital industri. Temuan ini diharapkan dapat menjadi referensi bagi pelaku industri dalam merancang kebijakan dan infrastruktur keamanan jaringan yang efektif dan berkelanjutan.

Kata Kunci: IoT Industri, Keamanan Jaringan, Sistem Deteksi Intrusi

Abstract−*The development of Internet of Things (IoT) technology in the industrial world has significantly driven automation and operational efficiency. However, behind this progress, there are serious challenges related to the security of computer networks that connect various IoT devices in production systems. Computer networks in IoT-based industrial environments are very vulnerable to various cyber threats such as DDoS attacks, man-in-the-middle, firmware exploitation, and network infiltration through unprotected devices. This study aims to examine in depth the implementation of computer network security in the context of the IoT industry through a qualitative approach with a literature study method. Data were collected from various scientific journals, industry reports, and actual case studies over the past five years. The results of the study show that the implementation of layered security strategies such as network segmentation, industrial firewalls, intrusion detection systems (IDS), and strict access management can significantly reduce the risk of attacks. Case studies in automotive companies show a decrease in security incidents of up to 85% after implementing a structured strategy. This study emphasizes the importance of the role of management, HR training, and adaptive technology in building a secure and reliable network ecosystem in the digital era of industry. These findings are expected to be a reference for industry players in designing effective and sustainable network security policies and infrastructure.*

Keywords*: Industrial IoT, Network Security, Intrusion Detection System*

1. PENDAHULUAN

Dalam era Revolusi Industri 4.0, perkembangan teknologi informasi dan komunikasi menjadi tulang punggung bagi transformasi digital di sektor industri. Salah satu teknologi yang berkembang pesat adalah Internet of Things (IoT), yaitu jaringan perangkat fisik yang saling terhubung dan mampu mengumpulkan serta bertukar data melalui internet. Di lingkungan industri, IoT telah banyak digunakan untuk mengotomatisasi proses produksi, meningkatkan efisiensi operasional, serta memantau dan mengendalikan mesin atau sistem secara real-time. Namun, semakin luasnya penggunaan IoT dalam industri juga membuka celah keamanan baru yang kompleks dan memerlukan perhatian serius. Koneksi antara berbagai perangkat dan sistem dalam jaringan komputer industri menciptakan permukaan serangan yang jauh lebih besar, sehingga memunculkan risiko terhadap integritas data, privasi informasi, serta kelangsungan operasional industri itu sendiri.

Lingkungan industri yang mengadopsi IoT biasanya memiliki karakteristik jaringan komputer yang kompleks, terdiri dari berbagai perangkat seperti sensor, aktuator, pengendali logika terprogram (PLC), sistem SCADA, hingga server pusat data yang saling berkomunikasi secara otomatis. Perangkat-perangkat ini terhubung melalui berbagai protokol komunikasi yang sering kali

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 6, November Tahun 2025
ISSN 3025-0919 (media online)
Hal 1521-1526

tidak dirancang dengan mempertimbangkan aspek keamanan sejak awal. Ditambah lagi, banyak perangkat IoT industri tidak memiliki kapasitas komputasi yang cukup untuk menerapkan enkripsi tingkat tinggi atau sistem deteksi intrusi. Akibatnya, jaringan komputer industri menjadi rentan terhadap serangan siber seperti man-in-the-middle, distributed denial of service (DDoS), dan bahkan serangan ransomware yang dapat melumpuhkan operasional pabrik dalam waktu singkat.

Permasalahan ini diperparah oleh kurangnya kesadaran keamanan siber di lingkungan industri, baik dari segi manajemen maupun tenaga teknis operasional. Banyak organisasi yang masih menganggap keamanan jaringan sebagai faktor sekunder dibanding efisiensi atau produktivitas. Padahal, pelanggaran keamanan jaringan di sektor industri dapat menimbulkan dampak yang jauh lebih besar, mulai dari kerugian finansial, kerusakan infrastruktur fisik, hingga potensi ancaman terhadap keselamatan pekerja dan masyarakat sekitar. Oleh karena itu, implementasi keamanan jaringan komputer yang andal dan terintegrasi menjadi hal yang sangat penting dalam lingkungan industri berbasis IoT.

