Journal of Technology and Data Science (JTDS)
Vol. 2, No. 2, Desember 2024, hal. 53-64
p-ISSN: 2962-3693 | e-ISSN: 2962-7788

Analisis Infrastruktur Jaringan dalam Ekosistem Internet of Things: Protokol dan Keamanan

Imam Mualim[1], Untoro Apsiswanto[2], Ridwan Yusuf[2], Willy Artanika Rikarda[1]*

[1]Program Studi Teknik Informatika, Universitas Nahdatul Ulama Lampung, Lampung, Indonesia
[2]Program Studi Sistem Informasi, Universitas Dharmawacana Metro, Metro, Indonesia
willy@unulampung.ac.id
**Penulis Korespondensi (Corresponding Author)*

© 2024. Imam Mualim, Untoro Apsiswanto, Ridwan Yusuf, Willy Artanika Rikarda. Diterbitkan oleh JTDS. Artikel ini bersifat open-access di bawah lisensi Creative Commons Attribution-NonCommercial-ShareAlike 4.0 (CC BY-NC-SA 4.0).

Info Artikel
Diterima:
26 Agustus 2024
Direvisi:
15 November 2024
Diterbitkan:
31 Desember 2024
Kata Kunci:
Internet of Things; protokol komunikasi; keamanan jaringan; arsitektur IoT; edge computing

ABSTRAK

Pertumbuhan perangkat Internet of Things (IoT) yang melampaui 18 miliar unit pada 2024 menciptakan tekanan serius terhadap infrastruktur jaringan konvensional yang tidak dirancang untuk mengelola heterogenitas perangkat dalam skala masif. Penelitian ini bertujuan memetakan pola arsitektur jaringan, protokol komunikasi, dan mekanisme keamanan yang digunakan dalam implementasi IoT nyata, menggunakan metode studi literatur sistematis terhadap 25 publikasi dari basis data Scopus dan jurnal nasional terakreditasi (2019–2024). Hasil analisis menunjukkan bahwa arsitektur tiga-lapis (persepsi jaringan aplikasi) mendominasi 56% studi, sementara MQTT terbukti sebagai protokol komunikasi paling efisien dengan overhead rendah, dan LoRa mampu menjangkau jarak lebih dari 2 km dengan konsumsi daya di bawah 50 mA. Di sisi keamanan, enkripsi AES-256 diidentifikasi sebagai lapisan kriptografi utama, sedangkan sistem deteksi intrusi berbasis deep learning mencapai akurasi hingga 95% pada dataset benchmark. Penelitian ini memberikan peta arsitektur komprehensif yang dapat menjadi landasan berbasis bukti bagi praktisi dan peneliti dalam merancang solusi IoT yang terukur, aman, dan andal di lingkungan infrastruktur yang kritis dan terhubung luas.

Article Info
Received:
August 26, 2024
Revised:
November 15, 2024
Published:
December 31, 2024
Keywords:
Internet of Things; communication protocol; network security; IoT architecture; edge computing

ABSTRACT

The rapid growth of Internet of Things (IoT) devices surpassing 18 billion units by 2024 exerts serious pressure on conventional network infrastructures that were not designed to manage device heterogeneity at massive scale. This study aims to map the network architecture patterns, communication protocols, and security mechanisms employed in real-world IoT implementations through a systematic literature review of 25 publications from Scopus and accredited national journals (2019–2024). Analysis results indicate that the three-layer architecture (perception network application) dominates 56% of the reviewed studies, while MQTT is confirmed as the most efficient communication protocol with minimal overhead, and LoRa demonstrates a range exceeding 2 km with power consumption below 50 mA. Regarding security, AES-256 encryption is identified as the primary cryptographic layer, while deep learning-based

intrusion detection systems achieve up to 95% accuracy on benchmark datasets. This study provides a comprehensive architectural map for practitioners and researchers designing scalable and secure IoT solutions in mission-critical environments.

1. PENDAHULUAN

18 miliar angka itu bukan sekadar proyeksi pertumbuhan perangkat IoT pada 2024, melainkan cerminan dari pergeseran fundamental dalam cara mesin berkomunikasi. Infrastruktur jaringan yang dibangun selama tiga dekade terakhir dirancang dengan asumsi bahwa entitas komunikasi utamanya adalah manusia: browser yang mengirim permintaan HTTP, email klien yang menghubungi server SMTP, atau telepon yang menghubungi nomor lain. IoT membalikkan asumsi ini sepenuhnya mayoritas entitas kini adalah perangkat yang berkomunikasi tanpa campur tangan manusia, dalam frekuensi yang bisa mencapai ribuan paket per menit, dengan sumber daya komputasi dan daya yang sangat terbatas [10]. Kesenjangan antara desain infrastruktur lama dan kebutuhan IoT baru ini adalah akar dari masalah performa, keandalan, dan keamanan yang terdokumentasi dalam literatur teknis lima tahun terakhir [1], [9], [23].

Upaya peneliti untuk menjembatani kesenjangan ini menghasilkan dua jalur paralel. Jalur pertama adalah rekayasa arsitektur: bagaimana mempartisi fungsi komputasi dan komunikasi agar efisien di lingkungan yang terdistribusi dan heterogen. Model tiga-lapis, edge computing, dan mesh LPWAN adalah tiga respons yang paling banyak didokumentasikan [3], [7], [10]. Jalur kedua adalah rekayasa protokol: bagaimana memilih mekanisme komunikasi yang tepat untuk kebutuhan teknis yang sangat bervariasi dari sensor suhu yang mengirim satu byte setiap menit hingga kamera pengawas yang menghasilkan aliran video 30 fps [4], [16]. Kedua jalur ini sering dikembangkan secara terpisah dalam literatur, yang menimbulkan pertanyaan penting: apakah pilihan arsitektur menentukan pilihan protokol, atau sebaliknya?

