Jurnal Riset Rumpun Ilmu Teknik
Volume 5, Nomor 1, April 2026
e-ISSN : 2829-016X; p-ISSN : 2829-0178, Hal. 431-442
DOI: https://doi.org/10.55606/jurritek.v5i1.7684
Tersedia: https://prin.or.id/index.php/JURRITEK

Analisis Komparatif Keamanan dan Kinerja Protokol Komunikasi pada Web of Things: Tinjauan Sistematis terhadap HTTP, CoAP, dan MQTT

Faid Rama Daniy[1*], Mirza Putra Firmansyah[2], Arief Muhammad Luthfi Yanuar[3], Putri Safira Augusta[4], Arief Arfriandi[5]
[1-5] Universitas Negeri Semarang, Indonesia

**Penulis Korepsondenis: faidramadaniy@students.unnes.ac.id [1]*

Abstract*. The integration of the Internet of Things (IoT) into the Web of Things (WoT) offers cross-platform interoperability but presents significant security challenges for constrained devices. This study aims to evaluate the effectiveness and efficiency of security mechanisms in three major WoT protocols: HTTP, CoAP, and MQTT. The research methodology employs a Systematic Literature Review (SLR) following PRISMA guidelines, reviewing 22 selected articles published between 2020 and 2025. The analysis utilizes PICOC criteria to compare communication overhead, computational consumption, and security mechanisms such as DTLS, OSCORE, and TLS integration. The results indicate that CoAP, combined with OSCORE and EDHOC mechanisms, provides the optimal balance between energy efficiency and end-to-end security for resource-constrained devices. MQTT demonstrates superiority in throughput and data transmission speed but requires additional security layers to ensure data confidentiality. Meanwhile, HTTP dominates in terms of Web service integration and access control, despite having the highest overhead burden. In conclusion, no single protocol is superior for all scenarios; the choice of protocol in WoT architecture must be based on the trade-offs between latency, resource efficiency, and system security requirements*

Keywords: *Communication Protocols; IoT Security; MQTT; PRISMA; Web of Things.*

Abstrak. Integrasi Internet of Things (IoT) ke dalam Web of Things (WoT) menawarkan interoperabilitas lintas platform, namun menghadirkan tantangan signifikan terkait keamanan pada perangkat dengan sumber daya terbatas (constrained devices). Penelitian ini bertujuan untuk mengevaluasi efektivitas dan efisiensi keamanan pada tiga protokol utama WoT: HTTP, CoAP, dan MQTT. Metode penelitian menggunakan pendekatan Systematic Literature Review (SLR) mengikuti pedoman PRISMA, dengan menelaah 22 artikel terpilih dari rentang tahun 2020 hingga 2025. Analisis dilakukan menggunakan kriteria PICOC untuk membandingkan aspek overhead komunikasi, konsumsi komputasi, dan mekanisme keamanan seperti DTLS, OSCORE, serta integrasi TLS. Hasil penelitian menunjukkan bahwa CoAP dengan mekanisme OSCORE dan EDHOC memberikan keseimbangan terbaik antara efisiensi energi dan keamanan end-to-end untuk perangkat terbatas. MQTT terbukti unggul dalam throughput dan kecepatan transmisi data, namun memerlukan mekanisme keamanan tambahan untuk menjamin kerahasiaan data. Sementara itu, HTTP mendominasi dalam kemudahan integrasi layanan Web dan kontrol akses, meskipun memiliki beban overhead tertinggi. Kesimpulannya, tidak ada protokol tunggal yang superior untuk semua skenario; pemilihan protokol dalam arsitektur WoT harus didasarkan pada trade-off antara latensi, efisiensi sumber daya, dan kebutuhan standar keamanan sistem.

Kata kunci: Keamanan IoT; MQTT; PRISMA; Protokol Komunikasi; *Web of Things*.

1. PENDAHULUAN

Internet of Things (IoT) dan pengembangannya, yaitu Web of Things (WoT), merupakan paradigma modern yang berfokus pada integrasi perangkat fisik dengan teknologi berbasis web untuk memungkinkan komunikasi dan pertukaran data secara efisien tanpa batasan platform (Wytrębowicz dkk., 2021). Konsep WoT hadir sebagai solusi atas keterbatasan interoperabilitas pada sistem IoT konvensional dengan mengadopsi standar protokol komunikasi web seperti HTTP, CoAP, dan MQTT. Melalui pendekatan ini, perangkat dengan karakteristik dan kemampuan berbeda dapat saling berinteraksi menggunakan mekanisme berbasis web yang fleksibel dan terstandardisasi. Namun, di balik potensi besar tersebut, masih

Naskah Masuk: 21 November 2025; Revisi: 25 Desember 2025; Diterima: 29 Januari 2026; Tersedia: 02 Januari 2026

terdapat tantangan signifikan terutama dalam aspek keamanan dan performa sistem komunikasi. Isu-isu utama yang dihadapi meliputi keterbatasan sumber daya perangkat IoT seperti daya, memori, dan prosesor, serta kebutuhan akan mekanisme keamanan yang efektif untuk menjamin integritas data, autentikasi pengguna, dan enkripsi komunikasi end-to-end (Albarrak, 2024; Seoane dkk., 2021).

