KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.5 Oktober 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 1466-1472
DOI: https://doi.org/10.61722/jipm.v4i5.3078

Kajian Literatur Keamanan Data End-to-End pada Sistem Internet of Things Berbasis Cloud

Adinda Aliya Maharani[1]*, Yulindon[2]
[1],[2] Sarjana Terapan Teknik Telekomunikasi, Politeknik Negeri Padang, Padang, Sumatera Barat, Indonesia
[1]adindaaliyamaharani@gmail.com

Abstrak Integrasi Internet of Things (IoT) dengan cloud computing meningkatkan kapasitas penyimpanan, pemrosesan, dan analisis data, tetapi juga memperluas permukaan serangan karena data melewati perangkat, jaringan, gateway, broker, antarmuka layanan, dan infrastruktur cloud. Perlindungan kanal seperti Transport Layer Security (TLS) dapat mengamankan komunikasi pada setiap hop, namun tidak selalu mempertahankan kerahasiaan payload ketika koneksi diterminasi pada komponen perantara. Penelitian ini bertujuan menganalisis pendekatan keamanan data end-to-end pada sistem IoT berbasis cloud melalui kajian literatur terstruktur. Literatur peer-reviewed periode 2020–Agustus 2026 diseleksi berdasarkan relevansi terhadap ancaman, enkripsi dan integritas, autentikasi, manajemen kunci, kontrol akses, cakupan perlindungan payload, serta overhead implementasi. Dua belas studi substantif digunakan sebagai dasar sintesis komparatif dan tematik. Hasil kajian menunjukkan bahwa perlindungan pada tingkat payload dapat melengkapi TLS, terutama pada arsitektur publish–subscribe ketika broker tidak seharusnya memperoleh plaintext. Pendekatan yang paling menonjol mencakup lightweight authenticated encryption, lightweight block cipher, dan conditional proxy re-encryption. Tantangan utama meliputi overhead komputasi dan komunikasi, kompleksitas siklus hidup kunci, skalabilitas, serta keterbatasan sumber daya perangkat. Kajian ini menegaskan pentingnya membedakan perlindungan end-to-end dari hop-by-hop dan mengusulkan kerangka evaluasi yang menghubungkan ancaman, mekanisme keamanan, cakupan E2E, dan biaya implementasi.
Kata Kunci: Internet of Things, cloud computing, end-to-end security, MQTT, lightweight cryptography.

Abstract The integration of the Internet of Things (IoT) with cloud computing improves data storage, processing, and analytics, but it also expands the attack surface because data traverses devices, networks, gateways, brokers, service interfaces, and cloud infrastructure. Channel protection such as Transport Layer Security (TLS) can secure individual communication hops, yet it does not always preserve payload confidentiality when connections are terminated at intermediary components. This study analyzes end-to-end data security approaches for cloud-based IoT systems through a structured literature review. Peer-reviewed studies published from 2020 to August 2026 were selected based on their relevance to threats, encryption and integrity, authentication, key management, access control, payload-protection coverage, and implementation overhead. Twelve substantive studies formed the basis of comparative and thematic synthesis. The findings indicate that payload-level protection can complement TLS, particularly in publish–subscribe architectures where brokers should not obtain plaintext. Prominent approaches include lightweight authenticated encryption, lightweight block ciphers, and conditional proxy re-encryption. Major challenges involve computational and communication overhead, key-lifecycle complexity, scalability, and constrained IoT resources. The review highlights the need to distinguish end-to-end protection from hop-by-hop protection and proposes an evaluation framework linking threats, security mechanisms, E2E coverage, and implementation cost.
Keywords: Internet of Things, cloud computing, end-to-end security, MQTT, lightweight cryptography.

