Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

Analisis Protokol Keamanan Jaringan dalam Era Internet of Things (IoT)

Fauzan Prasetyo Eka Putra[1] , Muhafiz Khairi[2], Moh. Imam Hidayatullah[3*], Irfan maulana[4]
[1,2,3,4] Program Studi Teknik Informatika, Universitas Madura
*imamhidayat629@gmail.com

Abstrak

Penelitian ini bertujuan untuk menganalisis berbagai tantangan dan solusi yang berkaitan dengan keamanan sistem informasi dalam era Internet of Things (IoT), dengan fokus utama pada penerapan di lingkungan smart home dan industri. Kajian dilakukan melalui pendekatan kualitatif dengan metode studi literatur yang mendalam terhadap berbagai referensi akademik, termasuk jurnal ilmiah, laporan teknis, dan publikasi penelitian. Hasil studi menunjukkan bahwa ancaman siber seperti malware, ransomware, dan serangan denial of service (DoS) memiliki potensi besar dalam mengganggu kinerja dan keandalan sistem IoT. Selain itu, sejumlah persoalan mendasar seperti tidak adanya standar keamanan yang seragam, keterbatasan interoperabilitas antar perangkat dari produsen yang berbeda, serta rendahnya kesadaran dan literasi keamanan di kalangan pengguna menjadi hambatan signifikan. Kontribusi unik dari penelitian ini adalah pemetaan sistematis terhadap isu-isu keamanan utama dalam ekosistem IoT, serta penyusunan rekomendasi strategis yang mencakup penguatan protokol keamanan, pengembangan kebijakan perlindungan data, dan peningkatan edukasi bagi pengguna. Dengan demikian, penelitian ini diharapkan dapat menjadi rujukan dalam pengembangan sistem IoT yang lebih aman, adaptif, dan berkelanjutan di tengah pertumbuhan konektivitas digital yang semakin pesat.

Kata kunci : Keamanan, Sistem Informasi, Internet of Things (IoT), Smart Home, Industri

Abstract

This study explores the challenges and solutions related to information system security in the Internet of Things (IoT) era, focusing on smart homes and industrial settings. Using a qualitative approach through a comprehensive literature review, this research analyzes academic sources including journals, technical reports, and research publications. Findings show that cyber threats such as malware, ransomware, and denial of service (DoS) attacks significantly affect IoT system performance and reliability. Key issues include the absence of standardized security measures, limited device interoperability, and low user awareness. The study contributes by mapping critical security concerns in IoT ecosystems and offering strategic recommendations such as enhancing security protocols, developing data protection policies, and promoting user education. This research aims to support the development of secure, adaptive, and sustainable IoT systems in an increasingly connected digital world.

Keywords : *Security, Information Systems, Internet of Things (IoT), Smart Home, Industry.*

1. Pendahuluan

Di tengah kemajuan teknologi digital, Internet of Things (IoT) telah menjadi fondasi utama dalam perubahan besar di dunia teknologi [1],[2]. Konsep ini berfokus pada integrasi dan konektivitas antar perangkat elektronik, sensor, dan sistem komputer yang terhubung melalui jaringan internet[3][4]. IoT memungkinkan objek yang sebelumnya pasif menjadi lebih cerdas dan berdaya guna[5]. Perangkat-perangkat ini dapat berinteraksi dan bertukar informasi tanpa intervensi manusia secara langsung, sehingga menghadirkan efisiensi baru dalam berbagai aspek kehidupan[6].

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

Salah satu contoh implementasi IoT yang berkembang pesat adalah dalam sistem smart home. Berbagai perangkat seperti lampu, pendingin ruangan, kunci pintar, oven, kulkas, serta sistem keamanan seperti CCTV diintegrasikan melalui jaringan berbasis IoT. Pengguna dapat mengontrol dan memantau perangkat-perangkat tersebut menggunakan aplikasi pada smartphone atau perangkat digital lainnya [7],[8]. Tidak hanya memberi kemudahan, sistem ini juga mampu merespons kondisi lingkungan secara otomatis. Misalnya, ketika sensor mendeteksi gerakan, lampu akan menyala secara otomatis, atau sistem keamanan akan mengirimkan peringatan secara real-time [9],[10],[11]. Bahkan, beberapa perangkat telah dilengkapi kemampuan pembelajaran perilaku pengguna guna menyesuaikan kinerja secara optimal, seperti AC yang menyesuaikan suhu berdasarkan kebiasaan pengguna[12],[13].