Berbagai penelitian terdahulu telah dilakukan untuk mengevaluasi efektivitas dan efisiensi protokol komunikasi dalam konteks WoT, baik dari sisi konsumsi energi, latensi transmisi, maupun tingkat keamanannya. Beberapa studi menunjukkan bahwa protokol CoAP memiliki keunggulan dalam hal efisiensi bandwidth dan cocok digunakan pada perangkat dengan kapasitas terbatas, sedangkan MQTT unggul dalam komunikasi berbasis publish/subscribe yang memerlukan keandalan tinggi dan skalabilitas besar. Di sisi lain, HTTP masih banyak digunakan karena kompatibilitasnya yang luas dengan infrastruktur web modern, meskipun memiliki beban komunikasi yang relatif tinggi dibandingkan protokol lainnya (Albarrak, 2024; Silva dkk., 2021). Oleh karena itu, diperlukan analisis komprehensif yang tidak hanya membandingkan performa teknis ketiga protokol tersebut, tetapi juga menilai sejauh mana mekanisme keamanan seperti TLS, DTLS, dan OSCORE dapat diimplementasikan secara efektif pada perangkat dengan keterbatasan sumber daya. Kajian ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem WoT yang lebih aman, efisien, dan adaptif terhadap kebutuhan masa depan.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini mengikuti pedoman Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Penerapan PRISMA bertujuan untuk memastikan proses identifikasi, penyaringan, dan inklusi artikel dilakukan secara sistematis, transparan, dan dapat direplikasi, dengan fokus pada studi yang membahas keamanan protokol komunikasi dalam konteks Internet of Things (IoT) atau Web of Things (WoT).

Protokol dan Kriteria Kelayakan

Protokol untuk review ini dikembangkan untuk mendefinisikan secara spesifik kriteria kelayakan, strategi pencarian, dan metode sintesis data. Selanjutnya kriteria inklusi dan eksklusi ditetapkan untuk memfokuskan review pada literatur yang membahas implementasi keamanan untuk protokol komunikasi ringan dalam IoT maupun WoT. Kriteria tersebut dipertimbangkan dengan menggunakan metode PICOC sebagai acuan, tabel 1 memberikan penjelasan bagaimana PICOC di implementasikan.

Tabel 1. Identifikasi PICOC.

Kriteria	kategori
P (Population)	IoT atau WoT
I (Intervention)	penggunaan HTTP, CoAP, atau MQTT
C (Comparison)	perbandingan HTTP, CoAP, dan MQTT dalam WoT
O (Outcome)	Melaporkan tentang komunikasi yang aman, protokol keamanan (security protocol), enkripsi, atau autentikasi
C (Context)	Web of Things (WoT)

Dengan begitu penelitian ini berfokus pada dua pertanyaan utama yaitu, RQ1: Apa saja protokol komunikasi yang digunakan untuk menjamin keamanan dalam lingkungan Web of Things (WoT)? RQ2: Di antara protokol tersebut, bagaimana perbandingan protokol HTTP, CoAP, dan MQTT dalam aspek kinerja dan keamanan pada sistem WoT?

Strategi Pencarian Informasi

Pencarian literatur dilakukan secara ekstensif pada basis data elektronik utama yang relevan dengan bidang ilmu komputer dan teknik. Basis data yang digunakan adalah Scopus dan Science Direct. Kata kunci yang digunakan dalam proses pencarian dilakukan dengan menggunakan operator logika AND dan OR, berikut variasi pencarian dilakukan:
("Web of Things" OR WoT OR "Internet of Things" OR IoT) AND (HTTP OR CoAP OR MQTT) AND ("secure communication" OR "security protocol" OR DTLS OR OSCORE OR encryption OR authentication)

