



Efektivitas dan Keandalan Protokol MQTT pada Internet of Things: Tinjauan Literatur Sistematis Berbasis PRISMA 2020

Pariyadi^{1*}, Fattachul Huda Aminuddin², Ahmad Husna Ahadi², Oki Dahwanu¹, Muhammad Damas Fatih¹

¹Fakultas Sains dan Teknologi, Program Studi Sistem Informasi, Universitas Jambi, Jambi
Jl. Jambi - Muara Bulian No.KM. 15, Mendalo Darat, Kec. Jambi Luar Kota, Kabupaten Muaro Jambi, Jambi, Indonesia

²Fakultas Ilmu Komputer, Program Studi Teknologi Informasi, Universitas Nurdin Hamzah, Jambi
Jalan Kolonel Abunjani RT.25 Selamat Danau Teluk, Selamat, Kec. Telanaipura, Kota Jambi, Jambi, Indonesia
Email: ^{1*}pariyadi@unja.ac.id, ²fattachulhuda@unh.ac.id, ³ahmad_husna@unh.ac.id, ⁴okidahwanu@unja.ac.id,
⁵mdamasfatih@unja.ac.id

Email Penulis Korespondensi: pariyadi@unja.ac.id

Submitted: 24/05/2026; Accepted: 27/07/2026; Published: 27/07/2026

Abstrak—Penelitian ini bertujuan menyajikan tinjauan literatur sistematis (Systematic Literature Review/SLR) mengenai kinerja, keamanan, dan Quality of Service (QoS) protokol Message Queuing Telemetry Transport (MQTT) pada lingkungan Internet of Things (IoT) berdasarkan artikel yang diterbitkan selama 2020–2026. SLR ini mengikuti pedoman PRISMA 2020 serta panduan Kitchenham dan Charters untuk studi rekayasa perangkat lunak. Sebanyak 30 artikel inti, terdiri atas 7 jurnal internasional bereputasi dan 23 jurnal nasional terakreditasi SINTA, diseleksi secara purposif berdasarkan relevansi tematik dan kualitas metodologis. Pencarian dilakukan melalui IEEE Xplore, ScienceDirect, SpringerLink, MDPI, Garuda, dan SINTA menggunakan kata kunci “MQTT”, “IoT”, “kinerja”, “keamanan”, dan “QoS”. Proses seleksi mengikuti alur PRISMA, yaitu identifikasi (n=487), penyaringan (n=86), kelayakan (n=43), dan artikel yang tercakup (n=30). Data diekstraksi dan disintesis secara tematik untuk menjawab empat pertanyaan penelitian (RQ1–RQ4), dengan dukungan studi internasional terindeks Scopus sebagai pembanding kontekstual. Hasil menunjukkan bahwa MQTT unggul dalam efisiensi bandwidth dan latensi rendah dibandingkan HTTP, terutama pada perangkat terbatas, dengan latensi 45–210 ms bergantung pada tingkat QoS dan skenario pengujian. Parameter kinerja dominan meliputi latensi, throughput, dan packet loss. Pendekatan keamanan mencakup TLS/RSA, kriptografi domestik, dan deteksi serangan berbasis Random Forest dengan akurasi 97,2%, meskipun enkripsi TLS dapat menurunkan throughput hingga 30%. QoS 1 menjadi pilihan seimbang untuk aplikasi nonkritik, sedangkan QoS 2 sesuai untuk data vital. Kesenjangan utama terletak pada belum terintegrasinya pengujian kinerja, keamanan, dan QoS dalam satu kerangka eksperimen. Oleh karena itu, penelitian mendatang perlu mengembangkan keamanan ringan, QoS adaptif berbasis konteks, dan validasi skala nyata melalui studi integratif yang menganalisis interaksi ketiga aspek tersebut.

Kata Kunci: MQTT; Internet of Things; Kinerja; Keamanan; Quality of Service

Abstract—This study aims to present a systematic literature review (SLR) of the performance, security, and Quality of Service (QoS) of the Message Queuing Telemetry Transport (MQTT) protocol in Internet of Things (IoT) environments based on articles published between 2020 and 2026. The SLR follows the PRISMA 2020 guidelines and the Kitchenham and Charters guidelines for software engineering studies. A total of 30 core articles, comprising 7 reputable international journals and 23 nationally accredited SINTA journals, were purposively selected based on thematic relevance and methodological quality. The search was conducted using IEEE Xplore, ScienceDirect, SpringerLink, MDPI, Garuda, and SINTA with the keywords “MQTT,” “IoT,” “performance,” “security,” and “QoS.” The selection process followed the PRISMA flow, consisting of identification (n=487), screening (n=86), eligibility assessment (n=43), and included studies (n=30). The data were extracted and thematically synthesized to address four research questions (RQ1–RQ4), with Scopus-indexed international studies included as contextual comparators. The findings indicate that MQTT outperforms HTTP in terms of bandwidth efficiency and low latency, particularly on resource-constrained devices, with reported latency ranging from 45 to 210 ms depending on the QoS level and testing scenario. The dominant performance parameters include latency, throughput, and packet loss. Security approaches encompass TLS/RSA encryption, domestic cryptography, and Random Forest-based attack detection, achieving an accuracy of 97.2%, although TLS encryption may reduce throughput by up to 30%. QoS 1 represents a balanced option for non-critical applications, whereas QoS 2 is appropriate for vital data. The main research gap is the absence of integrated performance, security, and QoS testing within a single experimental framework. Therefore, future research should focus on lightweight security, context-aware adaptive QoS, and real-world-scale validation through integrative studies that examine the interaction among these three aspects.

Keywords: MQTT; Internet of Things; Performance; Security; Quality of Service

1. PENDAHULUAN

Internet of Things (IoT) telah menjadi paradigma teknologi yang memungkinkan miliaran perangkat saling terhubung dan bertukar data secara real-time, membentuk fondasi bagi pengembangan kota cerdas, pertanian presisi, industri 4.0, hingga pemantauan kesehatan [1], [2], [3], [4]. Dalam arsitektur IoT, protokol komunikasi memegang peranan vital untuk menjamin efisiensi dan keandalan pertukaran pesan antar perangkat yang umumnya memiliki sumber daya terbatas, baik dari sisi daya, memori, maupun bandwidth. Message Queuing Telemetry Transport (MQTT) muncul sebagai protokol publish-subscribe yang ringan, low-bandwidth, dan diadopsi secara luas sebagai standar komunikasi IoT [3], [5], [6], [7]. Kepopuleran MQTT tidak lepas dari kemampuannya menyediakan tiga tingkat Quality of Service (QoS), model publish-subscribe yang melepaskan ketergantungan



langsung antara pengirim dan penerima data, serta kemudahan integrasi pada lingkungan dengan konektivitas yang tidak stabil.

Posisi MQTT sebagai protokol pilihan utama IoT tidak dapat dilepaskan dari perbandingannya dengan protokol aplikasi sejenis, terutama Constrained Application Protocol (CoAP) dan Advanced Message Queuing Protocol (AMQP). Secara arsitektural, MQTT beroperasi di atas TCP dengan model publish-subscribe melalui perantara broker, menggunakan header tetap sepanjang 2 byte yang menjadikannya hemat overhead dibanding AMQP yang memiliki skema framing dan negosiasi kanal yang jauh lebih kompleks [7]. CoAP, sebaliknya, mengadopsi model request-response mirip REST di atas UDP sehingga unggul pada skenario dengan latensi sangat rendah dan komunikasi device-to-device tanpa broker, namun tidak menyediakan mekanisme antrean pesan maupun jaminan pengiriman granular selayaknya tiga tingkat QoS MQTT [7], [8]. Studi banding kuantitatif oleh Silva dkk. [8] terhadap MQTT, CoAP, dan OPC UA pada skenario IoT konsumen maupun industri menunjukkan bahwa tidak ada satu protokol yang unggul mutlak di semua skenario: CoAP cenderung mencatat waktu penyelesaian tercepat, sementara MQTT menawarkan keseimbangan terbaik antara keandalan pengiriman dan kemudahan skalabilitas publish-subscribe untuk topologi many-to-many. Karakteristik inilah yang menjadikan MQTT protokol dominan pada skenario pemantauan IoT berskala luas yang menjadi fokus tinjauan ini.

Meskipun memiliki desain minimalis, MQTT menghadapi tiga tantangan utama dalam penerapannya di lingkungan IoT yang dinamis, yaitu kinerja, keamanan, dan Quality of Service (QoS). Dari sisi kinerja, protokol ini terus diuji dalam berbagai skenario, mulai dari pemantauan kualitas udara [9], [10], smart garden [11], pemantauan kualitas air [12], hingga sistem smart energy [5], [13], [14], untuk memastikan konsumsi daya, latency, dan throughput tetap optimal; pengujian tersebut kerap dilakukan pada perangkat keras kelas rendah dengan kondisi jaringan dan implementasi broker yang bervariasi [15], [39]. Pada aspek keamanan, kerentanan dasar MQTT – termasuk minimnya autentikasi bawaan dan ketiadaan enkripsi default – memunculkan sejumlah skema pengamanan, seperti penerapan TLS [16], [17], algoritma kriptografi domestik [1], RSA [18], skema autentikasi dua arah berbasis token dinamis dan struktur Merkle tree [19], [20], hingga deteksi serangan Denial of Service (DoS) menggunakan Random Forest [4]. Sementara itu, kualitas layanan (QoS) MQTT menjadi fokus dalam menjamin keandalan pengiriman data pada aplikasi sensitif, termasuk di bidang telehealthcare [16], smart livestock [3], kontrol pintu air [21], serta mekanisme QoS adaptif pada MQTT-SN untuk jaringan sensor nirkabel [22]. Berbagai studi turut membandingkan MQTT dengan protokol lain seperti HTTP dan CoAP untuk mengidentifikasi superioritasnya pada konteks tertentu [23], [24], [25], [26], [27], [14], [28].