Selain di rumah tangga, IoT memainkan peran signifikan dalam sektor industri. Sensor pada mesin dan peralatan kerja memungkinkan pemantauan performa, kondisi operasional, dan variabel produksi secara real-time[14],[15]. Informasi ini diproses untuk mendeteksi anomali, memprediksi kerusakan, serta meningkatkan efisiensi dan produktivitas sistem secara keseluruhan [16],[17]. Melalui pemanfaatan data operasional yang terus diperbarui, perusahaan dapat mengambil keputusan secara cepat, tepat, dan berbasis data, sehingga meningkatkan efisiensi dan stabilitas operasional [18],[19],[20].

Di ranah perkotaan, IoT juga menjadi pilar penting dalam pembangunan smart city. Teknologi ini memungkinkan pengawasan dan pengelolaan berbagai aspek infrastruktur kota seperti transportasi, penerangan jalan, pengelolaan sampah, hingga layanan masyarakat [21]. Dengan memanfaatkan sensor-sensor yang saling terhubung, data dikumpulkan secara real-time untuk mendukung efisiensi penggunaan sumber daya dan peningkatan kualitas pelayanan publik [22].

Namun, keberhasilan implementasi IoT juga diiringi tantangan besar, terutama dari sisi keamanan. Setiap perangkat yang terkoneksi menjadi potensi celah bagi serangan siber seperti pencurian data, peretasan sistem, atau gangguan operasional kritis. Risiko tersebut meningkat seiring dengan jumlah perangkat yang terhubung dan tingkat kompleksitas sistem yang tinggi. Ancaman seperti malware, ransomware, dan denial of service (DoS) semakin sering terjadi dan dapat membahayakan baik individu maupun institusi [7],[23],[24]. Oleh karena itu, perlindungan menyeluruh sangat diperlukan melalui penerapan enkripsi data, sistem autentikasi, dan manajemen akses yang ketat [25],[26],[27].

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

Berangkat dari permasalahan tersebut, penulis terdorong untuk menganalisis keamanan sistem informasi dalam ekosistem IoT. Kajian ini diharapkan dapat memberikan pemahaman mendalam mengenai berbagai tantangan dan potensi solusi guna menciptakan sistem yang lebih aman dan tangguh terhadap ancaman siber di era digital saat ini.

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Sejumlah penelitian sebelumnya telah membahas tantangan dan solusi dalam pengamanan sistem IoT yang relevan dengan kajian ini.

- Gunawan et al. (2024) mengungkapkan bahwa keamanan jaringan merupakan elemen kunci dalam mendukung konektivitas IoT, termasuk pada jaringan 5G yang menghadapi tantangan serius dari serangan siber, sehingga memerlukan pendekatan mitigasi yang sistematis melalui enkripsi dan autentikasi [28].
- Wulan et al. (2024) menegaskan bahwa dalam implementasi IoT berbasis cloud, kelemahan protokol keamanan dapat menyebabkan kebocoran data pengguna. Oleh karena itu, penggunaan enkripsi end-to-end dan kontrol akses menjadi keharusan untuk menjaga privasi data, terutama pada sistem yang menangani informasi sensitif [29].
- Penelitian oleh Syani et al. (2024) menunjukkan bahwa protokol komunikasi IoT yang andal memungkinkan pemantauan fasilitas secara real-time. Meski fokus pada sistem monitoring peternakan, penelitian ini menegaskan pentingnya stabilitas dan keamanan protokol dalam sistem IoT yang bersifat terdistribusi [30].
- Agustiana (2024) menyarankan integrasi teknologi blockchain untuk memperkuat keamanan protokol IoT. Blockchain dinilai mampu menjamin integritas dan transparansi data, serta mengurangi risiko manipulasi dan akses ilegal terhadap jaringan [31].
- Sementara itu, Rusnawati (2022) menyoroti pentingnya kesiapan infrastruktur dan protokol jaringan dalam menunjang transformasi digital berbasis IoT, khususnya dalam konteks pendidikan daring selama masa pandemi. Kesiapan infrastruktur ini menjadi dasar penting untuk menjaga konektivitas dan keamanan sistem secara berkelanjutan [32].

Penelitian-penelitian tersebut menguatkan bahwa isu keamanan IoT sangat luas dan kompleks, mencakup aspek teknis, kelembagaan, serta kesadaran pengguna, sebagaimana juga dibahas dalam artikel ini.

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

2.2. Landasan Teori

1. Internet of Things (IoT)

IoT adalah konsep yang menghubungkan berbagai objek fisik ke dalam jaringan internet, sehingga memungkinkan pertukaran data dan interaksi otomatis tanpa campur tangan manusia secara langsung [1],[4]. Dalam konteks smart home dan industri, IoT berperan penting dalam mengotomatisasi fungsi perangkat serta meningkatkan efisiensi sistem [5],[6],[9].