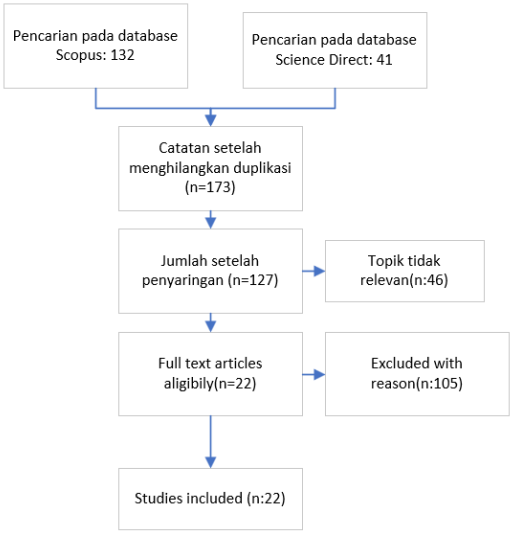
Pencarian dilakukan pada rentang waktu tahun 2020–2025, untuk memastikan bahwa artikel yang dipilih merepresentasikan perkembangan terkini dari topik keamanan komunikasi di WoT. Selain itu, hanya artikel yang ditulis dalam bahasa Inggris dan tersedia dalam bentuk lengkap (full text) yang dipertimbangkan.

Kriteria Inklusi dan Esklusi

Proses seleksi dilakukan menggunakan kriteria PICOC (Population, Intervention, Comparison, Outcomes, Context). Artikel yang dilihat menggunakan beberapa kategori Inklusi yaitu studi yang membahas penerapan atau evaluasi keamanan pada HTTP, CoAP, atau MQTT, artikel yang mengimplementasikan atau membandingkan mekanisme keamanan DTLS atau OSCORE, artikel yang menyajikan hasil evaluasi kinerja, efisiensi, atau efektivitas keamanan. Selanjutnya juga mengeklusi kategori artikel yang tidak fokus pada aspek keamanan komunikasi, publikasi non-ilmiah seperti white paper, editorial, atau laporan teknis internal, dan studi yang hanya membahas TLS tanpa relevansi terhadap WoT atau perangkat terbatas.

Protokol dan Kriteria Kelayakan

Prosedur seleksi mengikuti empat tahap utama sesuai panduan PRISMA, dumilai dengan Identifikasi (*Identification*) untuk mengumpulkan semua artikel potensial dari hasil pencarian awal di basis data. Selanutnya tahap Penyaringan (*Screening***)** untuk Menghapus artikel duplikat dan menyeleksi berdasarkan judul dan abstrak. Dilanjut tahap Kelayakan (*Eligibility*) yaitu dengan membaca teks penuh untuk menilai kesesuaian dengan kriteria inklusi. Terakhir tahap Inklusi (*Inclusion*) yaitu Menentukan artikel akhir yang layak untuk dianalisis lebih lanjut.



Gambar 1. Diagram Prisma.

Protokol dan Kriteria Kelayakan

Setiap artikel yang lolos seleksi diekstraksi berdasarkan beberapa parameter, antara lain: (a) Protokol komunikasi yang digunakan (HTTP, CoAP, MQTT, atau lainnya). (b) Mekanisme keamanan yang diterapkan (TLS, DTLS, OSCORE, atau protokol tambahan). (c) Metode evaluasi (simulasi, implementasi eksperimental, atau analisis teoretis). (d) Parameter evaluasi (latensi, throughput, overhead, konsumsi energi, tingkat keamanan). (e) Temuan utama terkait efektivitas dan efisiensi sistem.

Analisis dilakukan secara deskriptif dan komparatif, untuk mengidentifikasi tren, tantangan, serta celah penelitian (*research gap*) antara penerapan DTLS dan OSCORE pada ketiga protokol WoT. Hasil akhir pencarian didapat 23 artikel yang digunakan sebagai tinjauan sistematis.

3. HASIL DAN PEMBAHASAN

Protokol Komunikasi yang Digunakan dalam Lingkungan Web of Things (WoT)

Untuk mempermudah perujukan artikel yang dilakukan studi, dibuatkan tabel 2 yang berisi rujukan, judul artikel, serta refrensi terkait.

Tabel 2. Artikel Tinjauan.