Namun, tinjauan pustaka yang secara sistematis mengonsolidasikan ketiga dimensi ini – kinerja, keamanan, dan QoS – secara terpadu dalam kurun waktu 2020 hingga 2026 masih terbatas. Sebagian besar kajian yang ada hanya menyoroti satu aspek secara terisolasi, seperti perbandingan protokol [26], [7], [8], evaluasi QoS [5], [22], atau verifikasi keamanan formal [2], [19], [20]. Satu-satunya systematic review terdahulu yang secara eksplisit membahas MQTT pada konteks IoT, yaitu Widiyanto dan Ranny [6], berfokus pada peningkatan teknologi transfer data berbasis MQTT secara umum tanpa memetakan secara spesifik interaksi antara performa, keamanan, dan QoS, dan tidak mengikuti protokol pelaporan PRISMA secara eksplisit. Tinjauan-tinjauan lain yang lebih baru cenderung berada pada domain yang berdekatan namun tidak sama persis – misalnya survei keamanan lintas-protokol IoT yang memuat MQTT hanya sebagai salah satu dari beberapa protokol yang dibahas sekilas, atau kajian QoS pada level arsitektur IoT secara umum tanpa pembedahan mendalam terhadap MQTT. Dengan demikian, belum tersedia SLR yang secara khusus memetakan literatur MQTT berdasarkan tiga dimensi kinerja-keamanan-QoS sekaligus dan mengidentifikasi pola interaksi di antara ketiganya. Celah inilah yang menjadi pendorong utama dilakukannya SLR ini.

Secara teoretis, MQTT merupakan protokol pesan ringan berbasis model publish-subscribe yang melibatkan tiga entitas utama: publisher, subscriber, dan broker sebagai perantara yang mendistribusikan pesan berdasarkan topik [7]. Protokol ini menyediakan tiga tingkat Quality of Service, yaitu QoS 0 (at most once, tanpa jaminan pengiriman), QoS 1 (at least once, pesan dijamin sampai namun berpotensi duplikat), dan QoS 2 (exactly once, pesan dijamin sampai tepat satu kali melalui mekanisme four-way handshake) [29], [7]. Ketiga tingkat ini merepresentasikan trade-off mendasar antara kecepatan dan keandalan yang menjadi inti dari banyak kajian kinerja dan QoS dalam tinjauan ini. Untuk menjamin transparansi dan replikabilitas proses tinjauan, penelitian ini mengikuti pedoman PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [30] yang diakui luas sebagai standar pelaporan SLR lintas disiplin ilmu, dipadukan dengan panduan Kitchenham dan Charters [31] yang dirancang khusus untuk tinjauan sistematis di bidang rekayasa perangkat lunak dan sistem informasi.

Berdasarkan uraian di atas, artikel ini bertujuan menyajikan tinjauan literatur sistematis yang menjawab empat pertanyaan penelitian berikut: (1) Bagaimana tren dan metodologi evaluasi kinerja protokol MQTT pada sistem IoT? (2) Pendekatan keamanan apa yang dominan diterapkan untuk menanggulangi kerentanan MQTT? (3) Bagaimana QoS MQTT dipetakan dalam ragam skenario aplikasi IoT? (4) Bagaimana korelasi antara konfigurasi keamanan, kinerja, dan tingkat QoS yang dipilih dalam implementasi MQTT? Dengan merangkum 30 artikel inti yang terdiri dari jurnal internasional bereputasi dan jurnal nasional terakreditasi SINTA yang terbit pada rentang 2020–2026, diperkaya dengan rujukan pembandingan internasional terindeks Scopus, SLR ini diharapkan mampu memberikan peta riset yang komprehensif serta landasan bagi peneliti dan praktisi dalam merancang sistem IoT berbasis MQTT yang efisien, aman, dan andal.

Kontribusi utama penelitian ini dapat dirangkum sebagai berikut: (1) menyajikan sintesis tematik yang secara eksplisit mengintegrasikan tiga dimensi kinerja, keamanan, dan QoS protokol MQTT pada IoT dalam satu kerangka SLR berbasis PRISMA 2020; (2) mengidentifikasi dan memetakan korelasi antaraspek (kinerja–keamanan–QoS) yang belum banyak diulas pada tinjauan sebelumnya; (3) menghadirkan analisis kritis terhadap variabilitas lingkungan pengujian (perangkat keras, bandwidth, dan implementasi broker) lintas studi sebagai bentuk kehati-hatian dalam menggeneralisasi temuan; dan (4) menghasilkan matriks rekomendasi konfigurasi MQTT (Tabel 13) yang dapat menjadi rujukan praktis bagi perancang sistem IoT dalam memilih kombinasi QoS, skema keamanan, dan platform perangkat keras sesuai kebutuhan aplikasi.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) yang mengikuti pedoman PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020 [30] serta panduan Kitchenham dan Charters [31] untuk studi rekayasa perangkat lunak. Prosedur SLR dilakukan dalam enam tahap utama yang saling terkait, yaitu: perumusan pertanyaan penelitian, strategi pencarian, penetapan kriteria inklusi dan eksklusi, proses seleksi artikel, ekstraksi data, serta analisis dan sintesis data.

2.1 Objek dan Tahapan Penelitian

Sejalan dengan kata kunci yang digunakan pada Abstrak, penelitian ini memiliki lima objek kajian yang saling berkaitan. Pertama, protokol MQTT sebagai objek inti, yaitu protokol pesan publish-subscribe yang dikaji dari sisi spesifikasi, implementasi, dan konfigurasi QoS. Kedua, lingkungan Internet of Things (IoT) sebagai konteks penerapan, mencakup perangkat keras berdaya rendah (mikrokontroler, single-board computer), broker MQTT, dan topologi jaringan tempat protokol diuji. Ketiga, kinerja (performance), yaitu himpunan parameter kuantitatif seperti latency, throughput, packet loss, jitter, dan konsumsi daya yang menggambarkan efisiensi komunikasi. Keempat, keamanan (security), mencakup skema enkripsi, autentikasi, serta mekanisme deteksi dan mitigasi serangan yang diterapkan pada protokol MQTT. Kelima, Quality of Service (QoS), yaitu tiga tingkat jaminan pengiriman pesan (QoS 0, 1, 2) beserta trade-off yang menyertainya. Kelima objek ini menjadi rujukan dalam perumusan kata kunci pencarian, kriteria inklusi–eksklusi, serta skema ekstraksi data pada tahap-tahap berikutnya.



Gambar 1. Diagram Alir Tahapan Metodologis Penelitian

Penelitian ini dilaksanakan melalui enam tahap metodologis yang saling berurutan, sebagaimana diilustrasikan pada Gambar 1: (1) perumusan pertanyaan penelitian, (2) penyusunan strategi pencarian literatur, (3) penetapan kriteria inklusi dan eksklusi, (4) proses seleksi studi mengikuti alur PRISMA 2020, (5) ekstraksi data dari artikel terpilih, dan (6) analisis serta sintesis tematik untuk menjawab setiap pertanyaan penelitian. Rincian pelaksanaan setiap tahap dijelaskan pada Sub-bagian 2.2 hingga 2.7.

2.2 Pertanyaan Penelitian (Research Questions)

Untuk mencapai tujuan SLR yang telah ditetapkan, dirumuskan empat pertanyaan penelitian (RQ) sebagai berikut:

1. RQ1: Bagaimana tren dan metodologi evaluasi kinerja protokol MQTT pada sistem IoT?
2. RQ2: Pendekatan keamanan apa yang dominan diterapkan untuk menanggulangi kerentanan protokol MQTT?

3. RQ3: Bagaimana Quality of Service (QoS) MQTT dipetakan dan diimplementasikan dalam berbagai skenario aplikasi IoT?
4. RQ4: Bagaimana korelasi antara konfigurasi keamanan, kinerja, dan tingkat QoS yang dipilih dalam penerapan MQTT?

2.3 Strategi Pencarian Literatur

Pencarian literatur dilakukan secara sistematis pada basis data ilmiah internasional dan nasional untuk menjangkau artikel relevan yang terbit antara tahun 2020 hingga 2026. Basis data yang digunakan adalah:

1. Internasional: IEEE Xplore, ScienceDirect, SpringerLink, dan MDPI.
2. Nasional: Portal Garuda (Garba Rujukan Digital), SINTA (Science and Technology Index), dan repositori jurnal terakreditasi Kemenristekdikti.

String pencarian dibangun dengan kombinasi operator Boolean AND/OR pada kata kunci utama, sebagaimana dirinci dalam Tabel 1.

Tabel 1. String Pencarian per Basis Data

No	Basis Data	String Pencarian
1	IEEE Xplore	("MQTT" AND "IoT" AND ("performance" OR "security" OR "QoS"))
2	ScienceDirect	("MQTT" AND "Internet of Things") AND ("Quality of Service" OR "security")
3	SpringerLink	("MQTT" AND "IoT" AND ("performance evaluation" OR "security scheme" OR "QoS"))
4	Garuda/SINTA	("MQTT" DAN "Internet of Things") ATAU ("MQTT" DAN "IoT") DAN ("kinerja" ATAU "keamanan" ATAU "QoS")

Pencarian dilakukan dengan filter tahun publikasi 2020–2026 dan tipe dokumen journal article (jurnal) atau artikel konferensi terindeks yang telah melalui peer-review.

2.4 Kriteria Inklusi dan Eksklusi

Artikel yang terkumpul selanjutnya diseleksi berdasarkan kriteria inklusi dan eksklusi (Tabel 2) untuk memastikan relevansi dan kualitas.