1. Pendahuluan

Internet of Things (IoT) menghubungkan sensor, aktuator, perangkat komputasi, dan layanan digital untuk menghasilkan serta mempertukarkan data melalui jaringan. Keterbatasan penyimpanan dan komputasi pada perangkat mendorong integrasi dengan cloud computing karena cloud menyediakan sumber daya yang elastis untuk penyimpanan, pemrosesan, dan analitik. Di sisi lain, integrasi tersebut membuat aliran data melibatkan lebih banyak komponen—perangkat, jaringan, gateway, broker, API, dan layanan cloud—sehingga memperluas permukaan

Naskah Masuk: 06 Agustus 2026; Revisi: 07 Agustus 2026; Diterima: 08 Agustus 2026; ; Terbit: 21 Agustus 2026

serangan dan ketergantungan pada infrastruktur pihak ketiga (Almutairi & Sheldon, 2025; Singh et al., 2025).

Data IoT dapat bersifat sensitif pada aplikasi kesehatan, industri, transportasi, pertanian cerdas, dan smart home. Sepanjang perjalanan menuju cloud, data berpotensi mengalami eavesdropping, man-in-the-middle, spoofing, replay attack, manipulasi pesan, akses tanpa otorisasi, kebocoran, serta penyalahgunaan kredensial. Karena itu, keamanan IoT–cloud perlu mempertahankan confidentiality, integrity, authentication, authorization, availability, dan privacy pada seluruh siklus hidup data, bukan hanya pada satu segmen komunikasi (Tawalbeh et al., 2020; Yang, 2022).

Masalah tersebut menjadi penting pada arsitektur publish–subscribe seperti Message Queuing Telemetry Transport (MQTT). TLS efektif melindungi kanal komunikasi, tetapi terminasi TLS pada broker atau gateway dapat membuat payload tersedia dalam plaintext pada komponen perantara. Diro et al. (2020) menunjukkan relevansi authenticated encryption yang ringan untuk komunikasi publish–subscribe, sedangkan Winarno dan Sari (2022) mengembangkan skema komunikasi MQTT end-to-end berbasis lightweight block cipher. Pada skenario distribusi pesan, Lin et al. (2024) menggunakan conditional proxy re-encryption agar intermediary dapat membantu distribusi tanpa harus memperoleh plaintext.

End-to-end encryption (E2EE) karena itu tidak cukup dipahami sebagai pemilihan algoritma enkripsi. Efektivitasnya bergantung pada posisi enkripsi dan dekripsi, autentikasi endpoint, pembangkitan dan distribusi kunci, rotasi dan pencabutan kunci, serta hubungan kontrol akses dengan kepemilikan kunci. Tantangannya meningkat pada perangkat IoT yang memiliki keterbatasan prosesor, memori, energi, dan bandwidth karena operasi kriptografi dapat menambah latency, ukuran pesan, konsumsi CPU/memori, serta energi (Diro et al., 2020; Alotaibi et al., 2025).

Kajian terdahulu telah membahas keamanan IoT–cloud secara luas (Almutairi & Sheldon, 2025; Singh et al., 2025), keamanan dan privasi IoT (Tawalbeh et al., 2020; Kaur et al., 2024), autentikasi (Alotaibi et al., 2025), dan kontrol akses (Iqal et al., 2024). Namun, pembahasan yang membedakan secara eksplisit apakah payload tetap terlindungi hingga endpoint tujuan masih tersebar pada studi dengan fokus dan metrik yang berbeda. Penelitian ini karena itu menyintesis literatur menggunakan enam dimensi: ancaman, enkripsi dan integritas, autentikasi, manajemen kunci dan kontrol akses, cakupan perlindungan end-to-end, serta overhead implementasi. Kontribusi utama kajian adalah kerangka pembeda antara E2E, hop-by-hop, partial E2E, dan cakupan yang tidak dapat ditentukan, sehingga istilah secure communication tidak otomatis disamakan dengan E2EE.

