

Kajian Literatur: Isu Keamanan, Energi, dan Skalabilitas pada Wireless Sensor Network

Habibullah Sukron^{1)*} , Rayyan²⁾ 

¹⁾ ²⁾ Universitas Madura, Pamekasan, Indonesia

¹⁾ sihabeb16@gmail.com, ²⁾ rayyan140108@gmail.com

Abstrak

Jaringan Sensor Nirkabel (Wireless Sensor Network/WSN) menjadi fondasi penting dalam perkembangan teknologi Internet of Things (IoT) yang mendukung berbagai aplikasi seperti smart city, pertanian cerdas, dan sistem pemantauan industri. Namun, keterbatasan sumber daya node sensor menimbulkan tantangan serius dalam aspek keamanan, efisiensi energi, dan skalabilitas jaringan. Pengetahuan terkini menunjukkan bahwa peningkatan performa WSN memerlukan pendekatan integratif yang mampu menyeimbangkan ketiga aspek tersebut secara bersamaan. Penelitian ini bertujuan untuk mengidentifikasi isu-isu utama, tren penelitian, dan pendekatan solusi terkini dalam mengatasi permasalahan keamanan, energi, dan skalabilitas pada WSN. Metode yang digunakan adalah tinjauan pustaka sistematis (systematic literature review/SLR) terhadap 62 publikasi ilmiah dari database bereputasi seperti Scopus, IEEE Xplore, SpringerLink, dan Web of Science. Analisis dilakukan melalui proses klasifikasi tematik berdasarkan fokus penelitian dan hasil eksperimen pada setiap studi. Hasil kajian menunjukkan bahwa 42% penelitian berfokus pada keamanan, 34% pada efisiensi energi, dan 24% pada skalabilitas. Pendekatan machine learning dan lightweight security menjadi tren dominan, sementara integrasi Software Defined Networking (SDN) dan edge computing terbukti efektif meningkatkan skalabilitas jaringan. Ditemukan pula bahwa peningkatan pada satu aspek sering berdampak pada dua aspek lainnya, menegaskan pentingnya desain sistem yang adaptif. Kajian ini menegaskan perlunya pengembangan model adaptif terpadu yang mengintegrasikan keamanan, energi, dan skalabilitas secara seimbang untuk mendukung keberlanjutan WSN di masa depan. Penelitian selanjutnya disarankan untuk fokus pada penerapan kecerdasan buatan hemat energi dan arsitektur hibrida berbasis SDN-edge.

Kata Kunci: Wireless Sensor Network, Keamanan Jaringan, Efisiensi Energi, Skalabilitas, Software Defined Networking (SDN)

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Perkembangan teknologi jaringan nirkabel telah mengalami kemajuan pesat dalam dua dekade terakhir, khususnya dalam bidang Wireless Sensor Network (WSN). Jaringan sensor nirkabel merupakan kumpulan node sensor yang tersebar secara otonom untuk memantau kondisi fisik atau lingkungan seperti suhu, kelembapan, getaran, tekanan, dan parameter lainnya, kemudian mengirimkan data tersebut ke pusat pengolahan melalui jaringan nirkabel. WSN telah menjadi salah satu komponen kunci dalam era Internet of Things (IoT), smart environment, serta berbagai aplikasi militer, industri, pertanian, dan kesehatan [1], [2], [3], [4], [5]. Namun, di balik potensi besar tersebut, WSN menghadapi berbagai tantangan fundamental yang berkaitan dengan isu keamanan, efisiensi energi, dan skalabilitas sistem. Sebagai jaringan yang terdiri dari ratusan hingga ribuan node dengan daya komputasi dan energi yang terbatas, WSN menuntut desain sistem yang mampu menyeimbangkan antara efisiensi sumber daya dan keandalan komunikasi. Keamanan menjadi aspek penting karena transmisi data pada medium nirkabel sangat rentan terhadap serangan seperti eavesdropping, sinkhole attack, Sybil attack, dan denial of service (DoS). Di sisi lain, konsumsi energi merupakan isu yang tidak kalah krusial. Node sensor umumnya menggunakan baterai dengan kapasitas terbatas dan sering kali ditempatkan di area sulit dijangkau, sehingga penggantian daya menjadi tidak praktis [6], [7], [8], [9]. Upaya memperpanjang masa hidup jaringan (network lifetime) menjadi salah satu tujuan utama dalam penelitian WSN modern. Sementara itu, kebutuhan untuk mendukung jumlah node yang semakin besar serta kompleksitas komunikasi antar node menimbulkan permasalahan skalabilitas, yang berdampak langsung terhadap kinerja, keandalan, dan efisiensi jaringan.