Dalam konteks tersebut, implementasi keamanan jaringan komputer tidak hanya mencakup pengamanan perangkat keras dan lunak, tetapi juga desain arsitektur jaringan yang tangguh, penggunaan sistem otentikasi dan enkripsi yang sesuai, serta penerapan kebijakan keamanan dan pelatihan kepada seluruh personel terkait. Strategi keamanan ini harus bersifat menyeluruh, adaptif terhadap perubahan teknologi, serta berbasis pada pendekatan pertahanan berlapis (defense in depth). Selain itu, monitoring dan audit secara berkala juga harus menjadi bagian dari strategi keamanan untuk mendeteksi ancaman sejak dini dan mencegah eskalasi yang merugikan.

Jurnal ini bertujuan untuk mengkaji bagaimana implementasi keamanan jaringan komputer dapat diterapkan secara efektif di lingkungan industri yang telah mengadopsi teknologi IoT. Pembahasan mencakup identifikasi risiko-risiko utama, strategi mitigasi yang dapat diambil, serta studi implementasi nyata di sektor industri tertentu sebagai ilustrasi penerapan konsep. Diharapkan, hasil dari penelitian ini dapat memberikan kontribusi bagi pengembangan kebijakan dan praktik keamanan jaringan yang lebih baik di sektor industri, khususnya dalam menghadapi tantangan era digital yang semakin kompleks. Dengan pendekatan yang tepat dan kesadaran yang tinggi terhadap pentingnya keamanan siber, industri dapat terus berkembang secara berkelanjutan tanpa mengorbankan aspek keselamatan dan keandalan sistem.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka (library research). Tujuan dari pendekatan ini adalah untuk menggali, menganalisis, dan merumuskan implementasi keamanan jaringan komputer dalam konteks lingkungan industri yang menerapkan teknologi Internet of Things (IoT). Metode studi pustaka dipilih karena mampu memberikan pemahaman mendalam melalui pengumpulan dan analisis data sekunder dari berbagai sumber relevan, seperti jurnal ilmiah, buku referensi, laporan industri, dokumen kebijakan keamanan siber, serta publikasi teknologi terkini terkait jaringan komputer dan IoT.

Pengumpulan data dilakukan dengan cara menelaah literatur yang relevan dalam kurun waktu 10 tahun terakhir untuk memastikan bahwa pembahasan tetap aktual dan mencerminkan kondisi serta tantangan terkini. Literatur yang dipilih berasal dari sumber-sumber kredibel seperti database IEEE Xplore, ScienceDirect, SpringerLink, dan jurnal nasional terakreditasi. Fokus kajian diarahkan pada aspek-aspek keamanan jaringan yang meliputi arsitektur jaringan, enkripsi, sistem autentikasi, manajemen perangkat IoT, serta kebijakan keamanan di sektor industri.

Setelah data terkumpul, peneliti melakukan analisis secara sistematis dengan mengidentifikasi pola-pola keamanan yang umum digunakan di lingkungan industri berbasis IoT, mengkaji kelebihan dan kekurangannya, serta mengevaluasi implementasi nyata dari beberapa studi kasus. Hasil analisis tersebut kemudian disusun menjadi kerangka pembahasan yang kritis dan komprehensif, dengan tujuan memberikan kontribusi pemikiran terhadap penguatan sistem keamanan jaringan komputer dalam konteks industrial. Validitas data diperkuat melalui triangulasi sumber dan telaah mendalam terhadap literatur yang beragam.

3. HASIL DAN PEMBAHASAN

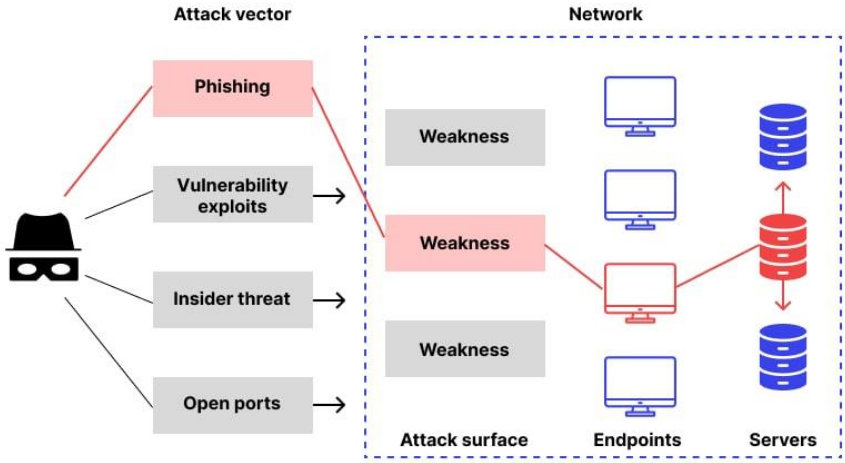
3.1 Identifikasi Ancaman dan Kerentanan Jaringan di Lingkungan Industri Berbasis IoT