2. Kajian Teoritis

2.1 IoT Berbasis Cloud dan Keamanan Data

IoT berbasis cloud memindahkan sebagian fungsi penyimpanan, pemrosesan, dan analitik dari perangkat ke infrastruktur yang lebih elastis. Konsekuensinya, perlindungan data harus mencakup endpoint, komunikasi, gateway/broker, API, serta layanan cloud. Ancaman pada tiap lapisan berbeda, sehingga satu mekanisme keamanan tidak cukup untuk menjamin seluruh properti keamanan (Almutairi & Sheldon, 2025; Singh et al., 2025).

2.2 End-to-End Security dan Hop-by-Hop Security

End-to-end security mempertahankan perlindungan payload dari sumber sampai endpoint tujuan. Pada E2EE, data diproteksi sebelum meninggalkan sumber dan hanya dapat dipulihkan oleh penerima yang memiliki hak kriptografis. Sebaliknya, hop-by-hop security melindungi setiap segmen komunikasi tetapi memungkinkan intermediary menjadi titik terminasi. Dengan demikian, penggunaan TLS tidak dapat langsung dikategorikan sebagai E2EE apabila broker atau gateway masih memperoleh plaintext.

2.3 Kriptografi, Autentikasi, Manajemen Kunci, dan Kontrol Akses

Kriptografi simetris dan authenticated encryption banyak digunakan untuk payload karena efisien, sedangkan kriptografi asimetris berperan pada autentikasi, pertukaran kunci, dan distribusi kepercayaan. Pada IoT, pemilihan mekanisme harus memperhatikan keterbatasan sumber daya (Diro et al., 2020; Winarno & Sari, 2022). Autentikasi memastikan endpoint sah, sedangkan manajemen kunci mencakup pembangkitan, distribusi, penyimpanan, rotasi, dan pencabutan. Kontrol akses menentukan pihak yang berhak menggunakan data atau layanan; pada E2EE, hak tersebut idealnya terkait dengan kepemilikan kunci, bukan sekadar izin mengakses broker atau cloud (Alotaibi et al., 2025; Iqal et al., 2024).

2.4 Kerangka Analisis

Kajian membandingkan setiap studi berdasarkan konteks IoT, arsitektur/protokol, ancaman, mekanisme keamanan, autentikasi, manajemen kunci, kontrol akses, security properties, cakupan perlindungan E2E, lingkungan implementasi, dan overhead. Cakupan perlindungan diklasifikasikan sebagai E2E, hop-by-hop, partial E2E, atau unclear. Kerangka ini digunakan untuk menilai apakah mekanisme benar-benar mengurangi paparan plaintext terhadap intermediary.

3. Metode Penelitian

3.1 Desain Penelitian

Penelitian menggunakan kajian literatur terstruktur (structured literature review) untuk mengidentifikasi, membandingkan, dan menyintesis penelitian tentang keamanan data end-to-end pada sistem IoT berbasis cloud. Pendekatan terstruktur dipilih agar proses penentuan fokus, kriteria literatur, ekstraksi, dan sintesis dapat dijelaskan secara transparan tanpa mengklaim meta-analisis kuantitatif pada studi yang sangat heterogen (Snyder, 2019).

3.2 Pertanyaan Penelitian

Tabel 1. Pertanyaan penelitian

Kode	Research Question
RQ1	Apa ancaman dan kerentanan utama terhadap keamanan data end-to-end pada sistem IoT berbasis cloud?
RQ2	Mekanisme keamanan apa yang digunakan untuk melindungi data IoT secara end-to-end?
RQ3	Teknologi, algoritma kriptografi, protokol, dan arsitektur apa yang digunakan?
RQ4	Bagaimana efektivitas mekanisme dievaluasi dari aspek keamanan dan overhead implementasi?
RQ5	Apa kelebihan, keterbatasan, trade-off, dan kesenjangan penelitian yang masih terbuka?