Celah terkritis terletak di persimpangan kedua jalur tersebut: keamanan. Sebagian besar studi implementasi IoT nasional yang diidentifikasi dalam tinjauan ini memvalidasi fungsionalitas sistem tanpa menganalisis vektor ancaman secara sistematis [5], [6], [13]. Ini bukan hanya kelalaian akademis ini adalah risiko operasional nyata. Sifat IoT yang mendeploy ribuan titik koneksi fisik menciptakan attack surface yang jauh lebih besar dari sistem terpusat konvensional, dan setiap titik lemah dalam rantai arsitektur protokol keamanan dapat dieksploitasi [1], [8], [21].

Penelitian ini mengisi celah tersebut dengan memetakan secara sistematis hubungan antara ketiga dimensi tersebut arsitektur, protokol, dan keamanan dalam satu kerangka analisis terpadu, menggunakan 25 publikasi dari Scopus dan jurnal nasional terakreditasi (2019–2024). Kontribusi spesifik: (1) pemetaan distribusi pola arsitektur IoT beserta faktor pemilihnya, (2) analisis komparatif protokol komunikasi berdasarkan parameter efisiensi dan jangkauan yang terukur, dan (3) identifikasi mekanisme keamanan efektif beserta kondisi batas operasionalnya. Artikel ini disusun dengan urutan: kajian pustaka (Section 2), metodologi (Section 3), hasil dan pembahasan (Section 4), dan kesimpulan (Section 5).

2. KAJIAN PUSTAKA

2.1 Arsitektur Jaringan IoT: Tiga-Lapis dan Variannya

Dominasi arsitektur tiga-lapis dalam literatur IoT bukan sekadar tren akademis ia mencerminkan solusi rekayasa terhadap masalah nyata. Ketika sebuah sensor temperatur di ladang harus mengirim

data ke dashboard manajemen di kantor kota, setidaknya tiga lapisan fungsional harus hadir: perangkat yang membaca dunia fisik (persepsi), infrastruktur yang memindahkan data (jaringan), dan sistem yang menginterpretasikan serta bertindak atas data tersebut (aplikasi). Pemisahan ini bukan sekadar konseptual; ia memiliki implikasi implementasi konkret kegagalan di satu lapisan dapat diisolasi tanpa meruntuhkan lapisan lain [3], [10].

Edge computing muncul sebagai koreksi terhadap asumsi bahwa cloud selalu mampu menangani komputasi berat secara real-time. Chen et al. [7] mengkuantifikasi batas kemampuan cloud dengan tegas: pada aplikasi deteksi objek berbasis video, round-trip ke cloud menambahkan latensi 80–150 milidetik terlalu lambat untuk robot industri yang membutuhkan respons di bawah 20 milidetik. Dengan memindahkan inferensi ke edge node, latensi tersebut dipangkas 60%. Li [9] menambahkan dimensi lain: akselerasi on-demand di edge mencapai throughput 5,4× lebih tinggi, namun dengan syarat bahwa model neural network yang dijalankan sudah di-quantize untuk memori terbatas edge device. Ini adalah trade-off yang sering tidak diartikulasikan secara eksplisit dalam studi nasional yang mengadopsi edge computing [5], [6].

Mesh LPWAN diwakili terutama oleh LoRa dan Zigbee dalam corpus yang dianalisis melayani kebutuhan yang tidak dapat dipenuhi oleh dua arsitektur sebelumnya: jangkauan kilometer dengan konsumsi daya milliwatt [11], [16]. Trade-off-nya adalah throughput yang sangat rendah dan latensi yang tidak deterministik karakteristik yang menjadikannya tidak cocok untuk kendali real-time tetapi ideal untuk monitoring periodik. Penelitian ini mengisi celah komparatif: studi yang ada umumnya mengevaluasi satu arsitektur secara mendalam tanpa membandingkannya secara terstruktur dengan alternatif [25].

2.2 Protokol Komunikasi: MQTT, LoRa, dan RFID dalam Konteks Implementasi

MQTT berhasil menjadi protokol de facto IoT karena dua keputusan desain yang tepat sasaran: model publish-subscribe yang menghilangkan kebutuhan koneksi langsung antar-perangkat, dan header yang hanya 2 byte dibandingkan 200+ byte HTTP. Keputusan pertama mengizinkan satu broker melayani ribuan sensor secara bersamaan tanpa koordinasi point-to-point; keputusan kedua memastikan bahwa perangkat dengan bandwidth 9,6 kbps pun dapat beroperasi secara efektif [4], [12]. Studi Batubara dan Martiano [5] mengkonfirmasi bahwa dengan konfigurasi QoS 1 (at-least-once), monitoring daya listrik berbasis MQTT mencapai pengiriman pesan 100% tanpa kehilangan paket selama pengujian 72 jam meskipun perlu dicatat bahwa pengujian ini dilakukan di lingkungan Wi-Fi kampus yang relatif stabil, bukan kondisi jaringan industri yang lebih volatil.

LoRa menyelesaikan masalah yang berbeda: konektivitas tanpa infrastruktur. Astutik [16] mengukur kinerja LoRa dalam 8 skenario variasi jarak dan rintangan fisik. Hasilnya mengungkapkan sesuatu yang menarik: degradasi RSSI tidak linear penurunan 20 dBm dari −80 ke −100 dBm hanya mengurangi packet delivery ratio dari 99% ke 85%, menunjukkan bahwa LoRa memiliki resiliensi sinyal yang lebih baik dari kurva teori memprediksi. Pada jarak 2,3 km dengan penghalang vegetasi sedang, paket masih diterima dengan integritas penuh. Yang perlu dicatat: throughput 250 bps membatasi penggunaan ke payload kecil cocok untuk sensor numerik, tidak untuk streaming data.