2. Keamanan Sistem Informasi

Keamanan sistem informasi melibatkan upaya menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dari data dan sistem yang digunakan. Dalam konteks IoT, ancaman seperti malware, ransomware, dan denial of service (DoS) menjadi semakin nyata dan berbahaya [23],[24],[33],[34]. Oleh karena itu, strategi perlindungan seperti enkripsi, autentikasi, serta firewall menjadi sangat krusial [25].

3. Protokol Komunikasi dalam IoT

Berbagai protokol seperti MQTT, CoAP, dan HTTPS digunakan untuk komunikasi antar perangkat IoT. Namun, tidak semua protokol ini dirancang dengan fitur keamanan bawaan, sehingga sering kali dibutuhkan penguatan tambahan seperti sertifikat digital, VPN, atau penggunaan blockchain [28],[29],[31].

4. Interoperabilitas dan Standar Keamanan

Salah satu tantangan utama dalam keamanan IoT adalah kurangnya standar keamanan yang seragam antar perangkat dari produsen berbeda. Ketidakterpaduan ini menciptakan celah keamanan dan memperbesar risiko serangan seperti spoofing atau man-in-the-middle [35],[36],[37],[38].

3. Metode Penelitian

3.1. Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur (library research) untuk mengkaji isu-isu keamanan sistem informasi dalam ekosistem Internet of Things (IoT), khususnya pada implementasi di lingkungan smart home dan industri. Desain ini dipilih karena sesuai untuk menggali pemahaman mendalam dari berbagai sumber ilmiah tanpa melakukan pengumpulan data primer di lapangan.

3.2. Tahapan Penelitian

Penelitian dilakukan melalui beberapa tahapan, yaitu :

1. Identifikasi topik dan perumusan masalah dengan fokus pada protokol keamanan jaringan dalam IoT
2. Pengumpulan data pustaka dari jurnal ilmiah nasional dan internasional, prosiding konferensi, serta laporan teknis yang diperoleh melalui penelusuran daring menggunakan kata kunci seperti “IoT

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

security", "network protocols in IoT", "cyber threat IoT", dan sejenisnya.

3. Seleksi dan klasifikasi sumber berdasarkan kriteria keterkinian (2019–2024), relevansi topik, serta kredibilitas publikasi.
4. Analisis isi dokumen yang mencakup pemetaan jenis ancaman, teknologi dan protokol keamanan, serta strategi perlindungan yang diusulkan dalam literatur.

3.3. Sumber Data dan Lokasi Penelitian

Sumber data dalam penelitian ini adalah data sekunder yang berasal dari dokumen akademik terpercaya dan tersedia secara daring. Karena tidak melibatkan observasi langsung atau eksperimen di lapangan, maka penelitian ini tidak memiliki lokasi fisik spesifik. seluruh proses dilakukan secara daring dan literatur yang digunakan berasal dari berbagai konteks global, sehingga lokasi penelitian bersifat universal.

4. Hasil dan Pembahasan

4.1. Hasil Penelitian

Penelitian ini menggunakan desain kualitatif deskriptif dengan metode studi literatur (library research). Desain ini dipilih karena sesuai untuk mengkaji dan menganalisis berbagai teori, hasil penelitian, serta dokumentasi ilmiah yang relevan dengan isu keamanan sistem informasi pada era Internet of Things (IoT). Tujuan utama dari desain ini adalah untuk memperoleh pemahaman yang mendalam terkait ancaman keamanan, protokol yang digunakan, serta solusi yang ditawarkan oleh para peneliti dalam berbagai konteks penerapan IoT. Desain kualitatif dipilih karena mampu mengungkap makna, kecenderungan, dan pola yang muncul dari berbagai literatur ilmiah. Studi literatur dipilih sebagai metode utama karena topik yang dikaji memerlukan pemetaan teoretis dan konseptual dari berbagai sumber terpercaya, bukan eksperimen langsung atau observasi lapangan.

Prosedur penelitian dilakukan dalam beberapa tahap. Pertama, peneliti melakukan identifikasi topik dan ruang lingkup kajian, yaitu fokus pada protokol keamanan jaringan dalam IoT, khususnya di domain smart home dan industri. Kedua, pengumpulan data dilakukan melalui penelusuran pustaka menggunakan kata kunci tertentu seperti "IoT security", "network protocols in IoT", "malware and ransomware in IoT", dan lainnya. Ketiga, dilakukan seleksi dan klasifikasi artikel atau dokumen berdasarkan kriteria keterkinian (maksimal 5 tahun terakhir), kredibilitas sumber, serta relevansi topik.