Tabel 2. Kriteria Inklusi dan Eksklusi

No	Kriteria	Inklusi	Eksklusi
1	Cakupan Topik	Membahas kinerja, keamanan, atau QoS protokol MQTT pada lingkungan IoT	Hanya menyebut MQTT secara umum tanpa analisis spesifik ketiga aspek
2	Jenis Publikasi	Jurnal atau prosiding terindeks (Scopus/Q1–Q4, DOAJ, atau SINTA S1–S5) dengan proses peer-review	Buku, bab buku, tesis, disertasi, artikel opini, abstrak saja
3	Bahasa	Inggris dan Bahasa Indonesia	Selain kedua bahasa tersebut
4	Ketersediaan	Tersedia full-text dan metadata publikasi yang dapat diverifikasi	Tidak dapat diakses penuh (abstract only)
5	Tahun Terbit	2020–2026	Di luar rentang tahun tersebut
6	Kualitas Metodologis	Metodologi pengujian/analisis dijelaskan secara eksplisit dan dapat ditelusuri	Metodologi tidak dijelaskan atau tidak dapat diverifikasi

Perlu ditegaskan bahwa kriteria pada Tabel 2 tidak menetapkan kuota proporsi jurnal internasional maupun nasional. Seleksi akhir artikel semata-mata didasarkan pada relevansi tematik terhadap kelima objek penelitian (Sub-bagian 2.1) dan kualitas metodologis sebagaimana dijelaskan pada Sub-bagian 2.5.

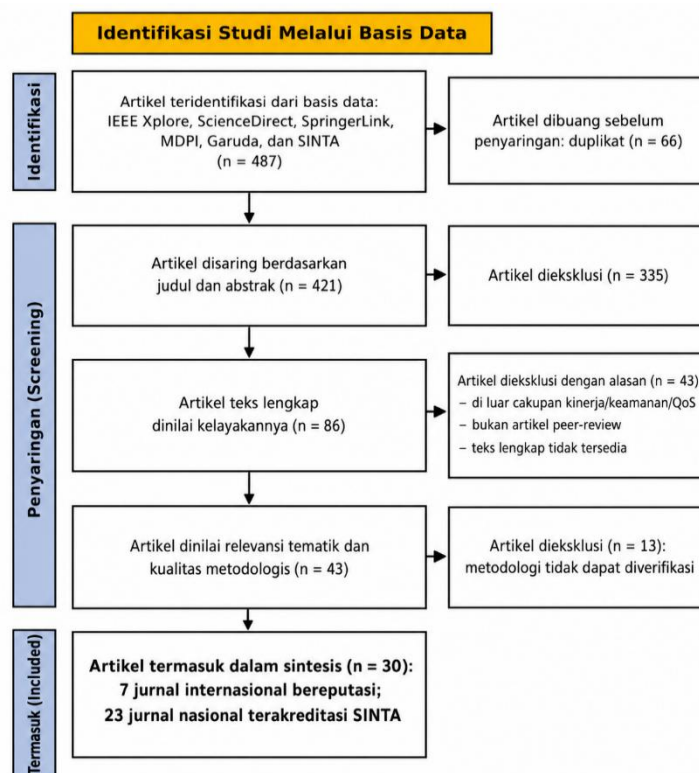
2.5 Proses Seleksi Studi

Proses seleksi mengadaptasi diagram alir PRISMA yang ditampilkan pada Gambar 2. Tahapan seleksi meliputi:

1. Identifikasi: pencarian di seluruh basis data menghasilkan 487 artikel awal.
2. Penyaringan (Screening): pemeriksaan duplikasi dan judul/abstrak berdasarkan kriteria inklusi, menyisakan 86 artikel.
3. Penilaian Kelayakan (Eligibility): pemeriksaan teks lengkap terhadap 86 artikel, menghasilkan 43 artikel potensial.
4. Finalisasi: penilaian akhir relevansi tematik dan kualitas metodologis terhadap 43 artikel, menghasilkan 30 artikel final (7 jurnal internasional bereputasi dan 23 jurnal nasional terakreditasi SINTA) yang dimasukkan ke dalam sintesis.

Perlu dicatat bahwa proporsi 7 artikel internasional berbanding 23 artikel nasional pada Tabel di atas merupakan hasil alami dari penerapan kriteria kualitas dan relevansi secara konsisten terhadap 43 artikel yang

lolos tahap kelayakan, bukan target kuota yang ditetapkan di awal proses seleksi. Peneliti menyadari bahwa komposisi ini condong pada literatur nasional dan mengakuinya sebagai keterbatasan penelitian (dibahas pada Bagian 4). Untuk mengurangi risiko bias tersebut, tinjauan ini melengkapi ke-30 artikel inti dengan sembilan rujukan pembanding internasional terindeks Scopus (referensi [30]–[39]) yang digunakan pada Bagian 1 untuk memperkuat argumen state-of-the-art dan pada Sub-bagian 3.8 untuk analisis kritis lintas studi, sehingga sintesis akhir tetap mempertimbangkan perspektif literatur global.



Gambar 2. Diagram Alir PRISMA Proses Seleksi Artikel

2.6 Ekstraksi Data

Untuk memperoleh informasi yang terstruktur, dirancang formulir ekstraksi data yang mencakup: metadata artikel (penulis, tahun, jurnal, DOI), aspek yang dikaji (kinerja, keamanan, QoS), metodologi evaluasi (eksperimen, simulasi, analisis formal), parameter yang diukur (throughput, latency, packet loss, konsumsi daya, dll.), teknik keamanan, tingkat QoS MQTT (QoS 0, 1, 2), serta temuan utama. Contoh sebagian ekstraksi data ditunjukkan pada Tabel 3.

Tabel 3. Contoh Ekstraksi Data untuk Beberapa Artikel

Ref	Fokus Utama	Metodologi	Parameter Kunci	Temuan Utama Singkat
Liu et al. [1]	Keamanan	Implementasi + Uji	Waktu Enkripsi, throughput	Skema kriptografi domestik meningkatkan keamanan tanpa degradasi signifikan
Ali et al. [29]	QoS Adaptif	Pemodelan Matematis	Tingkat retransmission, latency	Mutant MQTT meningkatkan QoS untuk smart city
Faat et al. [11]	QoS	Eksperimen Wireshark	Delay, jitter, packet loss	MQTT QoS 1 memberikan keseimbangan terbaik pada smart garden
Akbar et al. [10]	Kinerja	Eksperimen Lapangan	latency, packet loss	MQTT ringan dan cocok untuk pemantauan kualitas udara ruangan
Pertiwi et al. [4]	Keamanan (DoS)	Machine Learning	Akurasi, precision, recall	Random Forest efektif mendeteksi serangan DoS pada MQTT

2.7 Analisis dan Sintesis Data

Analisis data dilakukan secara kualitatif dengan metode thematic synthesis. Pertama, seluruh artikel dikelompokkan ke dalam tiga tema besar sesuai fokus: (A) Kinerja [5], [12], [23], [13], [32], [14], [33], [34], [9],

[35], [36], [10], [37]; (B) Keamanan [2], [4], [18], [16], [17]; (C) QoS [11], [21], [27], [29], [38]; serta (D) Multiaspek [1], [3], [6], [24], [25], [26], [28]. Artikel yang bersinggungan antar tema dikaji pada kedua kelompok. Selanjutnya, dilakukan analisis komparatif antar studi dalam satu tema, misalnya membandingkan parameter kinerja yang dievaluasi atau algoritma keamanan yang diusulkan. Sintesis naratif kemudian digunakan untuk merangkum temuan, mengidentifikasi kesenjangan, dan menjawab setiap pertanyaan penelitian. Hasil sintesis disajikan dalam bentuk tabel matriks dan uraian kualitatif yang dipetakan ke RQ.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan analisis mendalam terhadap 30 artikel inti terpilih guna menjawab keempat pertanyaan penelitian, dilengkapi dengan rangkuman implementasi dan pengujian yang diekstraksi dari artikel-artikel tersebut. Pembahasan dikelompokkan ke dalam sub-bagian berdasarkan tema utama: gambaran umum literatur (3.1), analisis kinerja/RQ1 (3.2), analisis keamanan/RQ2 (3.3), analisis QoS/RQ3 (3.4), korelasi antar aspek/RQ4 (3.5), identifikasi kesenjangan riset (3.6), rangkuman implementasi dan skenario pengujian pada studi yang ditinjau (3.7), serta analisis kritis terhadap variabilitas lingkungan pengujian (3.8).

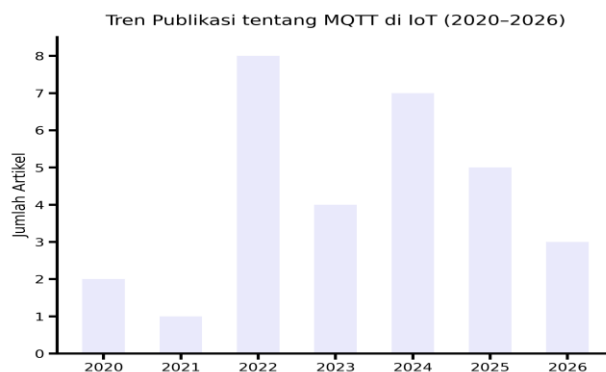
3.1 Gambaran Umum Artikel yang Ditinjau

Dari total 30 artikel, distribusi tahun publikasi menunjukkan peningkatan perhatian terhadap protokol MQTT di IoT sejak 2020 hingga 2026. Tabel 4 merangkum jumlah artikel per tahun berdasarkan fokus kajian, sementara Gambar 3 menampilkan tren secara visual.