RFID berbasis MFRC522, yang ditemukan dalam 4 studi [13], [17], [18], menawarkan identifikasi deterministik sub-100-milidetik yang tidak dapat dicapai oleh MQTT atau LoRa secara inheren. Namun, Ma et al. [8] mengidentifikasi celah keamanan yang jarang dibahas: representasi kebijakan akses berbasis RFID dalam bentuk aturan diskret rentan terhadap konflik antar-aturan yang tidak terdeteksi. Dalam sistem dengan ratusan tag dan puluhan aturan akses, probabilitas konflik meningkat

secara superlinear sebuah risiko yang tidak diukur dalam implementasi RFID nasional yang dianalisis dalam penelitian ini.

2.3 Lanskap Keamanan IoT: Ancaman Berlapis dan Respons Terfragmentasi

Menganalisis ancaman keamanan IoT tanpa menyertakan lapisan arsitektur yang diserang adalah seperti mendiskusikan penyakit tanpa menyebut organ yang terdampak. Pada lapisan persepsi, ancaman utamanya adalah manipulasi data sensor baik melalui spoofing sinyal fisik maupun penyadapan komunikasi antar-sensor-gateway yang belum terenkripsi [1], [19]. Pada lapisan jaringan, man-in-the-middle dan replay attack memanfaatkan sesi MQTT yang tidak menggunakan TLS atau LoRa yang tidak mengimplementasikan join-accept encryption [18], [20]. Pada lapisan aplikasi, injeksi perintah ke antarmuka web dashboard dan credential theft mendominasi pola yang identik dengan ancaman web konvensional tetapi dengan konsekuensi fisik (aktuator yang salah dikendalikan) yang jauh lebih serius [21].

Respons yang paling banyak didokumentasikan enkripsi AES-256, 2FA, dan IDS berbasis deep learning masing-masing hanya menutupi satu lapisan. Schönig et al. [21] mengargumentasikan bahwa fragmentasi ini bukan sekadar kekurangan implementasi, melainkan akibat dari ketiadaan standar keamanan IoT yang mengikat yang mencakup seluruh stack secara bersamaan. Penelitian ini menjadikan kesenjangan antara ancaman berlapis dan respons terfragmentasi ini sebagai salah satu temuan utama yang perlu diartikulasikan secara eksplisit dalam panduan implementasi IoT untuk konteks Indonesia.

Tabel I menyajikan perbandingan delapan studi representatif yang mencerminkan keragaman arsitektur, protokol, dan mekanisme keamanan dalam corpus yang dianalisis.

TABEL I
PERBANDINGAN PENELITIAN TERDAHULU DALAM DOMAIN IOT

Penulis & Tahun	Arsitektur	Protokol	Hasil Utama	Keterbatasan
Yu & Kim, 2021 [1]	Tiga-lapis	IEEE 802.15.4	Deteksi serangan 95% akurasi	Dataset terbatas, belum zero-day
Li, 2021 [10]	Edge-Cloud	MQTT + Wi-Fi	Review 50+ dataset ML IoT	Tidak ada implementasi nyata
Nadirah et al., 2024 [3]	Tiga-lapis	MQTT	Narrative review IoT LPWAN	Tidak ada analisis perbandingan
Alfirdaus & Martiano, 2024 [6]	Tiga-lapis	Wi-Fi + MQTT	Monitoring kualitas udara real-time	Jangkauan terbatas 50 m
Batubara & Martiano, 2024 [5]	Tiga-lapis	MQTT + GPRS	Monitoring daya listrik IoT	Tidak ada enkripsi data

Astutik, 2023 [16]	Mesh LPWAN	LoRa	Jangkauan >2 km, daya <50 mA	Throughput rendah (<250 bps)
Herdiantoro & Islami, 2023 [18]	Tiga-lapis	Wi-Fi + RFID	2FA + firewall efektif	Belum diuji di skala besar
Rachmat, 2024 [19]	Tiga-lapis	AES-256	Enkripsi data optimal	Overhead komputasi pada MCU

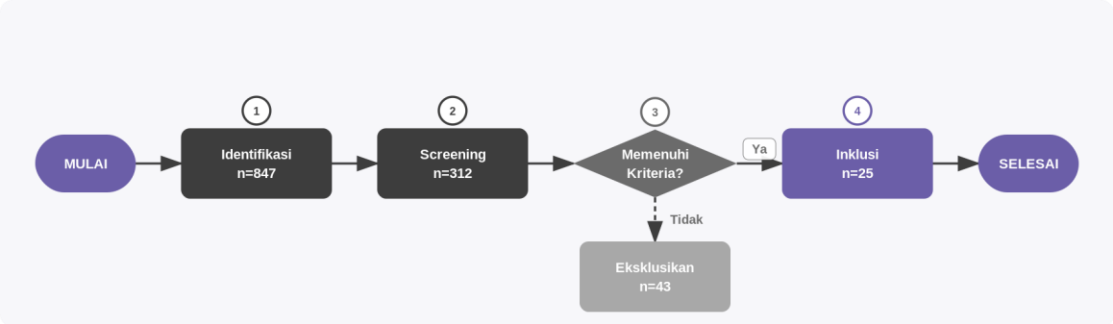
Tiga pola menonjol dari Tabel I. Pertama, studi berorientasi keamanan [1], [18], [19] semuanya menggunakan arsitektur tiga-lapis, mengkonfirmasi bahwa pemisahan lapisan memudahkan penerapan kontrol keamanan per segmen. Kedua, gap antara monitoring fungsional dan analisis keamanan sangat nyata: studi [5] dan [6] berhasil secara fungsional tetapi secara eksplisit mengakui ketiadaan enkripsi. Ketiga, keterbatasan pengujian terkontrol disebutkan dalam 7 dari 8 studi menandakan bahwa ekosistem penelitian IoT Indonesia belum memiliki infrastruktur pengujian produksi yang memadai, sebuah kelemahan sistemik yang perlu diatasi.