No	Judul	Refrensi
[1]	Lightweight and secure mutual authentication scheme for IoT devices using CoAP protocol	(Oliver & Purusothaman, 2022)
[2]	The Cost of OSCORE and EDHOC for Constrained Devices	(Hristozov dkk., 2021)
[3]	UIP2SOP: A Unique IoT Network applying Single Sign-On and Message Queue Protocol	(Thanh dkk., 2021)
[4]	A Multi-Tier MQTT Architecture with Multiple Brokers Based on Fog Computing for Securing Industrial IoT	(Kurdi & Thayananthan, 2022)
[5]	A Novel MQTT 5.0-Based Over-the-Air Updating Architecture Facilitating Stronger Security	(Chien & Wang, 2022)
[6]	Automatic Key Update Mechanism for Lightweight M2M Communication and Enhancement of IoT Security: A Case Study of CoAP Using Libcoap Library	(Tsai dkk., 2022)
[7]	BMDD: A novel approach for IoT platform (broker-less and microservice architecture, decentralized identity, and dynamic transmission messages)	(Nguyen dkk., 2022)
[8]	Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things	(Gong & Feng, 2022)
[9]	A Robust Security Scheme Based on Enhanced Symmetric Algorithm for MQTT in the Internet of Things	(Hintaw dkk., 2023)
[10]	Design and Implementation of Efficient IoT Authentication Schemes for MQTT 5.0	(H. Y. Chien & Ciou, 2023)
[11]	On the Efficiency of a Lightweight Authentication and Privacy Preservation Scheme for MQTT	(Tian & Vassilakis, 2023)
[12]	Implementation of Http Security Protocol for Internet of Things Based on Digital Envelope	(Insan & Samopa, 2024)
[13]	Designing a Secure and Scalable Service Agent for IoT Transmission through Blockchain and MQTT Fusion	(Hsu, 2024)
[14]	Broken-Stick Regressive Lightweight Speck Cryptographic Constrained Application Protocol for Data Security in IoT Aware Smart Home	(Subhashini & Jyothi, 2024)
[15]	Enabling Lightweight Device Authentication in Message Queuing Telemetry Transport Protocol	(Narasimha Swamy dkk., 2024)
[16]	Enhancing MQTT-SN Security with a Lightweight PUF-Based Authentication and Encrypted Channel Establishment Scheme	(Gong dkk., 2024)
[17]	Secure Communication for the IoT: EDHOC and (Group) OSCORE Protocols	(Höglund dkk., 2024)
[18]	MQTT-PRESENT: Approach to secure internet of things applications using MQTT protocol	(Sahmi dkk., 2021)
[19]	CoAP/DTLS Protocols in IoT Based on Blockchain Light Certificate	(Khoury dkk., 2025)
[20]	DLKS-MQTT: A Lightweight Key Sharing Protocol for Secure IoT Communications	(Kaganurmath dkk., 2025)
[21]	Enabling Robust Security in MQTT-Based IoT Networks with Dynamic Resource-Aware Key Sharing	(Kaganurmath & Cholli, 2025)
[22]	HECS4MQTT: A Multi-Layer Security Framework for Lightweight and Robust Encryption in Healthcare IoT Communications	(Alharbi dkk., 2025)

Berdasarkan hasil penelaahan terhadap 23 studi, terdapat beberapa kelompok protokol komunikasi yang digunakan untuk menjamin keamanan dalam lingkungan Web of Things (WoT). Klasifikasi protokol komunikasi yang digunakan dalam studi-studi terkait keamanan

Web of Things (WoT) dapat dilihat pada Tabel 2. Pertama, protokol CoAP dan variasinya, termasuk CoAP-DTLS, OSCORE, dan EDHOC, muncul pada tujuh studi ([1], [6], [8], [14], [19], [2], [17]). Kelompok ini menekankan mekanisme keamanan berbasis application-layer encryption dan lightweight key exchange yang mampu beroperasi pada perangkat terbatas sambil mempertahankan end-to-end security, termasuk dalam lingkungan yang melibatkan proxy. Kedua, protokol MQTT, MQTT 5.0, dan MQTT-SN mendominasi dengan tiga belas studi ([4], [5], [7], [9], [10], [11], [13], [15], [16], [18], [20], [21], [22]), menunjukkan bahwa ekosistem WoT banyak mengandalkan arsitektur publish–subscribe yang ringan. Upaya pengamanan dalam kelompok ini umumnya meliputi peningkatan autentikasi, manajemen kunci dinamis, enkripsi payload, serta integrasi dengan kerangka keamanan modern seperti PUF, blockchain, dan OAuth2. Ketiga, protokol HTTP dan mekanisme Web-based security seperti OAuth2 muncul pada tiga studi ([12], [3], [7]), terutama digunakan pada sistem WoT yang lebih dekat dengan arsitektur Web tradisional atau yang mengadopsi Single Sign-On untuk kontrol akses terpusat. Selain itu, dua studi ([13], [19]) menggabungkan protokol komunikasi dengan mekanisme blockchain-enhanced communication untuk memberikan integritas, non-repudiation, serta model manajemen kunci yang lebih terdistribusi. Terakhir, tiga studi ([7], , [22]) berfokus pada platform keamanan dan arsitektur non-protokol, yaitu pendekatan yang tidak mengusulkan protokol baru, tetapi membangun kerangka kerja, identitas terdesentralisasi, atau mekanisme pelacakan untuk memperkuat keamanan tingkat sistem.