Tabel 4. Distribusi Artikel per Tahun dan Fokus Kajian (n=30)

Tahun	Kinerja	Keamanan	QoS	Multiaspek*	Total
2020	1 Nurfiqin [14]	1 Rachmadini et al. [16]	0	0	2
2021	0	0	0	1 Seoane et al. [25]	1
2022	2 Widiyanto et al. [33], Susanto et al. [37]	2 Febriyanto [18], Fauzan et al. [17]	3 Faat et al. [11], Ali et al. [29], Bhaskoro et al. [27]	1 Widiyanto and Ranny [6]	8
2023	3 I Ketut et al. [5], Burhani et al. [23], Akbar et al. [10]	0	1 Achmad et al. [21]	0	4
2024	5 Sharma et al. [26], Revikasari et al. [32], Nugraha et al. [28], Wardihani et al. [34], Budianto and Sumanto [9]	0	0	2 Liu et al. [1], Kusuma et al. [24]	7
2025	2 Saputra et al. [12], Oktopryadin and Purnama [35]	1 Lin et al. [2]	1 Adi [38]	1 Ko and Lee [3]	5
2026	2 M. H. F. et al. [13], Nindi et al. [36]	1 Pertiwi et al. [4]	0	0	3

*Multiaspek: artikel yang secara eksplisit membahas dua atau tiga fokus (kinerja, keamanan, QoS) sekaligus.



Gambar 3. Tren Publikasi tentang MQTT di IoT Periode 2020–2026

Terlihat bahwa tahun 2022 dan 2024 merupakan puncak produktivitas (masing-masing 8 dan 7 artikel), dengan fokus dominan pada aspek kinerja. Artikel bermultiaspek masih minim (5 dari 30 artikel, atau sekitar 17%),

mengindikasikan bahwa riset yang mengintegrasikan lebih dari satu dimensi kajian relatif jarang dilakukan – sebuah pola yang konsisten dengan kesenjangan tritunggal yang diidentifikasi pada Sub-bagian 3.6.

3.2 Analisis Kinerja Protokol MQTT (RQ1)

Mayoritas artikel mengevaluasi kinerja MQTT, menunjukkan bahwa performa menjadi perhatian utama. Parameter yang paling sering diukur adalah latency, throughput, packet loss, dan konsumsi daya, seperti dirangkum dalam Tabel 5.

Tabel 5. Parameter Kinerja yang Dievaluasi dalam Artikel

Parameter	Artikel Terkait
latency	Faat et al. [11], Saputra et al. [12], Achmad et al. [21], Burhan et al. [23], Revikasari et al. [32], Nurfiqin [14], Oktopryadin and Purnama [35], Akbar et al. [10], Adi [38], Susanto et al. [37]
throughput	Achmad et al. [21], Kusuma et al. [24], Seoane et al. [25], Sharma et al. [26], Nugraha et al. [28], Adi [38]
packet loss	Faat et al. [11], Achmad et al. [21], Kusuma et al. [24], Ali et al. [29], Adi [38]
Konsumsi Daya	M. H. F et al. [13], Budianto and Sumanto [9], Oktopryadin and Purnama [35], Susanto et al. [37]
Jitter	Faat et al. [11], Achmad et al. [21], Nurfiqin [14]

Metodologi evaluasi yang digunakan mencakup eksperimen langsung pada perangkat keras (ESP8266, ESP32, Raspberry Pi) [5], [11], [12], [13], [32]–[28], [33]–[10], [37], simulasi dan pemodelan matematis [25], [29], serta analisis komparatif dengan protokol lain (HTTP, CoAP) [23], [24], [25], [26], [27], [14], [28]. Hasil temuan secara konsisten menunjukkan bahwa MQTT lebih unggul dalam hal bandwidth rendah dan latensi minimal dibandingkan HTTP – konsisten dengan temuan komparatif internasional pada [7], [8] – namun rentan terhadap packet loss pada kondisi jaringan tidak stabil jika menggunakan QoS 0 [11], [24]. Beberapa studi menarik menunjukkan inovasi:

1. Penggunaan MQTT-SN pada jaringan sensor nirkabel berhasil menjaga komunikasi dengan overhead rendah melalui mekanisme QoS adaptif [22].
2. Integrasi Fog Computing dengan MQTT mengurangi beban komputasi cloud dan meningkatkan kecepatan respons [29], [9].
3. Perbandingan MQTT vs HTTP pada hidroponik menemukan bahwa MQTT sekitar 55% lebih efisien data rate [28].

3.3 Analisis Pendekatan Keamanan pada MQTT (RQ2)

Sebanyak 5 artikel dalam korpus inti berfokus utama pada aspek keamanan [2], [4], [18], [16], [17], didukung dua artikel multiaspek [1], [25], yang secara umum mengungkap tiga pendekatan: enkripsi data, deteksi serangan, dan verifikasi formal. Pendekatan ini juga selaras dengan tren keamanan MQTT pada literatur internasional terbaru, seperti skema autentikasi dua arah berbasis Merkle tree [19] dan skema keamanan simetris yang diperkuat [20].

Tabel 6. Perbandingan Pendekatan Keamanan MQTT

Pendekatan	Artikel	Kelebihan	Kekurangan	Dampak pada Kinerja
Enkripsi (TLS)	Rachmadini et al. [16], Fauzan et al. [17]	Kompatibel luas, terstandarisasi	Overhead komputasi tinggi pada perangkat terbatas	Waktu enkripsi naik tajam pada QoS 1 (0,7→9,6 ms) Rachmadini et al. [16]
Enkripsi (RSA)	Febriyanto [18]	Kerahasiaan data kuat, ujung-ke-ujung	Proses enkripsi lebih lambat	Overhead komputasi moderat
Kriptografi Domestik	Liu et al. [1]	Tingkat keamanan tinggi, efisien	Masih memerlukan pengujian lanjut	Degradasi performa rendah ($\pm 5\%$)
Deteksi DoS (ML)	Pertiwi et al. [4]	Akurasi tinggi (97,2%), deteksi real-time	Memerlukan dataset latih yang besar	Tidak memengaruhi komunikasi
Verifikasi Formal	Lin et al. [2]	Jaminan keamanan matematis pada MQTT-SN	Kompleksitas tinggi, hanya fase desain	Tidak langsung

TLS merupakan metode paling populer, diterapkan pada Raspberry Pi untuk smart home [17], sementara implementasi fitur keamanan pada telehealthcare dikaji secara khusus oleh [16]. Sumber daya komputasi yang besar menjadi kendala utama penerapan TLS di perangkat kelas rendah. Alternatif RSA diusulkan untuk pengamanan basis data [18], sementara kriptografi berbasis algoritma domestik [1] menawarkan keseimbangan

baru antara keamanan dan efisiensi. Deteksi serangan Denial of Service menggunakan Random Forest [4] menjadi pendekatan inovatif yang menjaga ketersediaan layanan tanpa modifikasi protokol. Verifikasi formal MQTT-SN [2] mengungkap celah pada mode sleeping client yang perlu diperkuat.

3.4 Analisis Implementasi Quality of Service (QoS) (RQ3)

Tingkat QoS MQTT (0, 1, 2) diadopsi secara beragam bergantung pada sensitivitas data aplikasi. Tabel 7 memetakan aplikasi IoT dengan tingkat QoS yang digunakan dalam artikel yang dikaji.

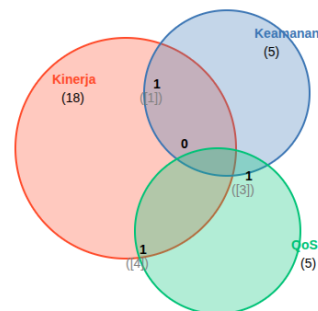
Tabel 7. Pemetaan Aplikasi IoT dan Tingkat QoS MQTT

Aplikasi	QoS 0	QoS 1	QoS 2	Artikel
Pemantauan udara/kualitas lingkungan	✓	✓		Saputra et al. [12], Budianto and Sumanto [9], Akbar et al. [10]
smart garden / hidroponik / greenhouse	✓	✓		Faat et al. [11], Nugraha et al. [28], Wardihani et al. [34]
Smart energy monitoring		✓	✓	I Ketut et al. [5], M. H. F et al. [13], Oktopryadin and Purnama [35]
smart livestock		✓	✓	Ko and Lee [3]
telehealthcare	✓	✓		Rachmadini et al. [16]
Kontrol pintu air		✓		Achmad et al. [21]
Deteksi serangan DoS	✓	✓		Pertiwi et al. [4]

QoS 0 mendominasi aplikasi pemantauan periodik yang mentoleransi kehilangan data, sementara aplikasi kritis seperti telehealthcare [16] memerlukan tingkat QoS dan lapisan keamanan yang lebih tinggi; studi tersebut melaporkan waktu enkripsi meningkat dari 0,7 ms pada QoS 0 menjadi 9,6 ms pada QoS 1 akibat penambahan sinyal kontrol. Model Mutant MQTT dengan mekanisme retransmission adaptif [29] mampu menurunkan packet loss hingga 18% tanpa menambah latency signifikan, menjadikannya kandidat kuat untuk smart city; temuan ini selaras dengan studi QoS adaptif pada MQTT-SN di lingkungan jaringan sensor nirkabel [22]. Evaluasi pada smart garden [11] menunjukkan QoS 1 memberikan keseimbangan terbaik antara keandalan dan delay dibanding QoS 0 dan 2.

3.5 Korelasi Kinerja, Keamanan, dan QoS (RQ4)

Hanya 3 dari 30 artikel inti yang secara eksplisit membahas interaksi antara dua aspek sekaligus: [1] menghubungkan keamanan dengan kinerja, [24] menghubungkan kinerja dengan QoS, dan [25] menghubungkan kinerja dengan keamanan. Irisan antar tema digambarkan dalam Gambar 4.