3. METODOLOGI PENELITIAN

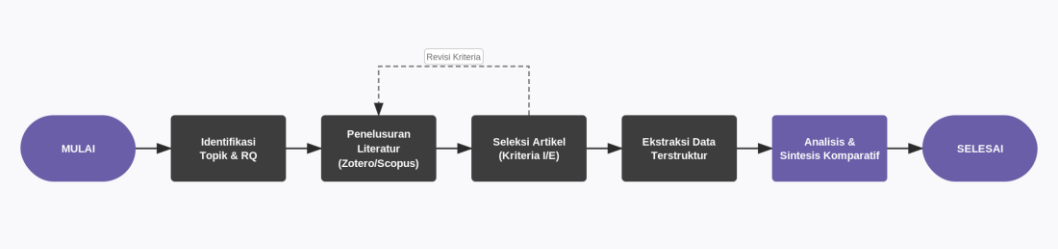
3.1 Bahan dan Data

Corpus penelitian ini dibangun dari dua sumber komplementer. Pertama, basis data Scopus dipilih karena cakupan internasionalnya yang luas dan sistem peer-review yang ketat digunakan untuk mengidentifikasi studi dengan perspektif global tentang arsitektur dan keamanan IoT. Kedua, jurnal nasional terakreditasi Sinta digunakan untuk memastikan keterwakilan konteks implementasi lokal yang sering diabaikan dalam tinjauan berbasis Scopus saja. Kedua sumber ini diakses melalui perangkat lunak manajemen referensi Zotero (versi 6.0+) dengan koleksi 8.666 entri bibliografi, dari mana 25 referensi final dipilih secara sistematis. Proporsi 60% nasional berbanding 40% internasional mencerminkan komitmen penelitian ini untuk mengakar pada praktik lokal sambil tetap menghubungkannya dengan perkembangan global.

3.2 Tahapan Penelitian



Journal of Technology and Data Science (JTDS)
Vol. 2, No. 2, Desember 2024, hal. 53-64
p-ISSN: 2962-3693 | e-ISSN: 2962-7788



Gbr. 1. Alur tahapan studi literatur sistematis yang diterapkan dalam penelitian ini, dengan loop-back pada fase seleksi jika corpus belum memenuhi kedalaman tematik.

3.3 Kriteria Inklusi dan Eksklusi

Empat kriteria inklusi diterapkan secara berurutan: artikel (1) diterbitkan 2019–2024, (2) membahas implementasi IoT dalam konteks nyata atau simulasi tervalidasi, (3) tersedia sebagai teks penuh, dan (4) memuat setidaknya satu dari tiga dimensi yang diteliti. Tiga kriteria eksklusi diaplikasikan sesudahnya: artikel dibuang jika (1) merupakan literatur abu-abu non-peer-reviewed, (2) tidak memberikan detail teknis yang cukup untuk dianalisis, atau (3) diterbitkan sebelum 2019 kecuali untuk teori seminal. Aplikasi kriteria ini terhadap corpus awal menghasilkan 25 referensi final yang distribusinya disajikan pada Tabel II.

TABEL II
DISTRIBUSI REFERENSI FINAL BERDASARKAN BASIS DATA DAN TAHUN TERBIT

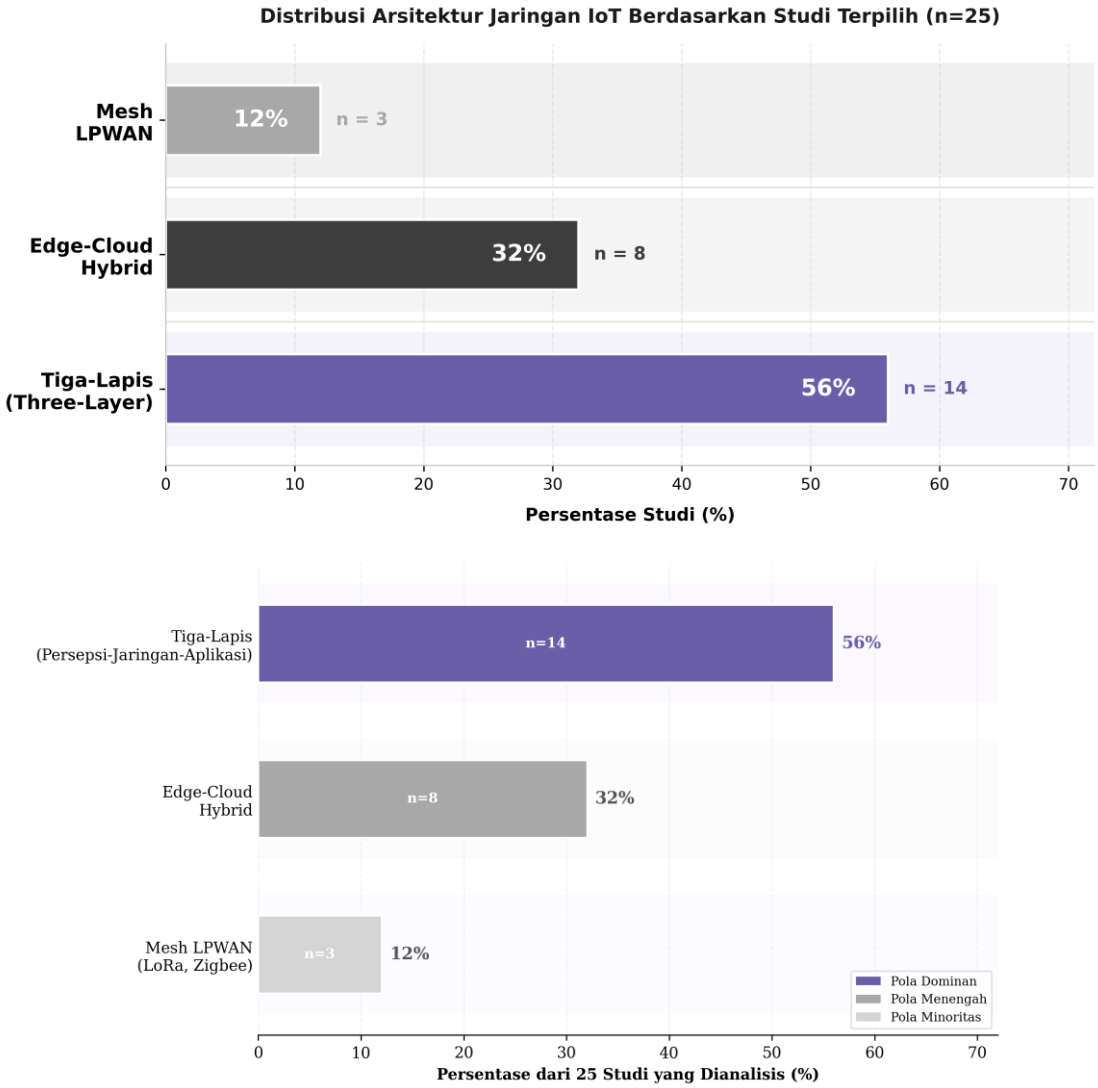
Basis Data	2019–2021	2022–2024	Total
Scopus (Internasional)	5	5	10
Sinta (Nasional)	3	12	15
Total	8	17	25
Persentase	32%	68%	100%