Secara keseluruhan, hasil klasifikasi menunjukkan bahwa ekosistem WoT mencakup berbagai lapisan pendekatan keamanan, mulai dari protokol komunikasi yang benar-benar lightweight (seperti CoAP/OSCORE/EDHOC), protokol publish–subscribe yang diperkuat (MQTT/MQTT-SN), protokol berbasis Web, hingga integrasi teknologi modern seperti blockchain dan microservice-based security frameworks. Keragaman ini menegaskan bahwa tidak ada satu protokol tunggal yang dominan, melainkan kombinasi pendekatan yang disesuaikan dengan kebutuhan perangkat, beban komputasi, dan tingkat keamanan yang diperlukan dalam lingkungan WoT.

Tabel 3. Klasifikasi Protokol Komunikasi Keamanan WoT.

Protokol Komunikasi	Frekuensi	Studi yang dikaji
CoAP / CoAP-DTLS / OSCORE / EDHOC	7	[1], [6], [8], [14], [19], [2], [17]
MQTT / MQTT 5 / MQTT-SN	13	[4], [5], [7], [9], [10], [11], [13], [15], [16], [18], [20], [21], [22]
HTTP / Web (OAuth2, Web-based security)	3	[12], [3], [7]
Blockchain-enhanced communication	2	[13], [19]
Security platform / Arsitektur non-protokol	3	[7], , [22]

Perbandingan protocol HTTP, CoAP, dan MQTT dalam aspek kinerja dan keamanan pada system WoT

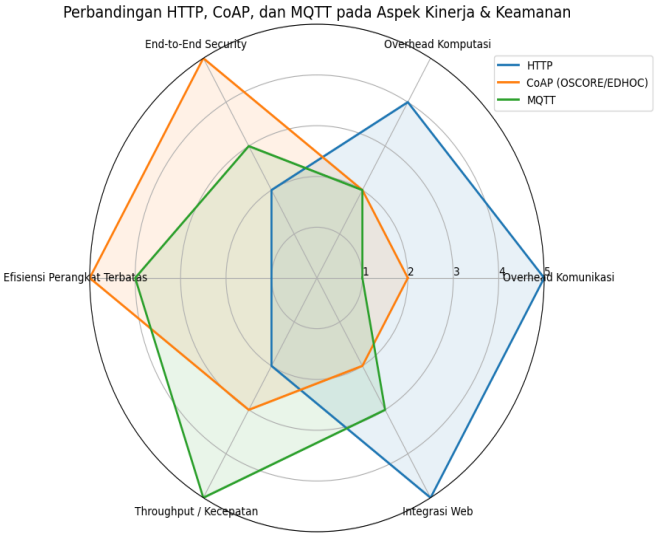
Berdasarkan 23 studi yang dianalisis, HTTP, CoAP, dan MQTT menempati posisi yang berbeda dalam spektrum kinerja dan keamanan pada sistem Web of Things (WoT). HTTP pada dasarnya bukan dirancang untuk perangkat sangat terbatas, tetapi tetap digunakan pada beberapa skenario WoT yang lebih dekat dengan arsitektur Web tradisional. Studi [12] menunjukkan bahwa HTTP membutuhkan mekanisme tambahan seperti digital envelope untuk menyediakan kerahasiaan, integritas, autentikasi, dan non-repudiation, yang pada akhirnya meningkatkan overhead komputasi dan ukuran pesan. Studi [3] dan [7] juga menambahkan bahwa HTTP sering dikombinasikan dengan OAuth2 atau SSO sehingga perannya cenderung berada pada kontrol akses dan manajemen layanan, sementara komunikasi sensor-ke-sensor dialihkan ke protokol yang lebih ringan seperti MQTT atau CoAP. CoAP, di sisi lain, dirancang khusus untuk jaringan terkendala. Studi [1], [6], [8], dan [14] menegaskan efisiensi CoAP dalam ukuran pesan dan dukungan multicast, sementara lapisan keamanan OSCORE dan EDHOC yang dibahas pada [2] dan [17] memperkuat kemampuan CoAP dalam menyediakan keamanan end-to-end yang ringan dan tetap stabil meskipun melalui proxy. MQTT, dengan model publish–subscribe-nya, mendominasi dari sisi kinerja komunikasi. Studi [3] menunjukkan bahwa MQTT mampu mengirim pesan hingga dua kali lebih cepat dibanding CoAP, namun keamanan bawaan MQTT terbatas sehingga berbagai studi lain ([9], [11], [15], [16], [20]–[21]) berfokus pada penambahan enkripsi simetris ringan, autentikasi token, PUF, hingga manajemen kunci dinamis.