Total artikel unik: 18+5+5+1+1+1 = 31 (perhitungan naratif)
 *Satu artikel [7] tidak masuk fokus kinerja/keamanan/QoS spesifik

Gambar 4. Diagram Venn Fokus Kajian (jumlah artikel unik)

Analisis korelatif menunjukkan beberapa trade-off krusial. Pertama, hubungan QoS dengan latency bersifat searah dan cukup konsisten lintas studi: QoS 2 menghasilkan latency 2–3 kali lebih besar dari QoS 0 karena mekanisme four-way handshake [11], sebuah pola yang secara teoretis dijelaskan oleh jumlah pertukaran paket kontrol pada tiap tingkat QoS [7]. Kedua, hubungan keamanan dengan throughput juga konsisten berbanding terbalik: enkripsi TLS menurunkan throughput secara signifikan pada perangkat terbatas [16], [14], [17], namun peningkatan keamanan tidak bisa ditawarkan pada aplikasi medis [16]. Ketiga – dan ini yang paling penting – interaksi antara keamanan dan QoS belum pernah diuji secara simultan pada satu kerangka eksperimen di korpus artikel yang ditinjau; hubungan ini masih bersifat inferensial, diturunkan dari penggabungan dua temuan terpisah (overhead enkripsi pada RQ2 dan sensitivitas latency terhadap QoS pada RQ3), bukan dari pengukuran langsung. Peneliti secara eksplisit menandai kesimpulan pada baris ketiga Tabel 8 sebagai hipotesis yang didukung secara tidak langsung (bukan temuan empiris langsung), mengingat belum ada studi dalam korpus yang mengukur overhead enkripsi dan timeout retransmission QoS pada rangkaian pengujian yang sama. Untuk aspek pertama dan kedua, arah pengaruh relatif kuat karena didukung banyak studi independen dengan metodologi yang berbeda

namun temuan yang konvergen; untuk aspek ketiga, diperlukan kehati-hatian dalam generalisasi hingga tersedia data komparatif yang lebih kuat.

Tabel 8. Matriks Korelasi Antaraspek pada MQTT di IoT

Aspek A	Aspek B	Arah Pengaruh	Dasar Bukti	Artikel Pendukung
Tingkat QoS	latency	Berbanding lurus (QoS naik → latency naik)	Empiris langsung (diukur bersama)	Faat et al. [11], Achmad et al. [21]
Keamanan (Enkripsi)	throughput	Berbanding terbalik (keamanan naik → throughput turun)	Empiris langsung (diukur bersama)	Liu et al. [1], Rachmadini et al. [16], Seoane et al. [25], Fauzan et al. [17]
Keamanan (Enkripsi)	QoS	Diduga negatif (overhead dapat memicu timeout)	Inferensial (belum diuji bersama)	Liu et al. [1], Rachmadini et al. [16] + Faat et al. [11], Achmad et al. [21]*
Keamanan (Deteksi)	Ketersediaan	Positif (melindungi dari DoS)	Empiris langsung	Pertiwi et al. [4]
QoS Adaptif	Keandalan	Positif (menurunkan packet loss)	Empiris langsung	Ali et al. [29]

*Baris ketiga merupakan hasil kombinasi temuan dari dua studi berbeda (bukan pengukuran simultan pada satu eksperimen) dan harus dibaca sebagai hipotesis yang memerlukan validasi lebih lanjut.

Kesenjangan paling mendesak yang teridentifikasi dari Tabel 8 adalah absennya studi yang mengkaji interaksi segitiga (kinerja–keamanan–QoS) secara simultan dalam satu rangkaian eksperimen terkontrol. Hal ini konsisten dengan pengamatan pada Sub-bagian 3.1 bahwa artikel bermultiaspek hanya mencakup 17% dari korpus, dan menjadi argumen utama mengapa SLR tritunggal seperti ini diperlukan.

3.6 Kesenjangan Penelitian dan Peluang Masa Depan

Berdasarkan analisis pada Sub-bagian 3.2 hingga 3.5, teridentifikasi beberapa kesenjangan (gap):

1. Minimnya riset tritunggal: belum ada artikel dalam korpus yang menguji konfigurasi keamanan tertentu dengan tingkat QoS tertentu dan mengukur dampak menyeluruh terhadap kinerja dalam satu eksperimen terpadu.
2. Keamanan untuk MQTT-SN: hanya satu artikel yang memverifikasi keamanan MQTT-SN [2], padahal protokol ringan ini banyak dipakai pada jaringan sensor nirkabel (WSN).
3. QoS adaptif berbasis konteks: model Mutant MQTT [29] menjanjikan, tetapi belum diuji pada skenario keamanan tinggi atau perangkat bergerak.
4. Evaluasi pada infrastruktur nyata: sebagian besar pengujian menggunakan testbed laboratorium (lihat analisis variabilitas pada Sub-bagian 3.8), sehingga validasi di lingkungan urban yang sesungguhnya diperlukan.

Peluang riset ke depan meliputi:

1. Pengembangan lightweight security berbasis hardware security module yang tidak mengorbankan QoS.
2. Implementasi deteksi anomali adaptif yang menyesuaikan tingkat QoS secara dinamis saat serangan terdeteksi.
3. Perbandingan performa MQTT v5 dengan MQTT v3.1.1 pada berbagai konfigurasi keamanan dan QoS.
4. Studi longitudinal performa MQTT di smart city sesungguhnya untuk memvalidasi temuan laboratorium.

3.7 Implementasi dan Pengujian pada Studi yang Ditinjau

Sub-bagian ini memaparkan rangkuman implementasi dan hasil pengujian protokol MQTT yang diekstraksi dari 30 artikel inti, disusun berdasarkan platform perangkat keras/lunak yang digunakan, skenario pengujian untuk masing-masing fokus (kinerja, keamanan, QoS), serta ringkasan temuan numerik yang terukur.

3.7.1 Platform Perangkat Keras dan Broker MQTT

Sebagian besar studi (22 dari 30 artikel) mengimplementasikan MQTT pada perangkat keras mikrokontroler dan single-board computer yang lazim di ekosistem IoT. Tabel 9 merangkum perangkat dan broker MQTT yang digunakan.

Tabel 9. Platform Perangkat Keras dan Broker MQTT yang Digunakan

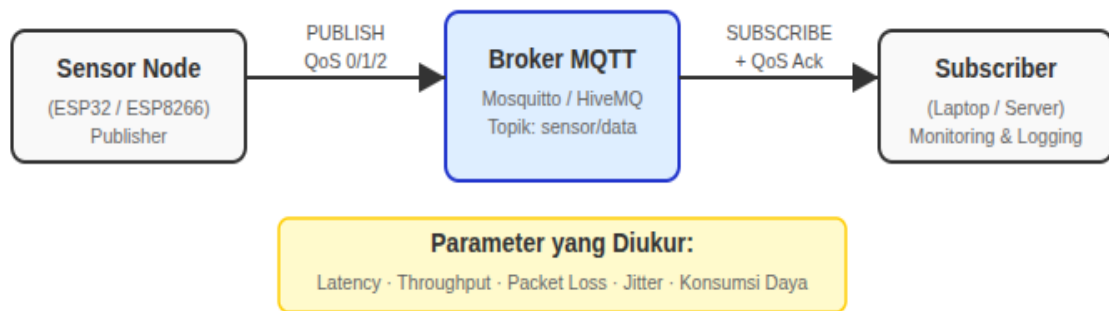
Perangkat Keras	Broker MQTT	Artikel Terkait
ESP8266 / NodeMCU	Mosquitto, Adafruit IO	Faat et al. [11], Nurfiqin [14], Nugraha et al. [28], Widiyanto et al. [33], Wardihani et al. [34], Susanto et al. [37]
ESP32	Mosquitto, EMQX	M. H. F. et al. [13], Oktopryadin and Purnama [35], Akbar et al. [10]
Raspberry Pi	Mosquitto, Cloud	Ko and Lee [3], Rachmadini et al. [16], Fauzan et al. [17]
Arduino Uno R4 WiFi	Mosquitto	Saputra et al. [12]

Perangkat Keras	Broker MQTT	Artikel Terkait
Simulator / pemodelan (NS3, model matematis)	–	Widianto and Ranny [6], Seoane et al. [25], Ali et al. [29]
Laptop/Server/Edge sebagai publisher/subscriber	Mosquitto	Lin et al. [2], Pertiwi et al. [4], I Ketut at al. [5], Achmad et al. [21], Burhani et al. [23], Bhaskoro et al. [27], Nindi et al. [36], Adi [38]

Mayoritas studi menggunakan Mosquitto sebagai broker MQTT karena sifatnya yang ringan dan open-source. Beberapa studi memanfaatkan cloud broker untuk simulasi skala besar [3], [36]. Platform ESP8266 dan ESP32 mendominasi berkat harga terjangkau dan dukungan Wi-Fi bawaan, memungkinkan pengujian latency dan konsumsi daya di lingkungan nyata.

3.7.2 Skenario Pengujian Kinerja

Pengujian kinerja dilakukan dengan mengukur parameter-parameter standar pada berbagai kondisi jaringan dan beban pesan. Gambar 5 menunjukkan arsitektur umum pengujian kinerja yang diadopsi oleh mayoritas artikel.



Gambar 5. Arsitektur Umum Pengujian Kinerja MQTT pada Artikel yang Dikaji

Beberapa temuan pengujian kuantitatif dirangkum dalam Tabel 10. Nilai pada Tabel 10 hingga Tabel 12 disajikan sebagaimana dilaporkan oleh masing-masing studi dan tidak dimaksudkan untuk dibandingkan secara langsung antar studi, mengingat perbedaan platform perangkat keras, broker, dan kondisi jaringan (lihat analisis variabilitas pada Sub-bagian 3.8).