Karena penelitian ini berbasis literatur, maka populasi penelitian adalah seluruh dokumen ilmiah terkait keamanan IoT yang tersedia secara publik, sedangkan sampel penelitian adalah artikel dan dokumen yang dipilih berdasarkan kriteria inklusi yang telah ditentukan (tahun terbit, relevansi topik, dan kualitas publikasi). Instrumen

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

penelitian berupa pedoman analisis dokumen, yang memuat aspek-aspek seperti jenis ancaman, protokol keamanan yang digunakan, konteks penerapan, dan rekomendasi dari peneliti sebelumnya.

Tabel 1. Ringkasan ancaman dan masalah keamanan dalam ekosistem IoT

Kategori Ancaman / Isu	Deskripsi Singkat	Dampak Utama	Sumber Referensi
Malware	Perangkat lunak jahat yang menyusup ke system dan merusak fungsi perangkat	Pencurian data, kerusakan sistem, biaya pemulihan	[23],[24],[39]
Ransomware	Enskripsi data oleh penyerang, korban diminta membayar untuk membuka akses	Hilangnya control sistem, kerugian ekonomi	[25],[33],[40]
Denial of Service (DoS)	Serangan yang membanjiri jaringan agar system tidak merespons secara normal	Layanan tidak tersedia, gangguan produksi	[34],[41],[42]
Ketidakterpaduan antar perangkat	Perangkat tidak kompatibel satu sama lain secara protocol atau sistem keamanan	Celah keamanan, risiko spoofing/ MITM	[35],[36],[43]
Rendahnya literasi keamanan	Pengguna tidak menyadari pentingnya pengamanan perangkat	Eksploitasi mudah, lemahnya perlindungan data	[44],[45],[46]

4.2. Pembahasan

Temuan ini memperjelas bahwa keamanan IoT menghadapi tantangan dari berbagai sisi, dimulai dari ancaman teknis hingga persoalan perilaku pengguna. Serangan malware, sebagai contoh, menjadi masalah utama karena sifatnya yang tersembunyi dan mampu mengganggu fungsi perangkat secara langsung[47],[48],[49]. Dalam sistem smart home, malware dapat mengganggu fungsi kunci pintu otomatis, sistem pemanas, bahkan kamera pengawas. Selain kerugian material, serangan ini juga menimbulkan dampak psikologis berupa rasa tidak aman pada pengguna [23],[24],[39].

Dari malware, ancaman berkembang menjadi lebih canggih melalui ransomware. Ransomware tidak sekadar merusak, melainkan mengunci sistem secara total dan menahan akses pengguna terhadap data. Di lingkungan industri, konsekuensinya dapat mencakup terhentinya operasional, kehilangan data penting, hingga kerusakan reputasi perusahaan. Jenis serangan ini menunjukkan bahwa penjahat siber tidak hanya mengandalkan celah teknis, tetapi juga mengeksploitasi kepanikan dan keterbatasan waktu korban untuk bertindak cepat [33],[40].

Serangan denial of service (DoS) menambah kompleksitas risiko. Tidak seperti malware atau ransomware yang menyasar data dan kontrol, DoS menyerang ketersediaan sistem. Dalam sistem IoT yang bergantung pada komunikasi real-time—seperti pada transportasi pintar atau layanan medis—serangan DoS dapat berujung pada kegagalan sistem yang kritis, yang bahkan bisa mengancam keselamatan jiwa [34],[42]. Perlu dicatat bahwa keberhasilan DoS sering kali terjadi pada sistem yang tidak memiliki mekanisme pemantauan lalu lintas jaringan yang

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

andal.

Dari ancaman teknis, permasalahan beralih ke dimensi struktural, yakni ketidakterpaduan antar perangkat IoT. Setiap produsen cenderung menerapkan protokol dan sistem keamanan yang berbeda, yang menyebabkan komunikasi antar perangkat menjadi tidak seragam dan menciptakan banyak titik rawan. Ketiadaan standar universal membuat pengembangan sistem keamanan menyeluruh menjadi sulit dilakukan. Hal ini memperbesar risiko terjadinya serangan seperti spoofing dan man-in-the-middle [35],[36],[43].