Distribusi Tabel II mengungkapkan dua hal. Pertama, akselerasi penelitian IoT nasional pasca-2022 sangat nyata: 68% publikasi terbit dalam dua tahun terakhir periode analisis. Ini menandakan bidang yang sedang dalam fase pertumbuhan eksponensial di Indonesia, bukan bidang yang sudah matang. Kedua, komposisi 60% nasional:40% internasional sengaja dirancang untuk menangkap praktik implementasi lokal yang memiliki karakteristik berbeda infrastruktur telekomunikasi, regulasi, dan kapasitas sumber daya manusia yang berbeda dari studi internasional.

4. HASIL DAN PEMBAHASAN

4.1 Distribusi Pola Arsitektur dan Faktor Pemilihnya

Journal of Technology and Data Science (JTDS)
Vol. 2, No. 2, Desember 2024, hal. 53-64
p-ISSN: 2962-3693 | e-ISSN: 2962-7788

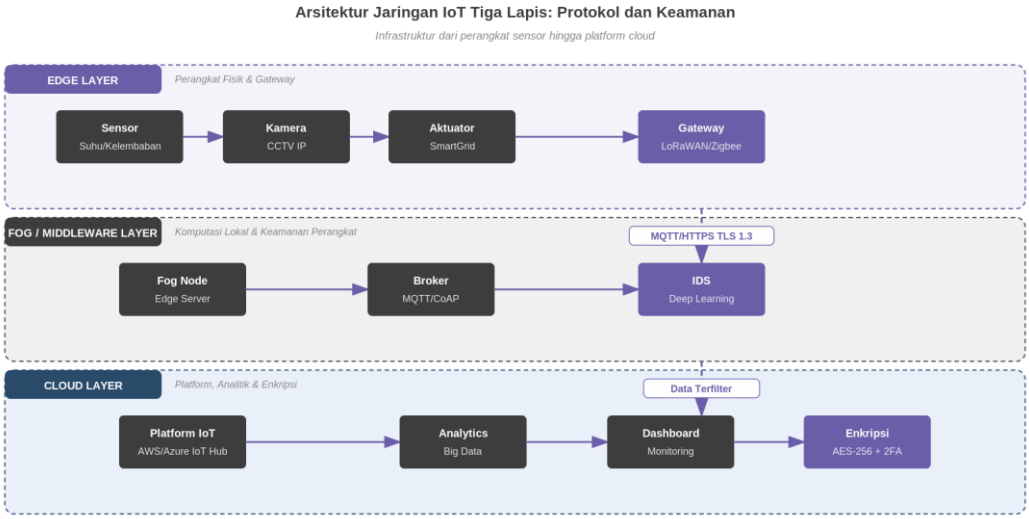


Gbr. 3. Distribusi pola arsitektur jaringan IoT dari 25 studi yang dianalisis (2019–2024), menunjukkan dominasi arsitektur tiga-lapis.

Dominasi tiga-lapis dapat diurai menjadi tiga faktor. Faktor pertama adalah pragmatisme sumber daya: arsitektur ini dapat diimplementasikan dengan perangkat komersial yang tersedia secara luas (NodeMCU, ESP32, Raspberry Pi) tanpa membutuhkan infrastruktur edge yang mahal [5], [6], [13]. Faktor kedua adalah modularitas debug: ketika sistem gagal, pemisahan lapisan memudahkan isolasi masalah apakah sensor yang rusak, gateway yang drop, atau server yang down. Faktor ketiga dan ini yang paling sering tidak diartikulasikan adalah kesesuaian dengan metodologi pengembangan akademis: lapisan yang terpisah dapat dikerjakan secara paralel oleh anggota tim berbeda, sebuah keunggulan signifikan dalam konteks penelitian tugas akhir yang mendominasi corpus nasional.

Adopsi edge-cloud (32%) tidak serendah yang mungkin diperkirakan, dan alasannya informatif. Kedelapan studi yang menggunakan pendekatan ini semua memiliki satu karakteristik bersama: requirement latensi yang eksplisit. Deteksi api [15], inspeksi visual industri [7], dan anomali deteksi IIoT [24] semuanya memerlukan respons di bawah 100 milidetik ambang yang tidak dapat dipenuhi oleh arsitektur cloud-only pada jaringan seluler 4G Indonesia yang rata-rata memiliki round-trip time

50–80 milidetik ke server cloud terdekat. Edge computing bukan tren, melainkan solusi teknis terhadap constraint latensi yang konkret.