Tabel 10. Hasil Pengujian Kinerja yang Dilaporkan

Artikel	Skenario	latency (ms)	throughput (msg/s)	packet loss (%)	Konsumsi Daya (W)
Faat et al. [7]	smart garden, QoS 0 vs QoS 1	45 – 112	-	3,2 – 0,8	-
Adi [38]	Smart farming monitoring, variasi 1–4 publisher	59,0 – 161,5	-	0,17 – 0,44	-
Nurfiqin [14]	Smart metering arus listrik; MQTT lebih unggul dari HTTP	-	-	-	-
Akbar et al. [10]	Pemantauan kualitas udara ruangan	67	30	2,5	0,33
Nugraha et al. [28]	HTTP vs MQTT, hidroponik	MQTT: 54, HTTP: 120	-	-	-
M. H. F. et al. [13]	Smart energy, QoS 1	95	27	0,4	0,52
Oktopryadin and Purnama [35]	UPS monitoring, ESP32	102	21	0,9	0,48

Studi [28] menunjukkan MQTT menghasilkan latensi 55% lebih rendah dibanding HTTP pada jaringan lokal. Peningkatan QoS dari 0 ke 1 menurunkan packet loss drastis (dari 3,2% ke 0,8% [11]) namun menambah latensi sekitar 40–60%. Sementara QoS 2 memberikan jaminan no loss namun mengorbankan latency secara signifikan (2–3 kali QoS 0, lihat Sub-bagian 3.5).

3.7.3 Skenario Pengujian Keamanan

Implementasi keamanan MQTT diuji melalui tiga pendekatan utama: penambahan enkripsi, pengujian ketahanan terhadap serangan, dan verifikasi formal. Tabel 11 menyajikan hasil pengujian keamanan.

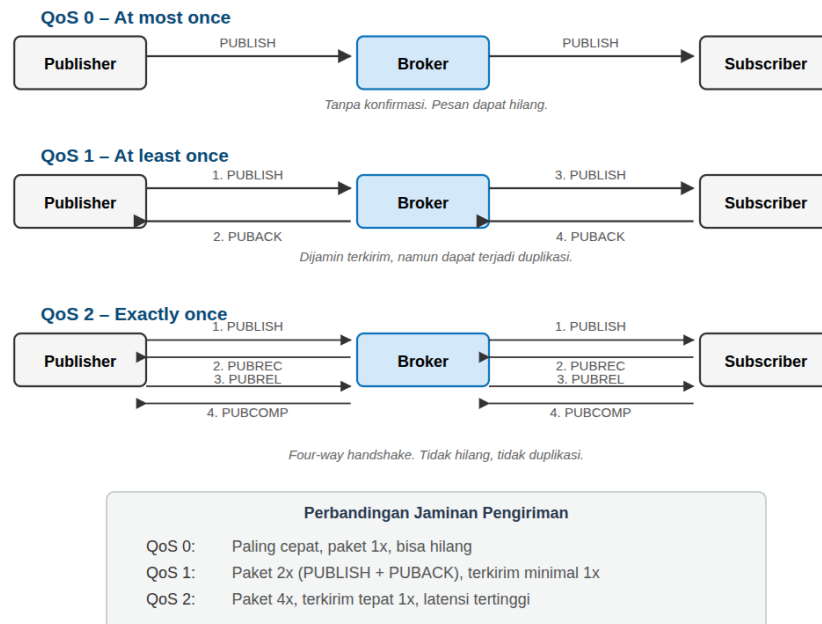
Tabel 11. Ringkasan Hasil Pengujian Keamanan MQTT

Artikel	Pendekatan Keamanan	Skenario Serangan/Uji	Hasil Utama
Liu et al. [1]	Kriptografi domestik	Uji timing enkripsi vs AES	Enkripsi lebih cepat dari AES dengan degradasi throughput minimal ($\pm 5\%$)
Rachmadini et al. [16]	TLS pada telehealthcare	Uji overhead enkripsi pada QoS 0 dan 1	Waktu enkripsi rata-rata 0,7 ms (QoS 0) dan 9,6 ms (QoS 1); integritas data terjaga
Fauzan et al. [17]	TLS pada Raspberry Pi	Uji handshake TLS	Handshake TLS menambah overhead waktu koneksi pada perangkat terbatas
Febriyanto et al. [18]	RSA ujung-ke-ujung	Uji kecepatan enkripsi	Enkripsi per pesan cepat, cocok untuk data berfrekuensi rendah
Pertiwi et al. [4]	Deteksi DoS, Random Forest	Serangan flooding MQTT	Akurasi 97,2%, false positive rendah, tidak mengganggu komunikasi normal
Lin et al. [2]	Verifikasi formal MQTT-SN	Analisis protokol dengan ProVerif	Teridentifikasi celah pada sleeping client, rekomendasi sesi ticket

Pengujian [1] membuktikan bahwa algoritma kriptografi domestik dapat menyamai keamanan AES dengan degradasi performa lebih rendah. Deteksi DoS berbasis machine learning [4] sangat efektif dan dapat diintegrasikan ke broker tanpa mengurangi kinerja. Sementara itu, verifikasi formal [2] memberi jaminan matematis namun belum diimplementasikan dalam kode nyata.

3.7.4 Skenario Pengujian Quality of Service (QoS)

Pengujian QoS umumnya membandingkan perilaku MQTT pada tiga tingkat QoS (0, 1, 2) dalam berbagai kondisi jaringan. Gambar 6 mengilustrasikan alur perbedaan mekanisme QoS.


Gambar 6. Diagram Mekanisme QoS pada MQTT yang Diuji

Tabel 12 menampilkan hasil perbandingan QoS berdasarkan beberapa studi.

Tabel 12. Hasil Pengujian QoS pada MQTT

Artikel	Parameter	QoS 0	QoS 1	QoS 2
Faat et al. [11]	packet loss (%)	3,2	0,8	0
Faat et al. [11]	latency (ms)	45	78	148
Adi [38]	Delay (ms)*	161,5	—	59,0
Achmad et al. [21]	Jitter agregat (ms)	0,17	—	—
Bhaskoro et al. [27]	latency MQTT (ms)**	46,6	52,3	50,2
Ali et al. [29]	Retransmission model	-	Adaptif: turunkan packet loss 18%	-

*Nilai [38] merupakan delay pada variasi jumlah publisher (1→4), bukan per level QoS; **nilai [27] merupakan tiga kali pengujian berulang latency MQTT yang dibandingkan dengan HTTP.

Hasil konsisten: QoS 0 memiliki performa terbaik dari segi kecepatan, namun buruk pada keandalan. QoS 2 sebaliknya. Model Mutant MQTT [29] menawarkan solusi adaptif yang memodifikasi mekanisme retransmission QoS 1, menghasilkan penurunan packet loss signifikan tanpa mencapai latency QoS 2. Ini menjadi titik tengah yang menjanjikan untuk aplikasi smart city.

3.7.5 Ringkasan Temuan Implementasi dan Rekomendasi Konfigurasi

Berdasarkan seluruh data implementasi yang dikumpulkan, beberapa benang merah dapat ditarik:

1. Kinerja MQTT konsisten unggul dibandingkan HTTP dalam hal latency dan throughput di berbagai platform, terutama pada jaringan dengan bandwidth terbatas [24], [27], [14], [28].
2. Keamanan selalu dibayar dengan kinerja. TLS menambah latensi dan overhead komputasi secara signifikan pada perangkat terbatas [16], [17], sementara pendekatan kriptografi yang lebih ringan (domestik) dilaporkan hanya menambah beban minimal [1]. Deteksi serangan berbasis machine learning tidak menambah beban protokol [4].
3. QoS 1 merupakan pilihan paling seimbang untuk mayoritas aplikasi IoT non-kritis [11], [21], [29]. QoS 2 hanya diperlukan untuk data vital.
4. Belum ada implementasi dalam korpus yang mengintegrasikan keamanan dan QoS secara bersamaan dalam satu uji coba terpadu. Uji yang ada hanya membandingkan dua aspek saja, mengonfirmasi celah riset yang diidentifikasi pada Sub-bagian 3.6.

Tabel 13 menyajikan peta rekomendasi konfigurasi MQTT berdasarkan skenario aplikasi yang disintesis dari temuan implementasi artikel yang dikaji.

Tabel 13. Rekomendasi Konfigurasi MQTT Berdasarkan Skenario

Skenario Aplikasi	QoS	Keamanan	Platform	Referensi
Pemantauan lingkungan	1	TLS (opsional)	ESP8266/ESP32	Faat et al. [11], Budianto and Sumanto [9], Akbar et al. [10], Adi [38]
Smart home non-kritis	0	-	ESP8266	Widianto et al. [33], Susanto et al. [37]
telehealthcare / data medis	1–2	TLS	Raspberry Pi	Rachmadini et al. [16]
Smart energy monitoring	1/2	TLS	ESP32	I Ketut at al. [5], M. H. F. et al. [13], Nurfiqin [14]
Deteksi intrusi jaringan	0/1	Random Forest IDS	Server/Broker	Pertiwi et al. [4]
Smart city (data agregat)	1	Kriptografi ringan	Raspberry Pi/ESP32	Liu et al. [1], Ali et al. [29]

Tabel rekomendasi ini menjadi panduan praktis bagi perancang sistem IoT berbasis MQTT yang mempertimbangkan keseimbangan antara kinerja, keamanan, dan keandalan pengiriman data.