Melengkapi tantangan teknis dan struktural, rendahnya literasi keamanan pengguna muncul sebagai masalah yang sering diabaikan[50]. Pengguna sering kali tidak menyadari bahwa tindakan sesederhana mengganti password default atau mengaktifkan autentikasi dua faktor dapat mencegah banyak serangan. Bahkan, sebagian pengguna tidak mengetahui kapan harus melakukan pembaruan perangkat lunak, atau cara mengenali perangkat yang telah terinfeksi [44],[45],[46].

Oleh karena itu, strategi peningkatan keamanan dalam sistem IoT harus mencakup pendekatan multidimensi. Upaya teknis seperti penguatan enkripsi, pemantauan jaringan, serta penggunaan blockchain untuk validasi data memang penting. Namun, aspek edukatif seperti peningkatan literasi pengguna, penyusunan panduan keamanan yang praktis, serta penguatan regulasi juga sangat dibutuhkan [31].

Keseluruhan temuan ini menunjukkan bahwa membangun ekosistem IoT yang aman tidak bisa dilakukan secara parsial. Diperlukan sinergi antara pengembang teknologi, regulator, sektor industri, dan pengguna akhir, agar solusi yang dirancang mampu menjawab ancaman dari berbagai sisi—baik teknis, struktural, maupun sosial. Tanpa kerja sama lintas sektor dan tanpa kesadaran kolektif, sistem IoT akan tetap menjadi target empuk bagi serangan siber di era konektivitas tinggi ini.

5. Kesimpulan

Studi mengenai keamanan sistem informasi di era Internet of Things (IoT) menunjukkan bahwa menjaga stabilitas dan perlindungan infrastruktur digital yang saling terhubung merupakan tantangan besar dan kompleks. Serangan berbahaya seperti malware, ransomware, dan denial of service (DoS) menuntut solusi yang menyeluruh dan tindakan pencegahan yang aktif. Masalah seperti tidak adanya standar keamanan yang seragam, lemahnya interoperabilitas antarperangkat, serta rendahnya tingkat kesadaran keamanan di kalangan pengguna menjadi isu utama yang harus ditangani. Oleh karena itu, kolaborasi antara sektor industri, lembaga pemerintahan, dan para pemangku kepentingan lainnya sangat diperlukan untuk

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

menyusun pedoman keamanan yang kokoh, meningkatkan literasi keamanan siber di tingkat pengguna, dan menyelesaikan persoalan integrasi antarperangkat. Melalui pendekatan terpadu ini, diharapkan tercipta ekosistem IoT yang lebih terlindungi dan andal, sehingga dapat menjaga keamanan data dan keberlangsungan sistem di tengah pertumbuhan konektivitas yang pesat dan kompleks.yang sudah dilakukan.

6. Daftar Pustaka

[1]. S. Megawati dan A. Lawi, "Pengembangan Sistem Teknologi Internet of Things Yang Perlu Dikembangkan Negara Indonesia," *JIIET (Journal of Information Engineering and Educational Technology)*, vol. 5, no. 1, hlm. 19–26, 2021, doi: https://doi.org/10.26740/jieet.v5n1.p19-26.

[2]. N. Kristianti, "Pengaruh Internet Of Things (Iot) Pada Education Business Model : Studi Kasus Universitas Atma Jaya Yogyakarta," *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, vol. 13, no. 2, hlm. 47–53, 2019, doi: https://doi.org/10.47111/jti.v13i2.254.

[3]. F. P. E. Putra, Ubaidi, Holipah, Moch. , A. Mahmud, dan R. Paradina, "Comparing the Performance of LoRaWAN and MQTT Protocols for IoT Sensor Networks," *Journal of Information and Technology*, vol. 6, no. 2, hlm. 221–228, 2024, doi: 10.60083/jidt.v6i2.565.

[4]. K. T. Antara, "Pengaruh IoT pada Transformasi Jaringan Multimedia: Literatur Review," *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI*, vol. 7, no. 1, hlm. 173–181, 2024, doi: https://doi.org/10.55338/jikomsi.v7i1.2736.

[5]. L. Maulana, A. Kusyanti, dan F. A. Bakhtiar, "Implementasi Metode Autentikasi dengan Zero Knowledge Proof menggunakan Protokol Feige-Fiat-Shamir Identification Scheme pada Perangkat Internet of Things," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 9, hlm. 8937–8945, 2019, doi: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6311.

[6]. B. W. Aulia, M. Rizki, P. Prindiyana, dan S. Surgana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi*, vol. 1, no. 1, hlm. 9–20, Des 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.