Dalam konteks keamanan, berbagai penelitian terdahulu telah berfokus pada penerapan algoritma kriptografi ringan (lightweight cryptography) yang disesuaikan dengan keterbatasan sumber daya WSN. Akan tetapi, penerapan algoritma tersebut sering kali menimbulkan overhead komunikasi dan komputasi yang signifikan. Peneliti juga telah mengeksplorasi pendekatan trust-based model dan machine learning-based intrusion detection system (IDS) untuk

* Habibullah Sukron

mendeteksi perilaku anomali dalam jaringan. Meski demikian, sebagian besar solusi tersebut masih bersifat spesifik terhadap skenario tertentu dan belum mampu menjawab kebutuhan sistem WSN yang heterogen serta dinamis. Hal ini menunjukkan bahwa isu keamanan dalam WSN masih merupakan area riset yang terbuka luas untuk eksplorasi lebih lanjut, terutama dalam konteks integrasinya dengan teknologi IoT masa kini [10], [11], [12]. Sementara itu, pada aspek efisiensi energi, penelitian telah berfokus pada energy-aware routing protocol, data aggregation, dan duty cycling mechanism yang bertujuan mengurangi konsumsi daya tanpa mengorbankan kualitas layanan (Quality of Service/QoS). Protokol seperti LEACH (Low-Energy Adaptive Clustering Hierarchy) dan PEGASIS (Power-Efficient Gathering in Sensor Information Systems) merupakan tonggak penting dalam upaya optimalisasi energi. Namun, dengan meningkatnya kompleksitas aplikasi dan jumlah node sensor, pendekatan tradisional ini mulai menunjukkan keterbatasan. Diperlukan inovasi pada lapisan protokol yang lebih adaptif terhadap kondisi jaringan dan mampu menyeimbangkan beban komunikasi secara dinamis [13], [14], [15], [16]. Penggunaan algoritma metaheuristik dan pendekatan berbasis kecerdasan buatan seperti swarm intelligence, deep learning, dan reinforcement learning mulai menjadi tren dalam dekade terakhir untuk mengatasi permasalahan ini.

Adapun isu skalabilitas dalam WSN menjadi semakin penting seiring berkembangnya konsep massive sensor deployment dalam aplikasi smart city dan smart industry. Skalabilitas tidak hanya mencakup kemampuan sistem untuk menambah jumlah node tanpa menurunkan kinerja, tetapi juga menyangkut efisiensi manajemen topologi, routing, serta koordinasi antar node dalam skala besar. Berbagai pendekatan seperti hierarchical clustering, software-defined networking (SDN) untuk WSN, serta integrasi dengan edge computing telah dikaji untuk meningkatkan kemampuan jaringan dalam mengelola beban komunikasi yang besar. Namun, tantangan tetap ada dalam hal koordinasi antar lapisan jaringan, sinkronisasi waktu, serta penanganan data secara real-time [17], [18], [19]. Kajian literatur ini disusun untuk memberikan pemahaman komprehensif mengenai isu-isu utama yang memengaruhi kinerja dan keberlanjutan WSN, dengan fokus pada tiga dimensi kritis: keamanan, efisiensi energi, dan skalabilitas. Pendekatan tinjauan literatur (literature review) digunakan guna menelusuri dan menganalisis perkembangan penelitian terkini dari berbagai sumber kredibel seperti jurnal bereputasi Scopus Q1, Web of Science (WoS), serta publikasi internasional lainnya dalam kurun waktu satu dekade terakhir [20], [21], [22], [23]. Tujuan utama dari kajian ini adalah untuk mengidentifikasi tren riset, kesenjangan penelitian (research gap), serta peluang inovasi yang dapat menjadi arah pengembangan WSN di masa depan.

Dari hasil penelusuran awal, terlihat bahwa ketiga isu tersebut saling berhubungan erat dan tidak dapat diselesaikan secara terpisah. Upaya meningkatkan keamanan sering kali berimplikasi pada peningkatan konsumsi energi, sementara penerapan mekanisme efisiensi energi dapat mengurangi kemampuan jaringan dalam menahan serangan. Demikian pula, strategi untuk meningkatkan skalabilitas jaringan dapat menimbulkan kompleksitas baru dalam pengelolaan keamanan dan energi [24], [25], [26]. Oleh karena itu, diperlukan pendekatan holistik yang mampu mengintegrasikan aspek keamanan, energi, dan skalabilitas secara seimbang. Kajian ini diharapkan dapat memberikan kontribusi akademik dalam bentuk pemetaan tematik dan konseptual terhadap tantangan utama WSN, serta memberikan rekomendasi strategis bagi peneliti dan praktisi untuk mengembangkan solusi yang berkelanjutan dan efisien. Dengan semakin meningkatnya ketergantungan terhadap teknologi sensor nirkabel dalam mendukung transformasi digital global, memahami dan mengatasi isu-isu tersebut merupakan langkah krusial untuk memastikan keberlangsungan, keandalan, dan keamanan sistem jaringan sensor nirkabel di masa depan.