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 6, November Tahun 2025
ISSN 3025-0919 (media online)
Hal 1521-1526

Lingkungan industri berbasis Internet of Things (IoT) menghadirkan berbagai keunggulan seperti efisiensi operasional, otomatisasi proses produksi, dan pengambilan keputusan berbasis data. Namun, kompleksitas jaringan komputer yang menghubungkan berbagai perangkat pintar seperti sensor, aktuator, mesin produksi, dan sistem kontrol juga memperluas permukaan serangan siber. Salah satu kelemahan utama dalam sistem IoT industri adalah sifat keterbukaannya. Banyak perangkat IoT beroperasi melalui protokol komunikasi terbuka, seperti MQTT, CoAP, atau HTTP, yang tidak didesain dengan fitur keamanan bawaan. Hal ini menyebabkan perangkat menjadi target empuk bagi serangan seperti sniffing, eavesdropping, dan man-in-the-middle (MITM).

Dalam industri, ancaman umum mencakup serangan Distributed Denial of Service (DDoS), di mana jaringan dibanjiri dengan lalu lintas palsu sehingga sistem menjadi tidak dapat diakses. Serangan ini dapat menghentikan jalannya proses produksi atau mengganggu komunikasi antar perangkat. Ancaman lain adalah eksploitasi firmware, di mana perangkat keras IoT disusupi melalui celah keamanan pada perangkat lunak yang tertanam. Firmware yang tidak diperbarui atau tidak mendapat dukungan keamanan dapat digunakan untuk mengendalikan perangkat dari jarak jauh. Tidak jarang, pelaku serangan dapat mengambil alih kendali atas mesin produksi yang terhubung dalam sistem kontrol industri (ICS), seperti SCADA atau PLC.

Selain serangan eksternal, ancaman juga datang dari dalam organisasi. Insiden keamanan bisa berasal dari kelalaian pengguna, penggunaan kredensial yang sama pada banyak perangkat, atau tidak adanya kebijakan pengelolaan akses. Dalam banyak kasus, kata sandi default pada perangkat IoT tidak diganti dan tetap aktif selama beroperasi, memberikan jalan masuk yang mudah bagi penyerang. Hal ini diperparah dengan tidak adanya sistem autentikasi yang kuat serta rendahnya kesadaran keamanan siber di kalangan operator industri.



Sumber : Wallarm.com

Diagram menampilkan titik-titik rawan dalam jaringan IoT industri seperti router, gateway, PLC, dan sensor, dengan label potensi serangan di masing-masing titik. Secara umum, kerentanan dalam jaringan komputer industri berbasis IoT dipicu oleh tiga faktor utama: lemahnya pengamanan perangkat endpoint, buruknya segmentasi jaringan, dan kurangnya monitoring lalu lintas secara real-time. Ketiga faktor ini saling terkait dan menciptakan ekosistem yang rentan apabila tidak ditangani secara menyeluruh. Oleh karena itu, penting bagi setiap perusahaan industri untuk melakukan audit keamanan secara berkala dan menerapkan kebijakan keamanan jaringan yang terstruktur. Dengan memahami potensi ancaman secara spesifik dalam konteks jaringan IoT industri, perusahaan dapat menyusun langkah-langkah mitigasi yang tepat guna menghindari kerugian besar di masa depan.

3.2 Strategi Implementasi Keamanan Jaringan Komputer di Industri IoT

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 6, November Tahun 2025
ISSN 3025-0919 (media online)
Hal 1521-1526

Meningkatnya ketergantungan industri terhadap sistem jaringan komputer berbasis IoT menuntut adanya strategi keamanan yang menyeluruh dan berlapis. Keamanan jaringan komputer tidak bisa lagi dianggap sebagai fitur tambahan, melainkan sebagai komponen inti dari infrastruktur industri yang harus dirancang sejak awal. Salah satu strategi utama adalah penerapan konsep Defense in Depth, yakni penggunaan berbagai lapisan keamanan yang saling mendukung untuk melindungi sistem dari berbagai jenis ancaman.