[7]. E. M. P. Siagian, J. Siregar, dan R. H. Siahaan, "Analisis Keamanan Pada Sistem Internet Of Things Untuk Pengendalian Perangkat Elektronik Rumah Tangga," *Jurnal Teknologi Informasi dan Industri*, vol. 4, no. 1, hlm. 45–53, 2023.

[8]. F. P. E. Putra, M. , A. Mahmud, dan I. S. Maqom, "Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus," *Digital Transformation Technology (Digitech)*, vol. 3, no. 2, hlm. 996–1001, 2023, doi: 10.47709/digitech.v3i2.3457.

[9]. Y. B. Widodo, A. M. Ichsan, dan T. Sutabri, "Perancangan Sistem Smart Home Dengan Konsep Internet Of Things Hybrid Berbasis Protokol Message Queuing Telemetry Transport," *Jurnal Teknologi Informatika dan Komputer MH Thamrin*, vol. 6, no. 2, hlm. 123–136, 2020, doi: http://journal.thamrin.ac.id/index.php/jtik/issue/view/31.

[10]. Y. Duhin Mukin, "Simulasi Jaringan Smart Home dengan Sistem Berbasis IoT," *Jurnal Komunikasi Sains dan Teknologi*, vol. 2, no. 1, hlm. 63–72, 2023, doi: https://doi.org/10.61098/jkst.v2i1.34.

[11]. Wilianto dan A. Kurniawan, "Sejarah, Cara Kerja Dan Manfaat Internet Of Things," *JURNAL MATRIX*, vol. 8, no. 2, hlm. 36–41,

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

2018, doi: https://dx.doi.org/10.31940/matrix.v8i2.818

[12]. M. F. Zulkarnaen, Aliy Nauval Hanafi, dan Mohammad Taufan Asri Zaen, "Rekayasa SmartHome System Berbasis Internet of Things," *Infotek: Jurnal Informatika dan Teknologi*, vol. 7, no. 2, hlm. 552–562, Jul 2024, doi: 10.29408/jit.v7i2.26545.

[13]. Kartarina, M. Madani, dan M. N. Dwitama, "Prototyping Pengendalian Keamanan Ruangan Berbasis Internet of Things (IoT) Menggunakan NodeMCU V3 (Prototyping Controlling Rooms Security Internet of Things (IoT) Using NodeMCU V3)," *JTIM : Jurnal Teknologi Informasi dan Multimedia*, vol. 3, no. 3, hlm. 138–143, 2021, doi: https://doi.org/10.35746/jtim.v3i3.153.

[14]. M. I. KURNIAWAN, U. SUNARYA, dan R. TULLOH, "Internet of Things : Sistem Keamanan Rumah berbasis Raspberry Pi dan Telegram Messenger," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, vol. 6, no. 1, hlm. 1–15, Apr 2018, doi: 10.26760/elkomika.v6i1.1.

[15]. I. Gunawan dan H. Ahmadi, "Kajian Dan Rancang Bangun Alat Pakan Ikan Otomatis (Smart Feeder) Pada Kolam Budidaya Ikan Berbasis Internet Of Things," *Infotek: Jurnal Informatika dan Teknologi*, vol. 7, no. 1, hlm. 40–51, Jan 2024, doi: 10.29408/jit.v7i1.23523.

[16]. A. Zein dan E. S. Eriana, "Perancangan Internet Of Things (IOT) Smart Home," *Sainstech*, vol. 31, no. 2, hlm. 48–53, 2021, doi: https://doi.org/10.37277/stch.v31i2.1156.

[17]. Anggy Giri Prawiyogi dan Aang Solahudin Anwar, "Perkembangan Internet of Things (IoT) pada Sektor Energi : Sistematik Literatur Review," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, hlm. 187–197, Jan 2023, doi: 10.34306/mentari.v1i2.254.

[18]. E. Susanto, Lady Antira, K. Kevin, E. Stanzah, dan A. A. Majid, "Manajemen Keamanan Cyber di Era Digital," *Journal of Business and Entrepreneurship*, vol. 11, no. 1, hlm. 23–33, 2023, doi: 10.46273/job&e.v11i1.365.

[19]. M. O. Hoshmand dan S. Ratnawati, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *Jurnal Sains dan Teknologi*, vol. 5, no. 2, hlm. 679–686, 2023, doi: https://ejournal.sisfokomtek.org/index.php/saintek/article/view/2347.

[20]. Atmaja Rafli, Rosalina Nela, dan Wardoyo Andika, "Penerapan Teknologi Cerdas Dalam Bidang Industri Jaringan," *Jurnal Fakultas Teknik Kuningan*, vol. 5, no. 1, hlm. 38–42, 2024, doi: https://doi.org/10.70476/jft.v5i1.007.