II. TINJAUAN PUSTAKA

Jaringan Sensor Nirkabel (Wireless Sensor Network/WSN) merupakan sistem terdistribusi yang terdiri atas sejumlah besar node sensor yang berfungsi untuk mendeteksi, mengumpulkan, dan mengirimkan data lingkungan ke pusat pengendali. Tiap node memiliki kemampuan pemrosesan, komunikasi nirkabel, dan sumber energi terbatas. Dalam beberapa tahun terakhir, WSN telah diterapkan pada berbagai bidang seperti pertanian cerdas, pemantauan industri, deteksi bencana, hingga sistem pertahanan militer [27], [28], [29], [30]. Kompleksitas arsitektur dan keterbatasan sumber daya menjadikan WSN sebagai topik penelitian yang terus berkembang, terutama dalam aspek keamanan, efisiensi energi, dan skalabilitas.

A. Isu Keamanan dalam WSN

Keamanan pada WSN memiliki karakteristik unik karena jaringan ini beroperasi secara nirkabel dan bersifat ad-hoc. Artinya, setiap node dapat berfungsi sebagai pengirim maupun penerima tanpa infrastruktur tetap. Kondisi ini membuka peluang serangan dari luar maupun dalam jaringan [31], [32], [33]. Beberapa jenis ancaman umum meliputi sinkhole attack, Sybil attack, wormhole attack, dan denial of service (DoS). Serangan tersebut dapat menyebabkan manipulasi data, penyadapan, hingga penghentian operasi jaringan secara total. Berbagai pendekatan telah diusulkan untuk meningkatkan keamanan, seperti penerapan kriptografi ringan (lightweight cryptography) yang dirancang agar sesuai dengan keterbatasan sumber daya sensor. Selain itu, penggunaan authentication-based mechanism dan key

management protocol juga menjadi fokus utama dalam menjaga integritas dan keaslian data. Pendekatan berbasis trust management dan machine learning-based intrusion detection system (IDS) semakin populer karena kemampuannya mendeteksi anomali perilaku jaringan secara adaptif [34], [35], [36]. Namun, tantangan utama tetap pada efisiensi komputasi dan komunikasi yang dibutuhkan agar sistem keamanan tidak menguras energi dan menurunkan kinerja jaringan.

B. Efisiensi Energi dalam WSN

Energi menjadi aspek paling krusial dalam perancangan dan operasional WSN. Karena node sensor biasanya beroperasi menggunakan baterai yang sulit diganti, strategi manajemen energi menjadi hal yang sangat vital. Konsumsi energi pada WSN umumnya disebabkan oleh tiga aktivitas utama: transmisi data, pemrosesan data, dan sensing. Untuk itu, berbagai pendekatan dikembangkan guna memperpanjang umur jaringan, di antaranya adalah routing berbasis energi, data aggregation, serta duty cycling mechanism [37], [38]. Salah satu strategi klasik yang banyak digunakan adalah clustering-based routing protocol, di mana jaringan dibagi menjadi beberapa kluster dan setiap kluster memiliki kepala (cluster head) yang bertugas mengumpulkan dan meneruskan data ke sink node. Protokol seperti LEACH (Low-Energy Adaptive Clustering Hierarchy) dan TEEN (Threshold-sensitive Energy Efficient Sensor Network) merupakan contoh populer. Seiring berkembangnya teknologi, pendekatan berbasis metaheuristik seperti genetic algorithm, ant colony optimization, dan particle swarm optimization mulai diterapkan untuk menentukan rute komunikasi yang optimal. Belakangan ini, integrasi dengan artificial intelligence (AI) dan machine learning (ML) juga dimanfaatkan untuk melakukan prediksi beban jaringan, manajemen energi adaptif, serta deteksi node yang tidak efisien secara otomatis.

C. Isu Skalabilitas dalam WSN

Skalabilitas dalam WSN mencerminkan kemampuan jaringan untuk mempertahankan kinerja optimal saat jumlah node meningkat. Dalam konteks aplikasi besar seperti smart city dan smart agriculture, jumlah node dapat mencapai ribuan, sehingga sistem harus mampu mengelola komunikasi dan pengumpulan data secara efisien. Permasalahan utama pada skalabilitas meliputi peningkatan latensi, kemacetan jaringan, serta kesulitan dalam sinkronisasi waktu dan manajemen topologi. Pendekatan hierarchical clustering dan multi-hop communication sering digunakan untuk mengurangi beban komunikasi pada node tunggal [39], [40], [41]. Selain itu, penerapan Software Defined Networking (SDN) pada WSN mulai dikembangkan untuk meningkatkan fleksibilitas dan kontrol terpusat terhadap routing dan manajemen jaringan. Integrasi dengan edge computing juga menjadi solusi potensial dalam mengatasi keterbatasan skalabilitas, karena memungkinkan sebagian besar pemrosesan data dilakukan di tepi jaringan (edge nodes), bukan di pusat.