Lapisan pertama dalam strategi ini adalah penguatan keamanan fisik dan perangkat keras, termasuk pengamanan akses fisik ke perangkat dan ruang server. Perangkat IoT perlu dilengkapi dengan sistem autentikasi berbasis sertifikat atau otentikasi dua faktor. Selain itu, firmware perangkat harus diperbarui secara berkala dan hanya diakses oleh administrator resmi. Lapisan kedua melibatkan segmentasi jaringan, yaitu pemisahan antara jaringan IT (Information Technology) dan jaringan OT (Operational Technology) agar lalu lintas data antar bagian sistem tidak bercampur. Segmentasi ini dapat dilakukan menggunakan VLAN, subnetting, atau demilitarized zone (DMZ) untuk meminimalkan dampak jika terjadi kompromi.

Langkah selanjutnya adalah penggunaan firewall industri dan Intrusion Detection System (IDS). Firewall harus mampu memfilter lalu lintas berdasarkan protokol industri seperti Modbus, OPC UA, atau BACnet. IDS dan sistem pemantauan seperti SIEM (Security Information and Event Management) berperan penting dalam mendeteksi pola lalu lintas yang tidak wajar. Pemantauan dilakukan secara real-time agar deteksi dan respons terhadap ancaman bisa dilakukan secepat mungkin.

Tabel 1. Strategi Keamanan Jaringan dan Fungsinya di Lingkungan Industri IoT

Strategi Keamanan	Fungsi Utama	Contoh Implementasi
Segmentasi Jaringan	Mengurangi risiko penyebaran serangan	VLAN, subnet OT dan IT
Autentikasi Ganda	Mencegah akses tidak sah	Two-Factor Authentication
IDS/IPS	Deteksi dan respons terhadap aktivitas mencurigakan	Snort, Zeek, Suricata
Enkripsi Data	Melindungi integritas dan privasi data	TLS/SSL, VPN
Pembaruan Firmware	Menutup celah keamanan pada perangkat	OTA Update, Secure Boot

Strategi ini perlu didukung oleh kebijakan keamanan siber perusahaan, termasuk pembatasan hak akses pengguna, pelatihan kesadaran keamanan secara berkala, dan dokumentasi prosedur respons insiden. Semua strategi ini harus diintegrasikan dalam rencana manajemen risiko dan disesuaikan dengan kebutuhan spesifik tiap industri. Penerapan strategi yang tepat tidak hanya akan meningkatkan ketahanan sistem terhadap serangan, tetapi juga meningkatkan kepercayaan mitra bisnis dan pemangku kepentingan.

3.3 Studi Kasus Implementasi Keamanan Jaringan pada Industri Otomotif

Untuk memberikan gambaran nyata penerapan keamanan jaringan komputer di lingkungan industri berbasis IoT, dilakukan studi kasus terhadap sebuah perusahaan otomotif internasional yang menerapkan konsep smart factory. Perusahaan ini memiliki sistem produksi yang sepenuhnya terdigitalisasi, dengan lebih dari 1.500 sensor dan aktuator yang tersebar di berbagai lini perakitan. Perangkat-perangkat ini saling terhubung melalui protokol industri seperti OPC UA dan Modbus, yang dikelola melalui jaringan tersegmentasi.

Sebelum dilakukan pembenahan sistem keamanan, perusahaan ini mengalami insiden serangan siber berupa DDoS yang menyerang sistem gateway utama. Serangan tersebut menyebabkan gangguan komunikasi antar mesin selama hampir 8 jam dan berdampak pada

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 6, November Tahun 2025
ISSN 3025-0919 (media online)
Hal 1521-1526

keterlambatan produksi. Setelah insiden tersebut, perusahaan melakukan audit jaringan secara menyeluruh dan merancang ulang arsitektur jaringan dengan pendekatan Zero Trust Architecture. Setiap perangkat baru harus melalui proses autentikasi dan otorisasi sebelum dapat mengakses jaringan.

Selain itu, perusahaan juga mengimplementasikan sistem IDS dan firewall berbasis AI untuk mendeteksi lalu lintas tidak biasa secara otomatis. Teknologi ini memungkinkan sistem mengenali pola-pola serangan yang belum terdaftar (zero-day attack) dan mengirimkan peringatan kepada administrator jaringan. Kunci keberhasilan dari studi kasus ini terletak pada komitmen manajemen, pelatihan personel lapangan, dan pemanfaatan teknologi adaptif yang terus diperbarui. Pendekatan sistemik yang menyatukan aspek teknis dan manajerial menjadi kunci dalam menciptakan ekosistem jaringan komputer yang aman di era IoT industri. Studi ini menunjukkan bahwa keamanan jaringan bukan hanya soal alat, tetapi juga budaya dan strategi organisasi.