[21]. Y. Marine, E. Sukses, S. Devisi, P. Sistem, dan C. Y. C. Id Saluky, "Penerapan IoT untuk Kota Cerdas," *ITEJ (Information Technology Engineering Journals)*, vol. 3, no. 1, hlm. 36–47, 2018, doi: https://doi.org/10.24235/itej.v3i1.24.

[22]. M. Yusuf, M. Sodik, S. Darussalam, dan K. Nganjuk, "Penggunaan Teknologi Internet Of Things (IOT) Dalam Pengelolaan Fasilitas Dan Infrastruktur Lembaga Pendidikan Islam," *PROHEPTIK*, vol. 1, no. 2, hlm. 65–82, 2023, doi: https://doi.org/10.26533/prophetik.v1i2.3233.

[23]. Ömer Aslan Aslan dan Refik Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, hlm. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[24]. S. Afdilah, N. S. Agustina, I. Hani, dan I. Gunawan, "Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna," *JOURNAL SHIFT*, vol. 4, no. 2, hlm. 47–62, 2024, doi: https://doi.org/10.24252/shift.v4i2.142.

[25]. E. Susanto, D. Adika Prasetya, I. Arbatona, J. Christian Marpaung, dan S. Hikmatyar

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

Rahadian, "Pengamanan Objek Vital, Keamanan File, Dan Keamanan Cyber Pada Pt Pos Indonesia," *Jurnal Mutiara Ilmu Akuntansi (JUMIA)*, vol. 1, no. 3, hlm. 163–174, 2023, doi: https://doi.org/10.55606/jumia.v1i3.1516.

[26]. S. Ghildiyal, A. K. Mishra, A. Gupta, dan N. Garg, "Analysis of Denial of Service (DOS) Attacks in Wireless Sensor Networks," *IJRET : Internet Journal of Reasearch in Engineering and Technology*, vol. 3, no. 10, hlm. 140–143, 2014.

[27]. R. Roman, J. Zhou, dan J. Lopez, "On The Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Network Journal*, vol. 57, no. 10, hlm. 2266–2279, 2013, doi: https://doi.org/10.1016/j.comnet.2012.12.018.

[28]. S. Gunawan, A. A. R. Santosa, dan E. M. S. Sakti, "Analisis Keamanan Jaringan 5G: Ancaman dan Upaya Mitigasi," *TEKINFO*, vol. 22, no. 2, hlm. 54–62, Okt 2024, doi: 10.37817/tekinfo.v25i2.

[29]. Wulan *dkk.*, "Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis," *Jurnal Kewirausahaan dan Multi Talenta (JKMT)*, vol. 2, no. 2, hlm. 126–137, 2024, doi: 10.38035/jkmt.v2i2.

[30]. M. Syani, E. A. Firdaus, dan D. Mulyana, "Design a Chicken Coop Monitoring System Based on the Internet of Things," *NUANSA INFORMATIKA*, vol. 18, no. 1, hlm. 106–114, 2024, doi: https://doi.org/10.25134/ilkom.v18i1.64.

[31]. U. Z. Agustiana, "Pemanfaatan Blockchain untuk Meningkatkan Keamanan Siber dalam Pembayaran Lintas Batas di Industri Fintech," *Jurnal Bisnis, Ekonomi Syariah, dan Pajak*, vol. 1, no. 4, hlm. 206–215, 2024, doi: 10.61132/jbep.v1i4.738.

[32]. R. D. Rusnawati dan R. T. S. Hariyati, "Implementasi Internet Of Things Pada Layanan Kesehatan (Literature Review)," *Jorunal of Innovation Reasearch and Knowledge*, vol. 1, no. 8, hlm. 569–574, 2022, doi: https://doi.org/10.53625/jirk.v1i8.1082.

[33]. A. Irawan, W. Hamzah, N. Fadholi, Z. Erikamaretha, F. Sinlae, dan P. S. Informatika, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT," *JOURNAL ZETROEM*, vol. 6, no. 1, 2024, doi: https://doi.org/10.36526/ztr.v6i1.3376.

[34]. W. Najib, T. Ancaman dan Solusi Keamanan, S. Sulistyo, dan K. Kunci, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology)," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* |, vol. 9, no. 4, hlm. 375–384, 2020, doi: https://doi.org/10.22146/jnteti.v9i4.539.

[35]. F. P. E. Putra, H. Amir, W. Agel, dan R. , O. F. Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, no. 4, hlm. 82–87, Jan 2024, doi: 10.60083/jsisfotek.v5i4.329.