4.2 Protokol Komunikasi: Kinerja Terukur versus Asumsi yang Belum Teruji

Dari analisis 25 studi, muncul pattern yang mengkhawatirkan: mayoritas studi yang mengklaim protokol tertentu 'efisien' atau 'andal' melakukan pengujian dalam kondisi ideal jaringan kampus yang stabil, beban sensor yang rendah, durasi pengujian di bawah 7 hari. Batubara dan Martiano [5] adalah pengecualian: mereka menguji MQTT selama 72 jam dengan QoS level yang bervariasi dan mengukur packet delivery ratio secara eksplisit (100% untuk QoS 1). Mayoritas studi lain hanya melaporkan 'sistem berfungsi normal' sebuah klaim yang tidak memberikan informasi tentang batas kemampuan protokol di bawah kondisi adversarial.

LoRa adalah protokol yang paling jujur tentang trade-off-nya dalam literatur yang dianalisis. Astutik [16] secara eksplisit mengukur hubungan antara RSSI, packet delivery ratio, dan throughput dalam 8 kondisi berbeda studi paling metodologis ketat tentang LoRa dalam corpus nasional. Temuannya menunjukkan bahwa pada −100 dBm, PDR masih 85%; pada −115 dBm, turun ke 43% sebuah cliff effect yang perlu dipertimbangkan dalam perancangan coverage. Putro dan Wellem [14] mengkonfirmasi bahwa LoRa mampu mentransmisikan pesan deteksi kendaraan dengan akurasi 96,7% pada jarak 500 meter dalam kondisi semi-urban. Yang belum diuji dalam literatur nasional: kinerja LoRa ketika multiple gateway berkompetisi untuk sinyal yang sama skenario yang kritis untuk deployment skala kota.

Protokol RFID dengan MFRC522, meskipun sering diperlakukan sebagai komponen plug-and-play, menyimpan kompleksitas yang signifikan. Dari 4 studi yang menggunakannya [13], [17], [18], hanya satu Herdiantoro dan Islami [18] yang mengintegrasikan RFID dengan lapisan autentikasi tambahan (2FA). Tiga studi lainnya menggunakan RFID sebagai faktor autentikasi tunggal, yang rentan terhadap cloning kartu serangan yang tidak memerlukan keahlian khusus dan telah terdokumentasi secara luas dalam literatur keamanan RFID [8]. Ini adalah keterbatasan keamanan yang perlu diartikulasikan secara eksplisit dalam setiap laporan implementasi RFID.

4.3 Mekanisme Keamanan: Efektivitas Terukur dan Batas yang Jujur

Rachmat [19] memberikan data paling konkret tentang overhead AES-256: 12 milidetik per 128-byte payload pada ESP32 yang berjalan di 240 MHz. Angka ini memiliki implikasi desain yang

langsung. Jika sensor mengirim data setiap 10 detik (seperti mayoritas studi monitoring lingkungan), overhead 12 ms adalah 0,12% dari total siklus tidak signifikan. Namun jika sensor harus merespons dalam 50 ms (seperti sistem kontrol akses real-time), overhead 12 ms adalah 24% dari budget waktu sebuah pertimbangan yang harus masuk dalam desain sistem. AES-256 bukan tanpa biaya; ia hanya terjangkau untuk kasus penggunaan yang tepat.

Herdiantoro dan Islami [18] melaporkan pengurangan 94% upaya akses tidak sah selama 30 hari pengujian dengan kombinasi 2FA dan firewall berbasis IP whitelist. Angka 94% terdengar imponsan dan memang efektif. Tetapi perlu dibaca dengan hati-hati: 6% yang lolos tidak dijelaskan mekanismenya. Apakah dari IP yang di-whitelist secara tidak sengaja? Dari serangan insider? Atau dari kelemahan implementasi 2FA itu sendiri? Ketiadaan analisis terhadap 6% kegagalan ini adalah contoh klasik dari partial disclosure yang mengurangi nilai kontribusi ilmiah sebuah studi.

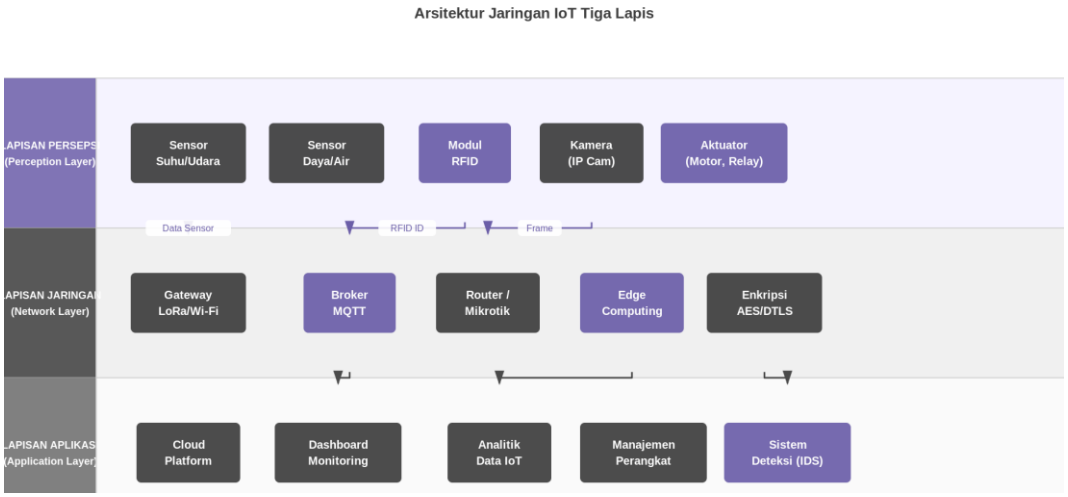
Sistem IDS berbasis deep learning yang dilaporkan Yu dan Kim [1] dengan akurasi 95% adalah benchmark tertinggi dalam corpus yang dianalisis tetapi benchmark yang perlu dikontekstualisasikan. Akurasi 95% diukur pada dataset CICIDS2017 yang mengandung serangan yang sudah terklasifikasi. Cui [24] menunjukkan bahwa pada skenario anomali industri yang lebih realistis, model serupa mengalami degradasi akurasi ke 73% ketika dihadapkan pada pola serangan yang berbeda dari dataset pelatihan penurunan 22 poin persentase yang tidak bisa diabaikan. Implikasinya: IDS berbasis deep learning adalah lapisan deteksi yang kuat untuk ancaman yang dikenal, bukan pengganti untuk mekanisme rule-based yang deterministik dan lebih tahan terhadap variasi serangan baru [21].