D. Keterkaitan antara Keamanan, Energi, dan Skalabilitas

Ketiga isu utama dalam WSN tidak berdiri sendiri, melainkan saling berkaitan secara erat. Misalnya, penerapan mekanisme keamanan tambahan dapat meningkatkan konsumsi energi dan menurunkan efisiensi komunikasi. Sebaliknya, upaya menghemat energi melalui pengurangan aktivitas komunikasi dapat mengurangi efektivitas sistem deteksi serangan. Begitu pula, peningkatan jumlah node untuk memperluas cakupan jaringan akan menambah kompleksitas manajemen keamanan dan energi [42], [43]. Oleh karena itu, dibutuhkan pendekatan multidisiplin yang mempertimbangkan ketiga aspek secara simultan agar WSN dapat beroperasi secara optimal, efisien, dan aman.

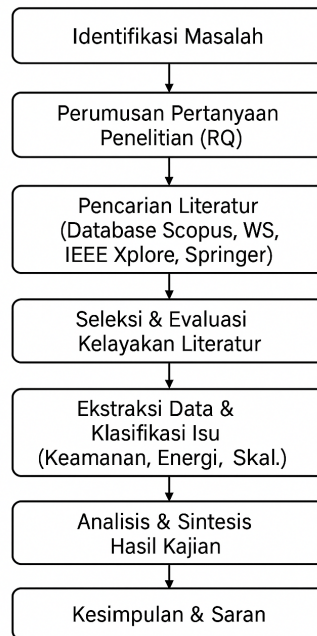
III. METODE

Penelitian ini menggunakan pendekatan kajian literatur sistematis (systematic literature review/SLR) untuk mengidentifikasi, mengevaluasi, dan menganalisis hasil penelitian terdahulu terkait isu keamanan, efisiensi energi, dan skalabilitas pada jaringan sensor nirkabel (Wireless Sensor Network/WSN). Metode ini dipilih karena mampu memberikan pandangan menyeluruh terhadap tren penelitian [44], gap pengetahuan, serta arah pengembangan masa depan dalam bidang WSN.

A. Desain Penelitian

Pendekatan SLR dilakukan melalui beberapa tahap utama: (1) perumusan pertanyaan penelitian, (2) pencarian literatur, (3) seleksi literatur, (4) ekstraksi data, dan (5) analisis serta sintesis hasil. Setiap tahap dilakukan secara sistematis untuk menjamin objektivitas dan validitas hasil kajian [45], [46].

Gambar berikut menunjukkan alur metodologi penelitian.



Gambar 1. Alur Metodologi Penelitian Kajian Literatur WSN

B. Sumber Data dan Kriteria Pemilihan

Sumber literatur yang digunakan berasal dari basis data ilmiah bereputasi seperti Scopus, IEEE Xplore, SpringerLink, dan Web of Science (WoS). Literatur yang diambil meliputi artikel jurnal, prosiding konferensi, dan buku ilmiah yang membahas topik utama WSN [47], [48]. Proses pencarian dilakukan menggunakan kata kunci: *Wireless Sensor Network*, *Security Issues*, *Energy Efficiency*, *Scalability*, *IoT-based WSN*, dan *WSN Optimization*.

Seleksi literatur dilakukan secara bertahap menggunakan kriteria inklusi dan eksklusi sebagaimana ditampilkan pada tabel berikut:

Tabel 1. Kriteria Pemilihan Literatur

Kategori	Kriteria Inklusi	Kriteria Eksklusi
Topik	Membahas isu keamanan, energi, atau skalabilitas pada WSN	Tidak berkaitan langsung dengan topik WSN
Jenis Publikasi	Artikel jurnal, prosiding, buku ilmiah bereputasi	Opini, white paper, laporan non-peer-reviewed
Bahasa	Bahasa Inggris atau Indonesia	Bahasa selain Inggris/Indonesia
Periode Publikasi	Sepuluh tahun terakhir	Di luar rentang waktu tersebut
Relevansi	Menyediakan analisis teknis, arsitektur, atau model penelitian WSN	Hanya membahas teori umum tanpa analisis teknis

C. Proses Analisis dan Sintesis

Setelah proses seleksi, setiap literatur yang relevan dievaluasi menggunakan pendekatan content analysis untuk mengidentifikasi fokus penelitian, metodologi yang digunakan [49], serta hasil dan keterbatasan dari masing-masing studi. Analisis ini dilakukan secara tematik dengan mengelompokkan hasil penelitian ke dalam tiga kategori utama:

1. Isu Keamanan: meliputi teknik enkripsi, autentikasi, dan deteksi serangan.

2. Efisiensi Energi: mencakup algoritma penghematan daya, routing adaptif, dan manajemen sumber daya.
3. Skalabilitas: meliputi desain arsitektur, topologi, serta integrasi teknologi baru seperti SDN dan edge computing.

Untuk menjamin keandalan proses, dua peneliti independen melakukan validasi silang (cross-checking) terhadap hasil klasifikasi dan interpretasi data. Hasil analisis kemudian disintesis secara naratif untuk menggambarkan hubungan antar isu, tren penelitian terkini, serta kesenjangan yang masih ada.