[36]. P. E. A. Kaunang, S. R. U. A. Sompie, dan A. S. M. Lumenta, "Implementasi Google Internet of Things Core pada Monitoring Volume Ban Angin Mobil," *Jurnal Teknik Elektro dan Komputer*, vol. 9, no. 3, hlm. 163–170, 2020, doi: https://doi.org/10.35793/jtek.v9i3.30131.

[37]. C. Qiang, G. Quang, B. Yu, dan L. Yang, "Research on Security Issues oof the Internet of Things," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 6, hlm. 1–10, 2013, doi: http://dx.doi.org/10.14257/ijfgcn.2013.6.6.01.

[38]. E. D. Meutia, "Internet of Things - Keamanan dan Privasi," *Seminar Nasional dan Expo Teknik Elektro 2015*, vol. 1, no. 1, hlm. 85–89, 2015.

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal. 356-366

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30257 Link : https://dx.doi.org/10.29408/jit.v8i2.30257

[39]. A. Esmaeily dan K. Kralevska, "Orchestrating Isolated Network Slices in 5G Networks," *Electronics (Switzerland)*, vol. 13, no. 8, Apr 2024, doi: 10.3390/electronics13081548.

[40]. A. R. Kelrey dan A. Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," *CyberSecurity dan Forensik Digital*, vol. 2, no. 2, hlm. 77–81, 2019, doi: https://doi.org/10.14421/csecurity.2019.2.2.1625.

[41]. S. Umar Anggono, E. Siswanto, dan L. Rajendra Haidar Azani Fajri, "User Interface Berbasis Web Pada Perangkat Internet Of Things," *JURNAL ILMU TEKNIK DAN INFORMATIKA (TEKNIK)*, vol. 3, no. 1, hlm. 35–54, 2023, doi: https://doi.org/10.51903/teknik.v3i1.326.

[42]. A. Ali *dkk.*, "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," *Sensors*, vol. 22, no. 2, Jan 2022, doi: 10.3390/s22020572.

[43]. K. A. Nugraha, "JEPIN (Jurnal Edukasi dan Penelitian Informatika) Efisiensi Pertukaran Data Client-Server menggunakan Web Socket pada Perangkat Berbasis Internet of Things," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 10, no. 1, hlm. 33–39, 2024, doi: https://dx.doi.org/10.26418/jp.v10i1.73145.

[44]. Rosmayati Siti dan Maulana Arman, "Peluang Dan Tantangan Ekonomi Bisnis Dan Kesehatan Di Era Society 5.0 ," *Coopetition Jurnal Ilmiah Manajemen*, vol. 15, no. 1, hlm. 113–130, Mar 2024, doi: https://dx.doi.org/10.32670/coopetition.v15i1.4124.

[45]. St. M. Muhtar, A. S. Amir, dan N. Arya, "Utilizing Social Media For Public Health Advocacy And Awareness In Digital Health Communication," *Prosiding Webinar Nasional IAHN-TP Palangka Raya*, no. 3, hlm. 195–202, Feb 2024, doi: 10.61942/msj.v2i1.96.

[46]. F. P. E. Putra, A. B. Tamam, R. W. Efendi, dan M. , Z. Mun'im, "Pertahanan Tingkat Server Terhadap Serangan Dns Spoofing Di Jaringan Modern," *Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, vol. 14, no. 2, hlm. 139–149, 2024, doi: https://doi.org/10.24853/justit.14.2.139-149.

[47]. F. P. E. Putra, S. M. Dewi, Maugfiroh, dan A. Hamzah, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, no. 2, hlm. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.

[48]. F. P. E. Putra, Ubaidi, A. Zulfikri, G. Arifin, dan R. M. Ilhamsyah, "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, hlm. 413–421, Agu 2024, doi: 10.47709/brilliance.v4i1.4357.

[49]. F. P. E. Putra, Ubaidi, S. A. A. Sugi, K. Mufidah, dan Y. R. Febriani, "Analysis of Cyber Attacks on Network Security," *Jurnal Informasi dan Teknologi*, vol. 6, no. 2, hlm. 204–208, 2024, doi: https://doi.org/10.60083/jidt.v6i2.569.

[50]. D. Kim, N. Kim, dan J. Ahn, "Systematic Security Guideline Framework through Intelligently Automated Vulnerability Analysis," *Computers, Materials and Continua*, vol. 78, no. 3, hlm. 3867–3889, 2024, doi: 10.32604/cmc.2024.046871