Tabel 4. Skor Perbandingan antar Protokol.

Aspek Penilaian	HTTP	CoAP (OSCORE/EDHOC)	MQTT
Overhead Komunikasi	5	2	1
Overhead Komputasi	4	2	2
End-to-End Security	2	5	3
Efisiensi Perangkat Terbatas	1	5	4
Throughput / Kecepatan	2	3	5
Integrasi Web	5	2	3

Untuk merangkum kecenderungan performa dan keamanan ketiga protokol tersebut secara lebih terstruktur, Tabel 3 menyajikan skor komparatif berdasarkan enam aspek utama yang paling sering dibahas pada literatur, yaitu overhead komunikasi, overhead komputasi, kemampuan end-to-end security, efisiensi perangkat terbatas, throughput, dan integrasi Web.

Penyajian tabel ini memberikan gambaran kuantitatif yang ringkas mengenai kekuatan dan kelemahan masing-masing protokol sebelum analisis mendalam dilakukan. Melengkapi tabel tersebut, Gambar 2 memvisualisasikan pola skor tersebut sehingga hubungan antar-aspek dapat terlihat secara intuitif. Visualisasi ini membantu memperjelas karakteristik utama ketiga protokol: HTTP menonjol dalam integrasi Web namun memiliki overhead terbesar, CoAP mencapai keseimbangan terbaik antara efisiensi dan keamanan, sementara MQTT unggul secara signifikan pada throughput namun memerlukan mekanisme keamanan tambahan.



Gambar 2. Perbandingan Protokol.

Rincian tersebut tampak konsisten dengan temuan mendalam dari literatur. HTTP memperoleh skor tertinggi pada integrasi Web, sejalan dengan penggunaannya sebagai protokol yang kompatibel dengan ekosistem layanan modern dan mekanisme autentikasi berbasis Web. Namun, skor overhead komunikasi dan komputasi yang tinggi menguatkan hasil studi [12], [3], dan [7] bahwa HTTP kurang relevan untuk perangkat IoT yang memiliki keterbatasan memori, energi, dan kebutuhan komunikasi real-time. Sementara itu, CoAP memperoleh skor terbaik dalam efisiensi perangkat terbatas serta keamanan end-to-end berkat OSCORE dan EDHOC. Hal ini sesuai dengan hasil studi [2] dan [17] yang menunjukkan bahwa EDHOC mampu menekan biaya handshake secara signifikan dibanding DTLS, sekaligus mempertahankan skema enkripsi yang kuat pada tingkat aplikasi. Dengan demikian, CoAP terbukti sebagai protokol RESTful yang paling stabil dan aman untuk lingkungan dengan perangkat yang sangat terbatas sumber dayanya.

MQTT, sebagaimana tercermin pada skor throughput yang tinggi dalam Tabel 3 dan pola grafik radar, memperlihatkan kemampuan komunikasi yang unggul dalam skenario event-driven berskala besar. Studi [3] menunjukkan bahwa kecepatan pengiriman MQTT secara

konsisten melampaui CoAP. Meskipun skor keamanan MQTT tidak sekuat CoAP, penelitian seperti [9], [18], [11], dan [15] membuktikan bahwa kelemahan ini dapat diatasi menggunakan skema keamanan berbasis enkripsi ringan, autentikasi sekali pakai, atau pendekatan berbasis PUF seperti pada [16]. Beberapa studi lainnya ([20], [21]) juga menekankan bahwa mekanisme manajemen kunci dinamis dapat meningkatkan fleksibilitas dan ketahanan MQTT tanpa mengorbankan performa komunikasi.

Secara keseluruhan, integrasi antara analisis literatur, Tabel 3, dan Gambar 2 menunjukkan bahwa ketiga protokol memainkan peran yang saling melengkapi dalam ekosistem WoT. HTTP unggul dalam integrasi layanan Web dan mekanisme otorisasi tingkat aplikasi, CoAP paling cocok untuk perangkat sangat terkendala yang membutuhkan keamanan end-to-end yang efisien, sedangkan MQTT menjadi pilihan utama untuk komunikasi berkecepatan tinggi pada sistem berbasis event. Dengan demikian, pemilihan protokol dalam arsitektur WoT harus mempertimbangkan prioritas operasional, keterbatasan perangkat, dan tuntutan keamanan agar mencapai konfigurasi yang optimal.