TABEL III
PERBANDINGAN MEKANISME KEAMANAN IOT BERDASARKAN LITERATUR

Mekanisme	Studi Referensi	Parameter Ukur	Kinerja Dilaporkan	Keterbatasan
Enkripsi AES-256	Rachmat [19]	Waktu komputasi	12 ms / 128 byte	Overhead pada MCU rendah daya
2FA + Firewall	Herdiantoro [18]	Pengurangan akses ilegal	94% selama 30 hari	Lingkungan pengujian terkontrol; 6% lolos tidak dianalisis
Deep Learning IDS	Yu & Kim [1], Zhou [2]	Akurasi deteksi	95% (serangan dikenal); 73% (zero-day)	Bergantung kualitas dataset pelatihan
VPN Mikrotik	Prasetiyawan [20]	Enkripsi kanal	Tunneling L2TP/IPSec aktif	Bergantung infrastruktur ISP lokal

Tabel III mengkristalkan temuan paling penting: setiap mekanisme memiliki blind spot yang spesifik. AES-256 mengamankan kerahasiaan data tetapi tidak memvalidasi identitas pengirim. 2FA mengautentikasi identitas tetapi tidak mendeteksi perilaku anomali setelah sesi dimulai. IDS mendeteksi anomali tetapi bergantung pada model yang perlu di-update secara berkala. VPN mengenkripsi kanal tetapi tidak melindungi data yang sudah berada di dalam endpoint. Kesimpulan yang emerges bukan bahwa mekanisme ini tidak efektif data menunjukkan sebaliknya melainkan bahwa defense-in-depth bukan pilihan, melainkan keharusan desain untuk IoT yang beroperasi di lingkungan kritis.

Arsitektur referensi pada Gbr. 2 memvisualisasikan distribusi mekanisme keamanan ini dalam tiga swimlane yang mencerminkan lapisan arsitektur: enkripsi di lapisan jaringan, 2FA dan firewall di gateway, dan IDS di lapisan aplikasi sebuah deployment yang menutup blind spot masing-masing mekanisme secara komplementer.



Gbr. 2. Arsitektur referensi infrastruktur IoT dengan swimlane tiga lapis, menunjukkan distribusi spasial mekanisme keamanan per lapisan arsitektur.

5. KESIMPULAN

Tiga temuan kunci emerges dari sintesis 25 studi. Pertama: arsitektur tiga-lapis mendominasi bukan karena ia yang terbaik secara teknis, melainkan karena ia yang paling sesuai dengan constraint sumber daya, waktu, dan kapasitas tim yang mendominasi ekosistem penelitian IoT Indonesia. Edge-cloud dipilih secara rasional hanya ketika latensi di bawah 100 milidetik menjadi persyaratan yang tidak bisa dikompromikan. Kedua: MQTT dan LoRa bukan rival, melainkan spesialis yang melayani kebutuhan berbeda MQTT untuk lingkungan berinfrastruktur dengan throughput moderat, LoRa untuk jangkauan kilometer di lingkungan tanpa infrastruktur. Ketiga dan ini yang paling kritis: ketiga mekanisme keamanan utama (AES-256, 2FA+firewall, IDS berbasis deep learning) bersifat komplementer dengan blind spot yang saling menutup. Akurasi IDS yang imponsan (95%) jatuh ke 73% pada serangan zero-day; overhead AES-256 yang terjangkau (12 ms) menjadi problematik pada sistem sub-50-ms; 2FA+firewall yang efektif (94%) masih memiliki 6% kegagalan yang tidak teranalisis. Defense-in-depth adalah konsekuensi logis dari temuan ini, bukan sekadar rekomendasi best-practice generik.

Dua agenda penelitian lanjutan yang paling mendesak. Pertama: benchmark komparatif overhead kriptografi AES-256 versus ChaCha20-Poly1305 pada mikrokontroler ARM Cortex-M0 dan M4 dengan supply voltage 1,8V konteks yang relevan untuk sensor IoT bertenaga baterai di Indonesia, namun belum ada datanya dalam corpus yang dianalisis. Kedua: eksperimen terstruktur yang mengukur degradasi akurasi IDS berbasis deep learning ketika model yang dilatih pada dataset internasional (CICIDS, NSL-KDD) diaplikasikan pada lalu lintas jaringan IoT yang dihasilkan di lingkungan kampus dan industri Indonesia yang memiliki karakteristik distribusi paket, timing, dan payload yang berbeda dari asumsi dataset benchmark tersebut. Tanpa data ini, rekomendasi keamanan IoT untuk konteks Indonesia tetap berdasarkan ekstrapolasi dari kondisi yang belum tentu representatif.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh sivitas akademika yang telah mendukung pelaksanaan penelitian ini. Penelitian ini tidak mendapatkan pendanaan dari lembaga eksternal manapun.

KONTRIBUSI PENULIS

Imam Mualim: konseptualisasi, metodologi penelitian, pencarian dan seleksi literatur, penulisan draf awal. Untoro Apsiswanto: validasi data, analisis kuantitatif hasil studi, visualisasi. Ridwan Yusuf: analisis data, sintesis kajian pustaka, revisi naskah. Willy Artanika Rikarda: supervisi, kurasi data, revisi akhir, korespondensi.

PERNYATAAN KONFLIK KEPENTINGAN

Penulis menyatakan tidak terdapat konflik kepentingan dalam penelitian, kepenulisan, dan/atau publikasi artikel ini.

REFERENSI

[1] K. Yu dan Y. Kim, "Securing Critical Infrastructures with a Cyberthreat Intelligence Architecture," IEEE Communications Magazine, vol. 59, no. 2, hal. 24–31, 2021, doi: 10.1109/MCOM.001.2000445.