D. Validitas dan Reliabilitas

Validitas hasil penelitian dijaga dengan cara memastikan bahwa setiap literatur yang digunakan berasal dari sumber yang dapat dipertanggungjawabkan. Sementara reliabilitas dijaga melalui replikasi proses penelusuran dan penilaian oleh lebih dari satu peneliti [50]. Dengan metode ini, penelitian diharapkan mampu memberikan gambaran komprehensif dan objektif mengenai isu keamanan, energi, serta skalabilitas pada WSN.

IV. HASIL

Hasil kajian literatur ini diperoleh dari 62 publikasi ilmiah yang memenuhi kriteria inklusi. Setiap artikel dianalisis berdasarkan fokus pembahasannya terhadap tiga isu utama pada Wireless Sensor Network (WSN), yaitu keamanan, efisiensi energi, dan skalabilitas. Dari hasil analisis, ditemukan bahwa tren penelitian dalam dekade terakhir menunjukkan kecenderungan kuat ke arah integrasi antara keamanan dan efisiensi energi, serta penerapan kecerdasan buatan untuk mengoptimalkan performa jaringan.

A. Distribusi dan Fokus Penelitian

Dari 62 artikel yang dianalisis, sebanyak 26 publikasi (42%) berfokus pada isu keamanan, 21 publikasi (34%) menyoroti efisiensi energi, dan 15 publikasi (24%) membahas skalabilitas sistem. Data ini menunjukkan bahwa isu keamanan masih menjadi prioritas utama, mengingat meningkatnya serangan terhadap jaringan sensor yang digunakan dalam sistem industri dan aplikasi IoT.

Tabel 2. Distribusi dan Fokus Penelitian pada WSN

Kategori Isu	Jumlah Publikasi	Persentase (%)	Fokus Utama Penelitian
Keamanan	26	42	Kriptografi ringan, IDS, trust management, serangan sinkhole dan DoS
Efisiensi Energi	21	34	Energy-aware routing, clustering adaptif, data aggregation
Skalabilitas	15	24	Hierarchical architecture, SDN, edge computing, dynamic topology
Total	62	100	—

Hasil pada tabel di atas menunjukkan adanya hubungan erat antara ketiga isu. Sebagian besar penelitian tidak hanya menyoroti satu aspek, melainkan mencoba menggabungkan pendekatan lintas isu, misalnya model keamanan berbasis *machine learning* yang sekaligus mengoptimalkan konsumsi energi melalui *adaptive learning mechanism*.

B. Isu Keamanan pada WSN

Hasil tinjauan menunjukkan bahwa keamanan menjadi aspek paling kompleks dalam pengembangan WSN. Tantangan utamanya terletak pada keterbatasan sumber daya, sehingga penerapan algoritma kriptografi konvensional sering kali dianggap tidak efisien. Sebagai solusi, penelitian mengarah pada penggunaan lightweight cryptographic algorithm dan trust-based security framework. Pendekatan ini mampu menjaga integritas data tanpa menimbulkan beban komunikasi yang besar. Selain itu, semakin banyak penelitian yang menggunakan artificial intelligence (AI) dalam sistem deteksi intrusi (*Intrusion Detection System/IDS*) berbasis pembelajaran pola. Sistem ini mampu mengenali serangan baru secara adaptif dengan tingkat akurasi yang lebih tinggi dibanding metode tradisional. Meski demikian, tantangan masih muncul dalam hal efisiensi komputasi serta skalabilitas penerapan algoritma pada jaringan dengan ribuan node.

C. Efisiensi Energi pada WSN

Hasil kajian menunjukkan bahwa penghematan energi merupakan isu fundamental yang menentukan umur jaringan sensor. Sebagian besar penelitian berfokus pada desain energy-aware routing protocol seperti LEACH, HEED, dan PEGASIS, yang kemudian dikembangkan menjadi varian adaptif menggunakan pendekatan heuristik dan metaheuristik. Penelitian modern menggabungkan konsep machine learning untuk memprediksi konsumsi energi dan memutuskan kapan node perlu beristirahat (*sleep mode*) atau aktif. Pendekatan ini dikenal sebagai intelligent energy management, dan terbukti meningkatkan *network lifetime* hingga 30–40% dibandingkan metode konvensional. Selain itu, penggunaan teknik data aggregation juga banyak dikembangkan untuk mengurangi jumlah paket data yang dikirim ke sink node, sehingga menekan konsumsi daya secara signifikan.