4. KESIMPULAN DAN SARAN

Penelitian ini telah menyajikan tinjauan sistematis terhadap aspek keamanan dan kinerja protokol komunikasi dalam lingkungan WoT berdasarkan 22 studi terpilih. Hasil analisis menunjukkan bahwa tidak terdapat satu protokol tunggal yang unggul di seluruh parameter; sebaliknya, setiap protokol memiliki karakteristik unik yang sesuai dengan skenario implementasi tertentu. Protokol CoAP, dengan dukungan mekanisme keamanan OSCORE dan EDHOC, terbukti menjadi solusi paling optimal untuk perangkat dengan keterbatasan sumber daya constrained devices. Kombinasi ini mampu menyeimbangkan efisiensi energi dengan keamanan end-to-end yang kuat, bahkan ketika melewati proxy. Di sisi lain, MQTT menunjukkan dominasinya dalam aspek throughput dan kecepatan transmisi data, menjadikannya pilihan utama untuk aplikasi real-time berskala besar dengan arsitektur publish-subscribe. Namun, implementasi MQTT menuntut penambahan lapisan keamanan eksternal, seperti enkripsi simetris ringan atau manajemen kunci dinamis, untuk menutupi celah keamanan bawaannya. Sementara itu, HTTP tetap relevan sebagai penghubung utama ke infrastruktur web global dan manajemen akses berbasis OAuth2, meskipun memiliki overhead komunikasi dan komputasi yang paling tinggi dibandingkan protokol lainnya. Secara keseluruhan, kontribusi utama dari kajian ini menegaskan bahwa perancangan arsitektur keamanan WoT tidak dapat dilakukan secara seragam. Pengembang sistem perlu menerapkan pendekatan hibrida atau selektif: menggunakan CoAP untuk komunikasi sensor-ke-gateway

guna efisiensi, MQTT untuk transmisi data cepat, dan HTTP untuk integrasi layanan di tingkat aplikasi. Penelitian selanjutnya disarankan untuk mengeksplorasi standardisasi mekanisme keamanan adaptif yang mampu berpindah antar-protokol secara dinamis sesuai kondisi jaringan dan daya baterai perangkat.

DAFTAR REFERENSI

Albarrak, K. M. (2024). Securing the future of web-enabled IoT: A critical analysis of Web of Things security. *Applied Sciences (Switzerland)*, *14*(23). https://doi.org/10.3390/app142310867

Alharbi, S., Awad, W., & Bell, D. (2025). HECS4MQTT: A multi-layer security framework for lightweight and robust encryption in healthcare IoT communications. *Future Internet*, *17*(7). https://doi.org/10.3390/fi17070298

Chien, H. Y., & Ciou, P. P. (2023). Design and implementation of efficient IoT authentication schemes for MQTT 5.0. *Journal of Internet Technology*, *24*(3), 665-674. https://doi.org/10.53106/160792642023052403012

Chien, H.-Y., & Wang, N.-Z. (2022). A novel MQTT 5.0-based over-the-air updating architecture facilitating stronger security. *Electronics (Switzerland)*, *11*(23). https://doi.org/10.3390/electronics11233899

Gong, X., & Feng, T. (2022). Lightweight anonymous authentication and key agreement protocol based on CoAP of Internet of Things. *Sensors*, *22*(19). https://doi.org/10.3390/s22197191

Gong, X., Kou, T., & Li, Y. (2024). Enhancing MQTT-SN security with a lightweight PUF-based authentication and encrypted channel establishment scheme. *Symmetry*, *16*(10). https://doi.org/10.3390/sym16101282

Hintaw, A. J., Manickam, S., Karuppayah, S., Aladaileh, M. A., Aboalmaaly, M. F., & Laghari, S. U. A. (2023). A robust security scheme based on enhanced symmetric algorithm for MQTT in the Internet of Things. *IEEE Access*, *11*(March 2023), 43019-43040. https://doi.org/10.1109/ACCESS.2023.3267718

Höglund, R., Tiloca, M., Selander, G., Preuß Mattsson, J. P., Vučinić, M., & Watteyne, T. (2024). Secure communication for the IoT: EDHOC and (Group) OSCORE protocols. *IEEE Access*, *12*, 49865-49877. https://doi.org/10.1109/ACCESS.2024.3384095

Hristozov, S., Huber, M., Xu, L., Fietz, J., Liess, M., & Sigl, G. (2021). The cost of OSCORE and EDHOC for constrained devices. *245*-250. https://doi.org/10.1145/3422337.3447834

Hsu, T.-C. (2024). Designing a secure and scalable service agent for IoT transmission through blockchain and MQTT fusion. *Applied Sciences (Switzerland)*, *14*(7). https://doi.org/10.3390/app14072975