3.3 Sumber Literatur dan Strategi Pencarian

Literatur difokuskan pada artikel peer-reviewed periode Januari 2020–Agustus 2026 yang relevan dengan IoT–cloud dan perlindungan data. Penelusuran diarahkan pada sumber yang terindeks atau tersedia melalui Scopus, Web of Science Core Collection, IEEE Xplore, ScienceDirect, SpringerLink, serta laman penerbit ilmiah. String utama yang digunakan adalah: ("Internet of Things" OR IoT OR IIoT) AND ("cloud computing" OR "cloud-based" OR "cloud IoT" OR "IoT-cloud") AND ("end-to-end security" OR "end-to-end encryption" OR "data security" OR "secure communication" OR encryption OR authentication OR "key management" OR "access control"). Penelusuran sitasi maju dan mundur digunakan untuk menemukan studi relevan tambahan.

3.4 Kriteria Seleksi Literatur

Tabel 2. Kriteria inklusi dan eksklusi

Kriteria	Inklusi	Eksklusi
Periode	Januari 2020–Agustus 2026	Di luar periode
Jenis	Artikel peer-reviewed	Editorial, poster, atau sumber non-peer-reviewed
Konteks	IoT terintegrasi cloud atau perangkat–gateway/broker–cloud	Tidak berkaitan dengan IoT–cloud
Fokus	Keamanan data, E2E, enkripsi, autentikasi, key management, access control, privacy	Hanya deteksi intrusi tanpa kaitan perlindungan data
Ketersediaan	Full text dan hasil/metode dapat dianalisis	Full text atau informasi teknis tidak memadai
Duplikasi	Satu rekaman unik per studi	Duplikat berdasarkan DOI/judul/penulis/tahun

Berdasarkan kriteria tersebut, 12 studi substantif digunakan sebagai dasar sintesis utama. Referensi metodologis digunakan terpisah untuk mendukung rancangan kajian. Karena rekaman pencarian awal dan log deduplikasi tidak disajikan sebagai dataset audit dalam naskah ini, penelitian tidak melaporkan angka PRISMA yang tidak dapat diverifikasi.

3.5 Evaluasi Kualitas dan Ekstraksi Data

Kualitas bukti dievaluasi secara kualitatif berdasarkan kejelasan tujuan, deskripsi arsitektur IoT–cloud, rincian mekanisme keamanan, metode evaluasi, pelaporan hasil keamanan/kinerja, serta keterbatasan penelitian. Data yang diekstraksi mencakup fokus studi, arsitektur/protokol, mekanisme, cakupan E2E, security properties, autentikasi, manajemen kunci, kontrol akses, dan indikator overhead. Sintesis dilakukan secara deskriptif, komparatif, dan tematik; meta-analisis tidak dilakukan karena perbedaan perangkat, algoritma, skenario, dan metrik antarstudi.

4. Hasil dan Pembahasan

4.1 Karakteristik Literatur yang Dikaji

Dua belas studi substantif yang digunakan membentuk dua kelompok. Kelompok pertama terdiri atas penelitian teknis yang secara langsung mengembangkan atau mengevaluasi mekanisme perlindungan payload end-to-end. Kelompok kedua berupa survey/review yang memetakan ancaman, autentikasi, kontrol akses, privasi, dan tantangan keamanan IoT–cloud. Kombinasi kedua kelompok memungkinkan kajian menghubungkan kebutuhan keamanan tingkat sistem dengan bukti implementasi mekanisme E2E.