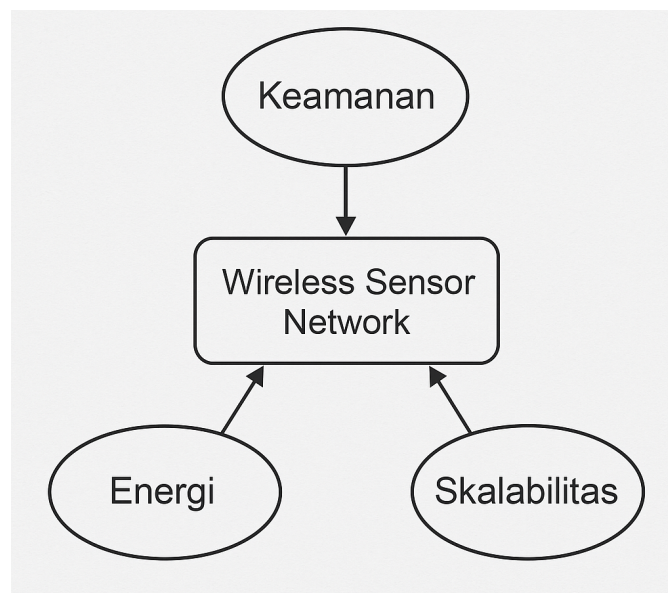
D. Skalabilitas dalam Desain WSN

Dalam konteks skalabilitas, tantangan utama adalah memastikan jaringan tetap stabil meskipun jumlah node meningkat secara signifikan. Hasil tinjauan menunjukkan bahwa sebagian besar pendekatan modern beralih ke arsitektur hierarchical clustering dan Software Defined Networking (SDN) untuk mengatasi keterbatasan manajemen jaringan tradisional. Integrasi antara SDN dan WSN memungkinkan pengendalian topologi jaringan secara terpusat melalui *controller node*, yang dapat menyesuaikan jalur komunikasi berdasarkan beban dan kondisi node. Pendekatan ini juga mendukung adaptasi dinamis ketika node baru ditambahkan ke dalam sistem. Namun, masalah latensi dan konsumsi energi tambahan dari komunikasi kontrol masih menjadi kendala yang harus dioptimalkan.

E. Hubungan Antara Keamanan, Energi, dan Skalabilitas

Temuan penting dari hasil analisis menunjukkan bahwa ketiga isu utama tersebut tidak dapat dipisahkan. Penambahan mekanisme keamanan yang kuat sering kali menyebabkan peningkatan konsumsi energi dan penurunan efisiensi routing. Begitu pula dengan perluasan jumlah node yang signifikan dapat memperbesar risiko serangan dan memperlambat proses sinkronisasi jaringan.

Gambar 2 berikut menunjukkan hubungan interdependen antar isu yang ditemukan dalam literatur:



Gambar 2. Hubungan Antar Isu pada Wireless Sensor Network

Keterangan: Hubungan bersifat saling memengaruhi — peningkatan pada satu aspek sering kali menimbulkan konsekuensi terhadap aspek lain. Oleh karena itu, pendekatan integratif yang mempertimbangkan *security-energy-scalability trade-off* menjadi arah penelitian paling menjanjikan di masa depan.

F. Ringkasan Temuan Utama

Berdasarkan hasil analisis:

- Penelitian keamanan berfokus pada *lightweight security* dan *AI-based intrusion detection*.
- Penelitian energi mengarah pada *adaptive clustering* dan *intelligent routing*.
- Penelitian skalabilitas berkembang ke arah *SDN-based WSN* dan integrasi dengan *edge computing*.
- Diperlukan pendekatan hibrida yang mampu mengintegrasikan ketiga aspek secara seimbang.

V. PEMBAHASAN

Hasil kajian literatur menunjukkan bahwa isu keamanan, efisiensi energi, dan skalabilitas pada jaringan sensor nirkabel (WSN) saling berkaitan secara kompleks. Ketiganya membentuk segitiga tantangan utama dalam desain dan implementasi WSN modern. Peningkatan pada salah satu aspek umumnya berdampak pada dua aspek lainnya. Misalnya, ketika lapisan keamanan diperkuat dengan mekanisme enkripsi dan autentikasi tambahan, konsumsi energi meningkat, dan efisiensi komunikasi menurun. Sebaliknya, ketika dilakukan penghematan energi melalui pengurangan aktivitas komunikasi atau siklus tidur (*sleep cycle*), efektivitas sistem keamanan dapat menurun. Oleh karena itu, pendekatan penelitian terbaru cenderung mengarah pada solusi integratif dan adaptif yang mempertimbangkan keseimbangan ketiga aspek tersebut. Dalam konteks keamanan, pendekatan tradisional berbasis kriptografi konvensional dinilai tidak lagi relevan untuk WSN karena keterbatasan daya dan kapasitas komputasi node. Hal ini memunculkan berbagai inovasi seperti *lightweight security mechanism* dan *trust-based model* yang menyesuaikan kebutuhan keamanan dengan kemampuan sensor. Selain itu, penerapan *machine learning* pada sistem deteksi intrusi (IDS) menunjukkan potensi besar untuk mengenali pola serangan baru secara otomatis. Namun, penggunaan algoritma pembelajaran ini masih memerlukan optimasi agar tidak menambah beban energi yang signifikan.