Insan, I. M., & Samopa, F. (2024). Implementation of HTTP security protocol for Internet of Things based on digital envelope. *Procedia Computer Science*, *234*(2023), 1332-1339. https://doi.org/10.1016/j.procs.2024.03.131

Kaganurmath, S., & Cholli, N. (2025). Enabling robust security in MQTT-based IoT networks with dynamic resource-aware key sharing. *Procedia Computer Science*, *252*, 633-642. https://doi.org/10.1016/j.procs.2025.01.023

Kaganurmath, S., Cholli, N. G., & Anala, M. R. (2025). DLKS-MQTT: A lightweight key sharing protocol for secure IoT communications. *Engineering, Technology and Applied Science Research*, *15*(2), 21532-21538. https://doi.org/10.48084/etasr.10216

Khoury, D., Haddad, S., Sondi, P., Balian, P., Harb, H., Danash, K., Merhej, J., & Sayah, J. (2025). CoAP/DTLS protocols in IoT based on blockchain light certificate. *Internet of Things*, *6*(1). https://doi.org/10.3390/iot6010004

Kurdi, H., & Thayananthan, V. (2022). A multi-tier MQTT architecture with multiple brokers based on fog computing for securing industrial IoT. *Applied Sciences (Switzerland)*, *12*(14). https://doi.org/10.3390/app12147173

Narasimha Swamy, S., Anna, D. M., Vijayalakshmi, M. N., & Kota, S. R. (2024). Enabling lightweight device authentication in Message Queuing Telemetry Transport protocol. *IEEE Internet of Things Journal*, *11*(9), 15792-15807. https://doi.org/10.1109/JIOT.2024.3349394

Nguyen, L. T. T., Ha, S. X., Le, T. H., Luong, H. H., Vo, K. H., Nguyen, K. H. T., Nguyen, A. T., Dao, T. A., & Nguyen, H. V. K. (2022). BMDD: A novel approach for IoT platform (broker-less and microservice architecture, decentralized identity, and dynamic transmission messages). *PeerJ Computer Science*, *8*. https://doi.org/10.7717/peerj-cs.950

Oliver, S. G., & Purusothaman, T. (2022). Lightweight and secure mutual authentication scheme for IoT devices using CoAP protocol. *Computer Systems Science and Engineering*, *41*(2), 767-780. https://doi.org/10.32604/csse.2022.020888

Sahmi, I., Abdellaoui, A., Tomader, T., & Hmina, N. (2021). MQTT-PRESENT: Approach to secure Internet of Things applications using MQTT protocol. *International Journal of Electrical and Computer Engineering*, *11*(5), 4577-4586. https://doi.org/10.11591/ijece.v11i5.pp4577-4586

Seoane, V., Garcia-Rubio, C., Almenares-Mendoza, F., & Campo, C. (2021). Performance evaluation of CoAP and MQTT with security support for IoT environments. *Computer Networks*, *197*. https://doi.org/10.1016/j.comnet.2021.108338

Silva, D., Carvalho, L. I., Soares, J., & Sofia, R. C. (2021). A performance analysis of Internet of Things networking. *Applied Sciences*, *11*(4879), 1-30. https://doi.org/10.3390/app11114879

Subhashini, R., & Jyothi, D. G. (2024). Broken-stick regressive lightweight speck cryptographic constrained application protocol for data security in IoT aware smart home. *International Journal of Computer Networks and Applications*, *11*(3), 335-350. https://doi.org/10.22247/ijcna/2024/21

Thanh, L. N. T., Phien, N. N., Nguyen, T. A., Vo, H. K., Luong, H. H., Anh, T. D., Tuan, K. N. H., & Son, H. X. (2021). UIP2SOP: A unique IoT network applying single sign-on and message queue protocol. *International Journal of Advanced Computer Science and Applications*, *12*(6), 19-30. https://doi.org/10.14569/IJACSA.2021.0120603

Tian, S., & Vassilakis, V. G. (2023). On the efficiency of a lightweight authentication and privacy preservation scheme for MQTT. *Electronics (Switzerland)*, *12*(14). https://doi.org/10.3390/electronics12143085

Tsai, W. C., Tsai, T. H., Wang, T. J., & Chiang, M. L. (2022). Automatic key update mechanism for lightweight M2M communication and enhancement of IoT security: A case study of CoAP using Libcoap library. *Sensors*, *22*(1). https://doi.org/10.3390/s22010340

Wytrębowicz, J., Cabaj, K., & Krawiec, J. (2021). Messaging protocols for IoT systems-A pragmatic comparison. *Sensors*, *21*(20). https://doi.org/10.3390/s21206904