Tabel 3. Karakteristik studi utama

Studi	Fokus	Mekanisme/jenis kajian	Cakupan E2E
Diro et al. (2020)	Publish–subscribe IoT	Lightweight authenticated encryption	Payload protection
Tawalbeh et al. (2020)	IoT privacy & security	Survey solusi keamanan	Tidak spesifik E2E
Winarno & Sari (2022)	Secure MQTT	Lightweight block cipher	End-to-end
Yang (2022)	IoT privacy	Overview solusi privasi	Tidak spesifik E2E
Iqal et al. (2024)	Access control IoT	Systematic review/taxonomy	Tidak spesifik E2E
Kaur et al. (2024)	IoT data security	Survey mitigasi	Tidak spesifik E2E
Lin et al. (2024)	IoT publish–subscribe	Conditional proxy re-encryption	End-to-end
Almutairi & Sheldon (2025)	IoT–cloud security	Survey	Tidak spesifik E2E
Singh et al. (2025)	Cloud-based IoT	Survey	Tidak spesifik E2E
Alotaibi et al. (2025)	IoT authentication	Review	Tidak spesifik E2E
Sebestyen et al. (2025)	IoT security	Literature review	Tidak spesifik E2E
Mishra et al. (2025)	SDN-enabled IoT	Review	Tidak spesifik E2E

4.2 Ancaman terhadap Keamanan Data End-to-End

Sintesis menunjukkan bahwa ancaman mengikuti posisi data dalam rantai komunikasi. Pada endpoint, risiko utama berupa kompromi kredensial, manipulasi perangkat, dan pengambilalihan. Pada jaringan, risiko mencakup eavesdropping, man-in-the-middle, spoofing, replay, dan message tampering. Pada intermediary, broker exposure menjadi penting ketika perlindungan hanya berada pada kanal sehingga broker memperoleh plaintext. Pada cloud, ancaman meliputi unauthorized access, insecure API, data leakage, dan misconfiguration (Almutairi & Sheldon, 2025; Singh et al., 2025; Kaur et al., 2024). Temuan ini menjawab RQ1: keamanan E2E harus dipandang sebagai perlindungan berlapis karena ancaman tidak berada pada satu titik saja.

4.3 Mekanisme Enkripsi, Integritas, dan Distribusi Pesan

Untuk RQ2 dan RQ3, studi teknis memperlihatkan tiga pola utama. Diro et al. (2020) menggabungkan confidentiality dan integrity melalui lightweight authenticated encryption pada komunikasi publish–subscribe. Winarno dan Sari (2022) menerapkan lightweight block-cipher cryptography pada komunikasi MQTT end-to-end untuk menyeimbangkan security strength dan resource efficiency. Lin et al. (2024) menggunakan conditional proxy re-encryption agar distribusi pesan dapat dibantu intermediary tanpa membuka plaintext. Ketiganya menunjukkan bahwa lokasi enkripsi/dekripsi dan pengelolaan kunci sama pentingnya dengan pilihan algoritma.

4.4 Autentikasi, Manajemen Kunci, dan Kontrol Akses

Enkripsi tidak menjamin keamanan apabila endpoint palsu dapat memperoleh kunci. Alotaibi et al. (2025) menekankan autentikasi yang mempertimbangkan resource constraints, scalability, dan ketahanan terhadap serangan. Iqal et al. (2024) menunjukkan bahwa kontrol akses IoT perlu dievaluasi dari kebutuhan, teknologi, skalabilitas, dan metrik yang digunakan. Pada E2EE, autentikasi dan kontrol akses harus terhubung dengan key ownership dan key lifecycle. Kunci yang kuat tetapi didistribusikan kepada pihak yang tidak berwenang tetap menghasilkan kebocoran; sebaliknya, kontrol akses cloud tidak cukup apabila broker atau administrator masih dapat memperoleh plaintext.

4.5 E2E Protection Coverage sebagai Pembeda Utama

Istilah secure communication tidak selalu berarti end-to-end security. Penilaian harus melihat posisi enkripsi dan dekripsi serta pihak yang memiliki akses terhadap kunci. Klasifikasi berikut digunakan untuk mencegah penyamaan TLS channel protection dengan E2EE.