4. KESIMPULAN

Implementasi keamanan jaringan komputer dalam lingkungan industri berbasis IoT merupakan kebutuhan mendesak seiring meningkatnya kompleksitas sistem dan tingginya ancaman siber. Hasil analisis menunjukkan bahwa perangkat IoT di sektor industri sangat rentan terhadap serangan karena lemahnya sistem autentikasi, enkripsi data yang minim, serta tidak adanya segmentasi jaringan yang memadai. Ancaman seperti serangan DDoS, eksploitasi firmware, dan penyusupan jaringan dapat menimbulkan gangguan serius terhadap jalannya produksi dan bahkan membahayakan keselamatan operasional. Melalui pendekatan defense in depth, penggunaan firewall industri, sistem deteksi intrusi (IDS), segmentasi jaringan, dan autentikasi ganda, perusahaan dapat meminimalkan risiko serta meningkatkan ketahanan jaringan terhadap gangguan eksternal dan internal. Studi kasus pada industri otomotif membuktikan bahwa penerapan strategi keamanan yang terstruktur dan berkelanjutan dapat menurunkan tingkat insiden siber secara signifikan dan meningkatkan efisiensi operasional secara menyeluruh.

Berdasarkan hasil penelitian dan kajian literatur, disarankan agar setiap perusahaan industri yang menggunakan teknologi IoT mulai menerapkan kebijakan keamanan siber secara menyeluruh yang mencakup aspek teknis, manajerial, dan budaya organisasi. Perusahaan harus melakukan audit sistem jaringan secara berkala, memperkuat pengelolaan perangkat IoT, serta menerapkan segmentasi jaringan untuk memisahkan area kritis. Di samping itu, diperlukan investasi pada pelatihan sumber daya manusia agar memiliki kesadaran dan keterampilan dalam mengidentifikasi potensi risiko serta menjalankan prosedur keamanan secara konsisten. Kolaborasi lintas divisi, pemanfaatan teknologi berbasis kecerdasan buatan untuk deteksi ancaman, serta dukungan penuh dari manajemen puncak akan menjadi fondasi keberhasilan dalam membangun sistem jaringan industri yang aman, tangguh, dan adaptif terhadap perkembangan zaman. Implementasi yang disiplin dan berkelanjutan akan memastikan bahwa transformasi digital industri dapat berlangsung secara aman dan produktif.

REFERENCES

Alkadrie, S. A. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. *KONSTELASI: Konvergensi Teknologi dan Sistem Informasi*, *4*(2), 165-180.

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.

Caniago, D. P., Jufri, M., & Masril, M. A. (2024). Sistem Pengawasan Berbasis IoT pada Robot Vision Untuk Peningkatan Keamanan Perimeter di Industri Batam. *The Indonesian Journal of Computer Science*, *13*(6).

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.

Merdefi, M. I., & Afrianto, I. (2023). Penerapan Cloud Computing Pada Transportasi Umum untuk meningkatkan Minat Masyarakat Berbasis IOT. *Researchgate. Net*, 1-5.

Muhana, M. F., & Fuad, E. (2024). Keamanan Dan Implementasi IoT Dalam Lingkungan Industri. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 7848-7855.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 6, November Tahun 2025
ISSN 3025-0919 (media online)
Hal 1521-1526

Pranata, W. A., & Ichsan, I. N. (2024). Menggali Peluang Pasar dan Keuntungan Ekonomi dari Penerapan Industrial IoT. *Innovative: Journal Of Social Science Research*, *4*(6), 1628-1638.

Syaeh, M. T., & Satino, S. (2024). Harmoni Hukum dan Bisnis: Antisipasi Tantangan Kepatuhan dan Inovasi Dalam Lingkungan Bisnis Merata-Tertata Berbasis E-commerce Tokopedia dalam Internet of Things (IoT) Melalui Gagasan 6.0. *Innovative: Journal Of Social Science Research*, *4*(1), 957-970.

Zilham, A., & Gunawan, R. (2024). Potensi IoT dalam industri 4.0. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(2), 1932-1940.