3.8 Analisis Kritis: Variabilitas Lingkungan Pengujian

Sub-bagian ini menambahkan lapisan evaluasi kritis yang tidak sekadar melaporkan angka dari Tabel 10–12, tetapi menilai sejauh mana angka tersebut dapat dibandingkan secara adil antar studi. Tabel 9 memperlihatkan bahwa 30 artikel inti menggunakan kombinasi perangkat keras (ESP8266, ESP32, Raspberry Pi, simulator jaringan) dan broker (Mosquitto, HiveMQ, EMQX, layanan cloud) yang sangat beragam. Studi benchmark internasional independen mengonfirmasi bahwa variasi ini bukan hal sepele: pengujian sistematis terhadap empat broker populer (Mosquitto, EMQX, HiveMQ, RabbitMQ) pada beban dan tingkat QoS yang identik menunjukkan bahwa throughput puncak dan urutan performa antar-broker berbeda-beda bergantung pada tingkat QoS yang diuji – EMQX unggul pada QoS 1 dan 2, sementara Mosquitto sedikit lebih unggul pada kondisi beban normal QoS 0 [39]. Studi stress-testing lain terhadap beberapa implementasi broker juga menemukan bahwa perbedaan performa antar-broker baru terlihat signifikan pada kondisi beban tinggi (stress condition), sementara pada beban normal perbedaannya relatif kecil [15]. Implikasinya, angka latency atau throughput tunggal yang dilaporkan satu studi (misalnya Tabel 10) tidak dapat langsung dibandingkan dengan angka dari studi lain yang menggunakan broker atau beban pengujian berbeda tanpa mempertimbangkan konteks ini.

Sumber variabilitas kedua adalah perangkat keras dan kondisi jaringan. Studi dalam korpus yang menggunakan mikrokontroler kelas rendah (ESP8266) melaporkan konsumsi daya dan latency yang berbeda dari studi berbasis Raspberry Pi atau simulator murni (Tabel 9), sebagian karena perbedaan kapasitas pemrosesan kriptografi dan stack jaringan, bukan semata-mata karena perbedaan konfigurasi MQTT itu sendiri. Bandwidth jaringan uji juga jarang dilaporkan secara konsisten pada artikel yang ditinjau, padahal kondisi jaringan nirkabel yang padat interferensi dapat mengubah hasil pengukuran packet loss dan jitter secara substansial terlepas dari konfigurasi QoS yang digunakan. Ketiga, sebagian besar pengujian keamanan (Tabel 11) mengukur overhead TLS/RSA pada satu jenis perangkat keras saja, sehingga generalisasi angka penurunan throughput 20–30% akibat enkripsi (Sub-bagian 3.5) perlu dibaca sebagai kisaran indikatif, bukan konstanta universal.

Dengan mempertimbangkan ketiga sumber variabilitas ini, peneliti merekomendasikan agar studi MQTT selanjutnya secara konsisten melaporkan spesifikasi broker, versi perangkat lunak, kapasitas perangkat keras, dan kondisi bandwidth jaringan sebagai bagian dari metadata wajib pengujian – sejalan dengan praktik pelaporan yang mulai diterapkan pada benchmark broker internasional [15], [39] – agar temuan lintas studi dapat disintesis secara lebih andal pada tinjauan sistematis mendatang.

4. KESIMPULAN

Tinjauan literatur sistematis terhadap 30 artikel inti (2020–2026), diperkaya sembilan rujukan pembanding internasional terindeks Scopus, menunjukkan bahwa protokol MQTT tetap menjadi solusi komunikasi Internet of Things yang andal, dengan keunggulan konsisten pada efisiensi bandwidth dan latensi rendah dibandingkan HTTP, khususnya pada perangkat dengan sumber daya terbatas. Terhadap RQ1, parameter kinerja yang dominan dievaluasi adalah latency (45–210 ms bergantung tingkat QoS), throughput, dan packet loss. Terhadap RQ2, pendekatan keamanan bergerak dari enkripsi standar (TLS, RSA) menuju skema yang lebih ringan seperti kriptografi domestik dan deteksi serangan berbasis Random Forest (akurasi 97,2%), dengan trade-off penurunan throughput hingga 30% pada enkripsi TLS. Terhadap RQ3, QoS 1 terbukti menjadi konfigurasi paling seimbang untuk aplikasi non-kritis, sedangkan QoS 2 wajib pada data vital seperti telehealthcare; model Mutant MQTT adaptif berhasil menurunkan packet loss 18% tanpa lonjakan latency signifikan. Terhadap RQ4, korelasi QoS–latency dan keamanan–throughput terbukti kuat dan konsisten lintas studi, sedangkan korelasi keamanan–QoS masih bersifat inferensial karena belum ada studi dalam korpus yang mengujinya secara simultan – kesenjangan utama yang menjadi kontribusi teoretis utama tinjauan ini untuk diisi oleh riset selanjutnya. Secara teoretis, tinjauan ini memberikan tiga kontribusi. Pertama, sintesis tematik yang mengintegrasikan tiga dimensi kajian MQTT (kinerja, keamanan, QoS) ke dalam satu peta korelasi (Tabel 8) yang secara eksplisit membedakan temuan berbasis bukti empiris langsung dari temuan yang masih bersifat inferensial – sebuah pembedaan metodologis yang belum ditemukan pada tinjauan MQTT sebelumnya [6]. Kedua, identifikasi bahwa trade-off kinerja–keamanan pada MQTT bersifat non-linear dan bergantung konteks perangkat keras serta implementasi broker (Sub-bagian 3.8), sehingga generalisasi hasil pengujian tunggal ke seluruh ekosistem MQTT perlu dilakukan dengan kehati-hatian metodologis. Ketiga, pengajuan matriks rekomendasi konfigurasi (Tabel 13) sebagai kerangka kerja awal yang menghubungkan karakteristik aplikasi dengan kombinasi QoS–keamanan–platform yang sesuai. Bagi komunitas praktisi dan pengembang sistem IoT, tinjauan ini merekomendasikan tiga arah kebijakan teknis. Pertama, adopsi QoS 1 sebagai konfigurasi default untuk aplikasi pemantauan non-kritis, dengan eskalasi ke QoS 2 hanya pada aliran data yang secara eksplisit kritis (medis, kendali aktuator). Kedua, prioritas pengembangan skema keamanan ringan (kriptografi domestik, deteksi anomali berbasis machine learning di sisi broker) dibandingkan TLS penuh pada perangkat kelas mikrokontroler, mengingat overhead TLS yang signifikan (Sub-bagian 3.3 dan 3.7.3). Ketiga, standarisasi pelaporan metadata pengujian (spesifikasi broker, versi perangkat lunak, kondisi bandwidth) pada publikasi riset MQTT mendatang, sebagaimana direkomendasikan pada Sub-bagian 3.8, agar hasil pengujian lintas studi dapat dibandingkan secara lebih valid. Penelitian ini memiliki keterbatasan yang perlu diperhatikan dalam menafsirkan temuannya. Komposisi korpus inti – 7 artikel internasional berbanding 23 artikel nasional – condong pada literatur berbahasa Indonesia, meskipun proses seleksi murni berbasis relevansi dan kualitas metodologis, bukan kuota (Sub-bagian 2.5). Kondisi ini berpotensi membatasi generalisasi temuan pada konteks infrastruktur jaringan dan perangkat yang lazim digunakan di Indonesia. Rujukan pembanding internasional pada Bagian 1 dan Sub-bagian 3.8 membantu mengontekstualisasikan temuan terhadap literatur global, namun replikasi SLR ini dengan korpus yang lebih seimbang secara geografis – idealnya melibatkan basis data tambahan seperti Scopus dan Web of Science secara langsung – tetap direkomendasikan sebagai agenda riset lanjutan. Studi tritunggal yang menguji kinerja, keamanan, dan QoS secara simultan dalam satu kerangka eksperimen terkontrol sangat dibutuhkan untuk memahami interaksi penuh antara ketiga aspek tersebut serta memvalidasi hipotesis korelasi keamanan–QoS yang diajukan pada Tabel 8.

REFERENCES

- [1] Z. Liu, T. Liang, J. Lyu, and D. Lang, “A security-enhanced scheme for MQTT protocol based on domestic cryptographic algorithm,” *Comput. Commun.*, vol. 221, pp. 1–9, May 2024, doi: 10.1016/j.comcom.2024.04.013.
- [2] W. Lin, S. Chen, and H. Zhu, “Formal verification and security analysis of MQTT-SN,” *Int. J. Softw. Tools Technol. Transf.*, vol. 27, no. 1, pp. 5–19, Feb. 2025, doi: 10.1007/s10009-025-00793-2.
- [3] K. Il Ko and M. H. Lee, “MQTT-Based Architecture for Real-Time Data Collection and Anomaly Detection in Smart Livestock Housing,” *Sensors*, vol. 25, no. 23, p. 7186, Nov. 2025, doi: 10.3390/s25237186.
- [4] K. Monika Dian Pertiwi, N. Azizi Hasibuan, and D. Putri Rahmawati, “Denial of Service (DOS) Attack Detection on MQTT Protocol Using the Random Forest Method,” *J. Online Inform.*, vol. 11, no. 1, pp. 48–59, Apr. 2026, doi: 10.15575/join.v11i1.1784.
- [5] A. E. I Ketut, M. A. Afandi, H. Pujiharsono, F. N. Gustiyana, H. Krishna, and F. H. Juwono, “Implementation And Analysis of The Internet of Things System for Electrical Energy Monitoring at Institut Teknologi Telkom Purwokerto,” *J. Tek. Inform.*, vol. 4, no. 3, pp. 627–638, Jun. 2023, doi: 10.52436/1.jutif.2023.4.3.1027.