Tabel 4. Klasifikasi cakupan perlindungan end-to-end

Kategori	Karakteristik	Implikasi keamanan
E2E	Payload terlindungi dari sumber hingga tujuan; intermediary tidak memerlukan plaintext	Mengurangi paparan pada broker/gateway
Hop-by-hop	Setiap segmen diamankan tetapi intermediary dapat melakukan terminasi	Broker/gateway tetap menjadi titik kepercayaan
Partial E2E	Hanya bagian payload atau jalur tertentu yang terlindungi	Keamanan bergantung pada bagian yang tidak terlindungi
Unclear	Informasi posisi enkripsi/dekripsi tidak memadai	Cakupan perlindungan tidak dapat disimpulkan

4.6 Trade-off Keamanan dan Kinerja

RQ4 menunjukkan bahwa efektivitas E2E tidak cukup dinilai dari keberhasilan menjaga kerahasiaan. Enkripsi/dekripsi, pembuatan dan verifikasi authentication tag, pertukaran kunci, serta metadata kriptografi menambah beban komputasi dan komunikasi. Pada perangkat resource-constrained, dampaknya perlu diukur melalui latency, CPU, memory, energy, message size, bandwidth overhead, dan scalability. Karena lingkungan pengujian antarstudi berbeda, nilai kinerja tidak digabungkan secara kuantitatif; perbandingan dilakukan pada jenis overhead dan trade-off yang dilaporkan.

Tabel 5. Dimensi evaluasi keamanan dan kinerja

Dimensi	Pertanyaan evaluasi	Metrik yang relevan
Confidentiality	Apakah payload tetap rahasia terhadap intermediary?	E2E coverage, plaintext exposure
Integrity	Apakah manipulasi dapat terdeteksi?	Authentication tag/MAC
Authentication	Apakah endpoint dapat diverifikasi?	Authentication time/failure
Key management	Apakah kunci dapat dikelola pada skala besar?	Storage, rotation, distribution cost
Performance	Berapa biaya mekanisme keamanan?	Latency, CPU, memory, energy
Communication	Berapa tambahan data?	Message size, bandwidth overhead
Scalability	Apakah tetap layak saat perangkat bertambah?	Key/identity management complexity

4.7 Research Gap dan Implikasi Arsitektur

Untuk RQ5, terdapat empat kesenjangan utama. Pertama, banyak review IoT–cloud memetakan threat landscape dan mitigasi secara luas tetapi tidak menjadikan cakupan payload end-to-end sebagai variabel pembanding. Kedua, studi E2E teknis cenderung menilai protokol atau skema tertentu sehingga integrasi antara E2E coverage, identity, authorization, key lifecycle, dan overhead belum selalu dianalisis dalam satu kerangka. Ketiga, heterogenitas perangkat, algoritma, dan skenario membuat hasil kinerja sulit dibandingkan. Keempat, skalabilitas manajemen kunci dan evaluasi pada perangkat nyata tetap menjadi tantangan. Karena itu, arsitektur IoT–cloud yang lebih kuat sebaiknya menempatkan perlindungan payload pada endpoint, menggunakan authenticated encryption, menerapkan autentikasi dan lifecycle kunci yang jelas, serta tetap mempertahankan TLS untuk keamanan kanal. Kontrol akses cloud dan proteksi data at rest tetap diperlukan karena E2EE tidak menyelesaikan seluruh risiko penyimpanan dan pemrosesan.

4.8 Keterbatasan Kajian

Kajian ini memiliki tiga keterbatasan. Pertama, jumlah studi teknis yang secara eksplisit mengevaluasi perlindungan payload end-to-end lebih sedikit dibandingkan survey keamanan IoT secara umum. Kedua, metrik kinerja antarstudi tidak seragam sehingga perbandingan kuantitatif dan meta-analisis tidak dilakukan. Ketiga, kajian bergantung pada informasi yang dilaporkan penulis masing-masing studi dan tidak melakukan replikasi eksperimental terhadap algoritma atau arsitektur yang ditinjau. Keterbatasan tersebut membuat hasil lebih tepat digunakan sebagai kerangka komparatif dan dasar perancangan penelitian lanjutan daripada sebagai ranking absolut suatu algoritma.