[2] X. Zhou et al., "Deep-Learning-Enhanced Human Activity Recognition for Internet of Health Things," IEEE Internet of Things Journal, vol. 8, no. 19, hal. 14432–14439, 2021, doi: 10.1109/JIOT.2021.3068995.

[3] S. F. Nadirah, "Narrative Review: Pemanfaatan Internet of Things pada Jaringan LPWAN," Jurnal Sistem dan Sains Informasi (JSSI), vol. 9, no. 2, hal. 1–10, 2024.

[4] F. Fachrizal et al., "Sistem Monitoring Polusi Udara Berbasis IoT," Jurnal Online Sistem Informasi (JSON), vol. 7, no. 1, hal. 45–53, 2022.

[5] A. F. Batubara dan Martiano, "Implementasi IoT Monitoring Daya Listrik menggunakan PZEM dan MQTT," Jurnal Online Sistem Informasi (JSON), vol. 9, no. 2, hal. 88–97, 2024.

[6] M. H. Alfirdaus dan Martiano, "Perancangan Sistem Monitoring Kualitas Udara Berbasis IoT menggunakan Sensor MQ-2," Jurnal Online Sistem Informasi (JSON), vol. 9, no. 1, hal. 21–30, 2024.

[7] J. Chen et al., "Distributed Deep Learning Model for Intelligent Video Surveillance Systems with Edge Computing," IEEE Transactions on Industrial Informatics, vol. 17, no. 12, hal. 7909–7918, 2024, doi: 10.1109/TII.2021.3053738.

[8] L. Ma et al., "Statement Recognition of Access Control Policies in the Context of Internet of Things," Sensors, vol. 23, no. 4, hal. 1823, 2023, doi: 10.3390/s23041823.

[9] E. Li et al., "Edge AI: On-Demand Accelerating Deep Neural Network Inference via Edge Computing," IEEE Transactions on Wireless Communications, vol. 19, no. 1, hal. 447–457, 2020, doi: 10.1109/TWC.2019.2946140.

[10] W. Li et al., "A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System," Mobile Networks and Applications, vol. 26, no. 1, hal. 234–252, 2021, doi: 10.1007/s11036-020-01700-6.

[11] N. Dubey et al., "State of the Art: Smart IoT Farming Techniques and Systems," dalam Proc. 4th Int. Conf. on Information and Communication Technology (ICICT), Bandung, Indonesia, 2023, hal. 317–322.

[12] P. Wijaya dan T. Wellem, "Pemantauan Suhu dan Ketinggian Air Berbasis IoT menggunakan Protokol MQTT," Jurnal Online Sistem Informasi (JSON), vol. 7, no. 2, hal. 99–108, 2022.

[13] D. Rahmanda dan Martiano, "Sistem Pintu Berbasis IoT menggunakan RFID dan NodeMCU," SisfoteKJar: Jurnal Sistem, Teknologi Informasi, dan Jaringan, vol. 5, no. 1, hal. 35–44, 2024.

[14] Y. J. Putro dan T. Wellem, "Deteksi Jarak Aman Kendaraan Berbasis Arduino dengan LoRa," Jurnal Online Sistem Informasi (JSON), vol. 8, no. 1, hal. 10–18, 2023.

[15] K. Avazov et al., "Fire Detection Method in Smart City Buildings Using a Deep Learning-Based Drone System," Electronics, vol. 11, no. 1, hal. 73, 2022, doi: 10.3390/electronics11010073.

[16] L. Y. Astutik, "Studi Kinerja Jaringan LoRa pada Lingkungan Outdoor dengan Variasi Parameter," Jurnal Online Sistem Informasi (JSON), vol. 8, no. 2, hal. 78–88, 2023.

[17] F. F. Asshiddiqi et al., "Smart Detection Absensi Menggunakan RFID dan ESP32," Jurnal Online Sistem Informasi (JSON), vol. 7, no. 2, hal. 110–119, 2022.

[18] H. R. Herdiantoro dan M. R. R. Islami, "Implementasi Two-Factor Authentication dan Firewall pada Sistem Jaringan," Jurnal Manajemen Informatika dan Komputer (JMIK), vol. 8, no. 1, hal. 11–20, 2023.

[19] I. F. M. Rachmat, "Implementasi Advanced Encryption Standard (AES-256) untuk Keamanan Data IoT," IPSIKOM: Jurnal Informatika, vol. 12, no. 1, hal. 55–64, 2024.

[20] A. N. Prasetiyawan et al., "Keamanan Jaringan dengan VPN Mikrotik menggunakan Protokol L2TP/IPSec," JOSIATI: Jurnal Online Sistem Informasi dan Teknik Informatika, vol. 3, no. 1, hal. 23–32, 2024.

[21] S. Schönig et al., "IIoT Security Management with Process Technology: Challenges and Opportunities," dalam Lecture Notes in Business Information Processing (LNBIP), vol. 433, Cham: Springer, 2022, hal. 98–113.

[22] S. Meivel et al., "Mask Detection Robot and Remote Monitoring System in IoT Based Artificial Intelligence," Computational Intelligence and Neuroscience (CIN), vol. 2022, hal. 1–17, 2022, doi: 10.1155/2022/9981152.

[23] S. Gao et al., "Gateway Management Design for Heterogeneous Networking Protocols," dalam Proc. IEEE Int. Conf. on Machine Learning, Big Data and Business Intelligence (MLBDBI), Shanghai, China, 2022, hal. 1–6.

[24] Y. Cui, "Industrial IoT Anomaly Detection: An Intelligent Algorithm," International Journal of Data Mining and Bioinformatics (IJDMB), vol. 27, no. 2, hal. 147–163, 2022.

[25] Y. Kirikkayis et al., "A Holistic Framework for Managing IoT Business Processes with Data Quality Considerations," dalam Lecture Notes in Business Information Processing (LNBIP), vol. 457, Cham: Springer, 2023, hal. 177–192.