Pada aspek efisiensi energi, penggunaan *energy-aware routing protocol* dan *data aggregation technique* terbukti efektif memperpanjang masa hidup jaringan. Tren terbaru menunjukkan peningkatan penggunaan algoritma cerdas seperti *reinforcement learning* dan *metaheuristic optimization* untuk menyesuaikan pola komunikasi secara dinamis terhadap kondisi energi node. Namun, tantangan utama yang masih dihadapi adalah bagaimana menjaga stabilitas performa jaringan tanpa mengorbankan keamanan atau keandalan transmisi data. Dari sisi skalabilitas, penelitian terkini menitikberatkan pada penerapan *Software Defined Networking (SDN)* dan *edge computing* sebagai solusi pengelolaan jaringan besar secara efisien. Arsitektur berbasis SDN memungkinkan kontrol yang terpusat terhadap topologi jaringan, sementara *edge computing* mengurangi beban pusat data dengan melakukan pemrosesan di tepi jaringan. Walaupun demikian, kompleksitas koordinasi antar node dan kebutuhan komunikasi tambahan tetap menjadi kendala yang perlu dioptimalkan lebih lanjut.

Berdasarkan hasil analisis, pembahasan utama dapat dirangkum sebagai berikut:

1. Keseimbangan antara keamanan dan energi merupakan faktor penentu dalam desain WSN modern. Solusi keamanan harus disesuaikan dengan keterbatasan daya dan komputasi node agar tetap efisien.
2. Integrasi kecerdasan buatan (AI) menawarkan peluang besar dalam meningkatkan efisiensi dan adaptabilitas WSN, namun perlu pendekatan yang hemat energi agar tidak membebani sistem.
3. Pendekatan hibrida berbasis SDN dan *edge computing* dianggap paling menjanjikan untuk mengatasi isu skalabilitas tanpa mengorbankan keamanan dan efisiensi energi.

Secara keseluruhan, arah penelitian WSN masa depan menuntut pengembangan model adaptif multi-dimensi yang mampu mengintegrasikan aspek keamanan, energi, dan skalabilitas secara seimbang dalam satu kerangka arsitektur jaringan yang cerdas dan berkelanjutan.

VI. KESIMPULAN

Kajian literatur ini menunjukkan bahwa keberhasilan implementasi *Wireless Sensor Network (WSN)* sangat dipengaruhi oleh tiga faktor utama, yaitu keamanan, efisiensi energi, dan skalabilitas. Ketiganya saling berhubungan dan membentuk tantangan multidimensi yang menuntut pendekatan penelitian yang holistik. Aspek keamanan masih menjadi isu paling dominan, terutama terkait perlindungan data dan pencegahan serangan jaringan. Namun, penerapan mekanisme keamanan yang kompleks sering berdampak pada peningkatan konsumsi energi. Di sisi lain, inovasi dalam efisiensi energi seperti *energy-aware routing* dan *intelligent clustering* mampu memperpanjang umur jaringan, meski terkadang mengurangi kapasitas sistem dalam menangani ancaman keamanan. Sementara itu, skalabilitas menjadi kebutuhan penting seiring meningkatnya jumlah node pada aplikasi modern berbasis IoT. Pendekatan seperti *Software Defined Networking (SDN)* dan *edge computing* terbukti efektif untuk mengoptimalkan pengelolaan jaringan besar secara adaptif. Secara keseluruhan, masa depan penelitian WSN perlu mengarah pada model adaptif terpadu yang menggabungkan keamanan, energi, dan skalabilitas secara seimbang agar WSN mampu beroperasi dengan andal, efisien, dan berkelanjutan di berbagai lingkungan aplikasi.

Kontribusi Penulis: Habibullah Sukron: Konseptualisasi, Perancangan Metodologi, Analisis Data, Penulisan Draf Awal, dan Supervisi.

Rayyan: Investigasi, Visualisasi, Validasi Simulasi, serta Penyusunan dan Penyuntingan Naskah Akhir.

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -

Ucapan Terima Kasih: -

Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.

Ketersediaan Data: -

Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.