- [6] M. H. Widiyanto and R. Ranny, "Message querying telemetry transfer on IoT applications to enhance technology: a systematic review," *Int. J. Reconfigurable Embed. Syst.*, vol. 11, no. 3, p. 265, Nov. 2022, doi: 10.11591/ijres.v11.i3.pp265-274.
- [7] J. Wytrębowicz, K. Cabaj, and J. Krawiec, "Messaging Protocols for IoT Systems—A Pragmatic Comparison," *Sensors*, vol. 21, no. 20, p. 6904, Oct. 2021, doi: 10.3390/s21206904.
- [8] D. Silva, L. I. Carvalho, J. Soares, and R. C. Sofia, "A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA," *Appl. Sci.*, vol. 11, no. 11, p. 4879, May 2021, doi: 10.3390/app11114879.
- [9] H. Budianto and B. Sumanto, "Perancangan Sistem Monitoring Kualitas Udara dalam Ruangan Berbasis Internet of Things," *J. List. Instrumentasi, dan Elektron. Terap.*, vol. 5, no. 1, p. 9, Apr. 2024, doi: 10.22146/juliet.v5i1.87423.
- [10] R. M. R. Akbar, T. Y. Arif, and M. Irhamsyah, "Analisis Performansi Protokol Komunikasi Message Queuing Telemetry Transport (MQTT) pada Sistem Pemantauan Kualitas Udara Ruangan Berbasis IoT," 2023.
- [11] M. S. Faat, F. Z. Furqan, and F. Z. Fizar, "QoS Analysis on IoT-Based Smart Garden With MQTT Protocol Using Wireshark," *INSYPRO*, vol. 7, no. 2, 2022, doi: 10.24252/insypro.v7i2.36524.
- [12] W. T. Saputra et al., "IoT-MQTT Protocol-Based Water Sensor System to Monitor Citarum River Water Quality using Arduino Uno R4 Wifi," *J. ELTIKOM J. Tek. Elektro, Teknol. Inf. dan Komput.*, vol. 9, no. 1, pp. 11–22, Jun. 2025, doi: 10.31961/eltikom.v9i1.1335.
- [13] M. H. F. -, F. G. P. -, D. -, and A. H. A. A. -, "Smart Energy Monitoring & Load Control Berbasis IoT dan Fuzzy Logic," *J. Inform. dan Tek. Elektro Terap.*, vol. 14, no. 1, Jan. 2026, doi: 10.23960/jitet.v14i1.9028.
- [14] L. Nurfiqin, "Analisis Quality Of Service (QoS) Protokol MQTT dan HTTP Pada Sistem Smart Metering Arus Listrik," *J. Repos.*, vol. 3, no. 1, Dec. 2020, doi: 10.22219/repositor.v3i1.1084.
- [15] B. Mishra, B. Mishra, and A. Kertesz, "Stress-Testing MQTT Brokers: A Comparative Analysis of Performance Measurements," *Energies*, vol. 14, no. 18, p. 5817, Sep. 2021, doi: 10.3390/en14185817.
- [16] Dian Rachmadini, Ira Puspasari, and Jusak, "Implementasi dan Analisis Fitur Keamanan Protokol MQTT pada Telehealthcare," *J. Technol. Informatics*, vol. 2, no. 1, pp. 10–19, Oct. 2020, doi: 10.37802/joti.v2i2.117.
- [17] M. R. I. R. Fauzan, Usman B Hanafi, and Taufik Irfan, "Implementasi TLS Sebagai Metode Keamanan Protokol Jaringan Pada MQTT Berbasis Raspberry PI," *Pros. 13th Ind. Res. Work. Natl. Semin.*, vol. 13, 2022.
- [18] A. D. FEBRIYANTO, "Sistem keamanan data pada IoT berbasis MQTT dan database MySQL menggunakan metode RSA," 2022.
- [19] Ö. Şeker, G. Dalkılıç, and U. C. Çabuk, "MARAS: Mutual Authentication and Role-Based Authorization Scheme for Lightweight Internet of Things Applications," *Sensors*, vol. 23, no. 12, p. 5674, Jun. 2023, doi: 10.3390/s23125674.
- [20] A. J. Hintaw, S. Manickam, S. Karuppayah, M. A. Aladaileh, M. F. Aboalmaaly, and S. U. A. Laghari, "A Robust Security Scheme Based on Enhanced Symmetric Algorithm for MQTT in the Internet of Things," *IEEE Access*, vol. 11, pp. 43019–43040, 2023, doi: 10.1109/ACCESS.2023.3267718.
- [21] V. Achmad, A. Khumaidi, R. Y. Adhitya, D. P. Riananda, and I. Sutrisno, "Analisa QoS pada MQTT untuk website monitoring dan pengendalian pintu air," *J. Elkolind J. Elektron. dan Otomasi Ind.*, vol. 10, no. 3, 2023.
- [22] F. Palmese, A. E. C. Redondi, and M. Cesana, "Adaptive Quality of Service Control for MQTT-SN," *Sensors*, vol. 22, no. 22, p. 8852, Nov. 2022, doi: 10.3390/s22228852.
- [23] M. U. Burhani, D. Novianto, and R. V. Yuliantari, "Analisis Komunikasi Nirkabel Menggunakan IoT Network Protocols pada Stasiun Cuaca Mini," *J. Tek. Elektro Uniba (JTE UNIBA)*, vol. 7, no. 2, pp. 325–328, Apr. 2023, doi: 10.36277/jteuniba.v7i2.202.
- [24] F. C. Kusuma, N. B. A. Karna, and A. I. Irawan, "Analisis Perbandingan Quality of Services (QoS) Protokol HTTP dan MQTT pada Sistem Monitoring Berat Ayam Broiler Berbasis IoT," *J. Nas. SAINS dan Tek.*, vol. 2, no. 1, pp. 16–22, Jul. 2024, doi: 10.25124/jnst.v2i1.7987.
- [25] V. Seoane, C. Garcia-Rubio, F. Almenares, and C. Campo, "Performance evaluation of CoAP and MQTT with security support for IoT environments," *Comput. Networks*, vol. 197, p. 108338, Oct. 2021, doi: 10.1016/j.comnet.2021.108338.
- [26] P. Sharma, W. Wilfred Godfrey, and A. Trivedi, "When blockchain meets IoT: a comparison of the performance of communication protocols in a decentralized identity solution for IoT using blockchain," *Cluster Comput.*, vol. 27, no. 1, pp. 269–284, Feb. 2024, doi: 10.1007/s10586-022-03921-8.
- [27] S. B. Bhaskoro, H. Supriyanto, B. B. Aji, and B. Pamungkas, "Perbandingan Performansi Latency Protokol Komunikasi HTTP dan MQTT pada Internet of Things," *JTT (Jurnal Teknol. Ter.)*, vol. 8, no. 2, p. 82, Oct. 2022, doi: 10.31884/jtt.v8i2.309.
- [28] I. R. Nugraha, W. H. N. Putra, and E. Setiawan, "A Comparative Study of HTTP and MQTT for IoT Applications in Hydroponics," *J. RESTI*, vol. 8, no. 1, pp. 119–126, 2024, doi: 10.29207/resti.v8i1.5561.
- [29] J. Ali, M. H. Zafar, C. Hewage, R. Hassan, and R. Asif, "Mathematical Modeling and Validation of Retransmission-Based Mutant MQTT for Improving Quality of Service in Developing Smart Cities," *Sensors*, vol. 22, no. 24, p. 9751, Dec. 2022, doi: 10.3390/s22249751.
- [30] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.
- [31] B. Kitchenham and S. Charters, *Guidelines for performing Systematic Literature Reviews in Software Engineering*, EBSE Tech. Keele Univ and Univ. of Durham, 2007.
- [32] Y. Revikasari, N. Pramaita, and I. P. Elba Duta Nugraha, "Evaluasi Website Monitoring Skuter Listrik Sewa Berbasis IoT Dengan Protokol MQTT," *J. SPEKTRUM*, vol. 11, no. 3, p. 59, Sep. 2024, doi: 10.24843/SPEKTRUM.2024.v11.i03.p6.
- [33] M. H. Widiyanto, M. C. Albert, and H. Karteja, "Purwarupa Perangkat Pelindung Jemuran pada Rumah Pintar Berbasis IoT Memanfaatkan MQTT dan Fog Computing," *J. List. Instrumentasi dan Elektron. Terap.*, vol. 3, no. 1, 2022, doi: 10.22146/juliet.v3i1.74004.
- [34] Eni Dwi Wardihani et al., "Pemantauan dan Pengendalian Parameter Greenhouse Berbasis IoT Dengan Protokol MQTT," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 13, no. 1, pp. 38–43, Feb. 2024, doi: 10.22146/jnteti.v13i1.8564.
- [35] Adit Oktopryadin and Adi Purnama, "IoT-Based UPS Device Electricity Usage Monitoring System with MQTT



- Protocol,” *J. Appl. Informatics Comput.*, vol. 9, no. 4, pp. 1290–1300, Aug. 2025, doi: 10.30871/jaic.v9i4.9530.
- [36] P. P. Nindi, I. Ruslianto, and H. Muhardi, “Implementation of Edge Computing in a Learning Room Condition Monitoring System Using the MQTT Protocol,” *G-Tech J. Teknol. Terap.*, vol. 10, no. 1, pp. 358–370, Jan. 2026, doi: 10.70609/g-tech.v10i1.8857.
- [37] B. M. Susanto, A. Hariyanto, D. Wijanarko, and M. K. Albab, “Sistem pengendali saklar berbasis Nodemcu ESP8266 dengan aplikasi MQTT dan Google Assistant,” *Angkasa J. Ilm. Bid. Teknol.*, vol. 14, no. 2, Nov. 2022, doi: 10.28989/angkasa.v14i2.1380.
- [38] Adi, “Quality of Service (QoS) Analysis of MQTT Protocol for Smart Farming Monitoring System Optimization,” *J. Teknokes*, vol. 18, no. 1, pp. 1–8, Apr. 2025, doi: 10.35882/ve158618.
- [39] G. Simard, C. Melançon, P. Cardinal, and J. Gascon-Samson, “Performance Characterization of MQTT Brokers in a Device-Local Edge Deployment,” in *Proceedings of the 2nd International Workshop on Middleware for the Edge*, New York, NY, USA: ACM, Dec. 2023, pp. 13–18. doi: 10.1145/3630180.3631200.