5. Kesimpulan

Kajian menunjukkan bahwa keamanan data pada sistem IoT berbasis cloud perlu menggabungkan perlindungan endpoint, komunikasi, intermediary, dan cloud. E2EE memberikan nilai tambah dibandingkan hop-by-hop karena payload dapat tetap terlindungi ketika melewati broker atau gateway yang tidak sepenuhnya dipercaya. Namun, E2EE bukan mekanisme tunggal; efektivitasnya bergantung pada integritas pesan, autentikasi endpoint, manajemen kunci, kontrol akses, dan keamanan cloud.

Dari 12 studi substantif yang disintesis, pendekatan teknis yang paling relevan mencakup lightweight authenticated encryption, lightweight block cipher untuk MQTT, dan conditional proxy re-encryption. Penerapan mekanisme tersebut menghadapi trade-off pada latency, CPU, memory, energy, bandwidth, serta kompleksitas pengelolaan kunci. Penelitian selanjutnya perlu menggunakan benchmark yang lebih seragam, menguji mekanisme pada perangkat IoT nyata, dan mengembangkan key management yang scalable serta interoperabel agar perlindungan payload dapat dipertahankan sepanjang siklus hidup data.

Ucapan Terima Kasih

Penulis mengucapkan syukur kepada Tuhan Yang Maha Esa serta terima kasih kepada dosen pembimbing dan seluruh pihak yang telah memberikan arahan, dukungan, dan kontribusi selama penyusunan kajian ini.

Daftar Referensi

Almutairi, M., & Sheldon, F. T. (2025). IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. Electronics, 14(7), 1394. https://doi.org/10.3390/electronics14071394

Alotaibi, A., Aldawghan, H., & Aljughaiman, A. (2025). A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions. Sensors, 25(6), 1649. https://doi.org/10.3390/s25061649

Diro, A. A., Reda, H. T., Chilamkurti, N., Mahmood, A., Jhanjhi, N. Z., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication. IEEE Access, 8, 60539–60551. https://doi.org/10.1109/ACCESS.2020.2983117

Iqal, Z. M., Selamat, A., & Krejcar, O. (2024). A comprehensive systematic review of access control in IoT: Requirements, technologies, and evaluation metrics. IEEE Access, 12, 12636–12654. https://doi.org/10.1109/ACCESS.2023.3347495

Kaur, K., Kaur, A., Gulzar, Y., & Gandhi, V. (2024). Unveiling the core of IoT: Comprehensive review on data security challenges and mitigation strategies. Frontiers in Computer Science, 6, 1420680. https://doi.org/10.3389/fcomp.2024.1420680

Lin, S., Cui, L., & Ke, N. (2024). End-to-end encrypted message distribution system for the Internet of Things based on conditional proxy re-encryption. Sensors, 24(2), 438. https://doi.org/10.3390/s24020438

Mishra, S. R., Shanmugam, B., Yeo, K. C., & Thennadil, S. (2025). SDN-enabled IoT security frameworks—A review of existing challenges. Technologies, 13(3), 121. https://doi.org/10.3390/technologies13030121

Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A literature review on security in the Internet of Things: Identifying and analysing critical categories. Computers, 14(2), 61. https://doi.org/10.3390/computers14020061

Singh, N., Buyya, R., & Kim, H. (2025). Securing cloud-based Internet of Things: Challenges and mitigations. Sensors, 25(1), 79. https://doi.org/10.3390/s25010079

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102

Winarno, A., & Sari, R. F. (2022). A novel secure end-to-end IoT communication scheme using lightweight cryptography based on block cipher. Applied Sciences, 12(17), 8817. https://doi.org/10.3390/app12178817

Yang, G. (2022). An overview of current solutions for privacy in the Internet of Things. Frontiers in Artificial Intelligence, 5, 812732. https://doi.org/10.3389/frai.2022.812732