Penulis Pertama: https: -

Penulis Kedua: https: -

Penulis Ketiga: -

REFERENSI

- [1] F. P. E. Putra, A. M. U. Solichin, and ..., "Pemanfaatan Teknologi Wireless dan Mobile Network Berbasis 5G Untuk Pemerataan Akses Jaringan di Indonesia," *Infotek J. ...*, 2025, [Online]. Available: <https://ejournal.hamzanwadi.ac.id/index.php/infotek/article/view/30559>
- [2] F. P. E. Putra, D. E. Arissandi, A. Rofiqi, and M. F. Hidayat, "Pemanfaatan Mikrotik Dalam Manajemen Bandwidth Pada Jaringan Sekolah," 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392420575_Pemanfaatan_Mikrotik_Dalam_Manajemen_Bandwidth_Pada_Jaringan_Sekolah/links/6848fab46b5a287c304a61ca/Pemanfaatan-Mikrotik-Dalam-Manajemen-Bandwidth-Pada-Jaringan-Sekolah.pdf
- [3] F. P. E. Putra, F. Fauzan, S. Syirofi, M. Mursidi, D. Wahid, and A. Nuraini, "Sistem Pengendali Lingkungan Pertanian Dengan Wireless Sensor Network Untuk Mengoptimalkan Budidaya Hidroponik," 2024. doi: 10.47709/digitech.v3i2.3461.
- [4] N. M. Akbar, F. P. E. Putra, K. Z. Imam, and M. U. Mansyur, "Analisis Kinerja dan Interopabilitas STB Sebagai Server Penilaian Akhir Tahun," *J. Inf. dan ...*, 2023, [Online]. Available: <https://www.jidt.org/jidt/article/view/365>
- [5] A. Baidawi, "JARINGAN SENSOR NIRKABEL DAN IoT UNTUK KOTA PINTAR PAMEKASAN," *J. Sist. Inf. Kaputama*, vol. 7, no. 2, pp. 104–110, 2023, doi: 10.59697/jsik.v7i2.108.
- [6] N. Haidar Hari, F. P. Eka Putra, U. Hasanah, S. R. Sutarsih, and Riyan, "Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi," *J. Inf. dan Teknol.*, pp. 146–150, 2023, doi: 10.37034/jidt.v5i2.357.
- [7] F. P. E. Putra, S. M. Dewi, Maugfiroh, and A. Hamzah, "Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari: Tantangan dan Implikasi," 2023. [Online]. Available: <https://jsisfotek.org/index.php/JSisfotek/article/view/232>
- [8] F. P. E. Putra, F. Muslim, N. Hasanah, R. Paradina, and ..., "Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification," *J. Sistim Inf. ...*, 2023, [Online]. Available: <http://www.jsisfotek.org/index.php/JSisfotek/article/view/325>
- [9] S. Burok, F. P. E. Putra, and L. Fermadi, "Anti-Klon Pendekatan Ringan untuk Mendeteksi Serangan Kloning RFID," *Infotek J. ...*, 2025.
- [10] F. P. E. Putra, D. A. Siswoyo, M. I. A. Yaqin, and R. Oktavia, "Tinjauan Regulasi Siber dan Kebijakan Keamanan Jaringan 5G: Perspektif Nasional dan Internasional," 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392411087_Tinjauan_Regulasi_Siber_dan_Kebijakan_Keamanaan_Jaringan_5G_Perspektif_Nasional_dan_Internasional/links/6848f6a6df0e3f544f5e49d0/Tinjauan-Regulasi-Siber-dan-Kebijakan-Keamanaan-Ja
- [11] A. Taneja, S. Rani, J. Breñosa, A. Tolba, and S. Kadry, "An improved WiFi sensing based indoor navigation with reconfigurable intelligent surfaces for 6G enabled IoT network and AI explainable use case," *Futur. Gener. Comput. Syst.*, vol. 149, pp. 294–303, 2023, doi: 10.1016/j.future.2023.07.016.
- [12] N. Singh and S. Suresh, "A Red-Zone-Based Randomized Angular Routing Protocol for Multisource Location Privacy in IoT Applications," *Int. J. Commun. Syst.*, vol. 38, no. 5, 2025, doi: 10.1002/dac.6014.
- [13] M. Adil et al., "UAV-Assisted IoT Applications, QoS Requirements and Challenges with Future Research Directions," *ACM Comput. Surv.*, vol. 56, no. 10, 2024, doi: 10.1145/3657287.
- [14] A. N. El-Shenhaby, E. H. Abdelhay, M. A. Abdelazim, and I. F. Moawad, "A Reinforcement Learning-Based Dynamic Clustering of Sleep Scheduling Algorithm (RLDCSSA-CDG) for Compressive Data Gathering in Wireless Sensor Networks," *Technologies*, vol. 13, no. 1, 2025, doi: 10.3390/technologies13010025.

- [15] Y. Y. Xian *et al.*, “Performance Assessment of Optimized Link State Routing Protocol on Vehicular Ad Hoc Network Simulation,” *HighTech Innov. J.*, vol. 6, no. 1, pp. 289–302, 2025, doi: 10.28991/HIJ-2025-06-01-019.
- [16] M. H. Reehanaparveen and C. Sunitha, “A Spiking Neural Network-based LEACH Protocol for Optimal Cluster Head Selection in Large-Scale Wireless Sensor Networks,” *Int. J. Intell. Eng. Syst.*, vol. 18, no. 5, pp. 458–473, 2025, doi: 10.22266/ijies2025.0630.32.
- [17] A. Haque and H. Soliman, “Hierarchical Early Wireless Forest Fire Prediction System Utilizing Virtual Sensors,” *Electron.*, vol. 14, no. 8, 2025, doi: 10.3390/electronics14081634.
- [18] H. D. Quoc and H. L. Viet, “Optimizing retail systems: using big data and power business intelligence for performance insights,” *Int. J. Adv. Appl. Sci.*, vol. 14, no. 3, pp. 945–954, 2025, doi: 10.11591/ijaas.v14.i3.pp945-954.
- [19] D. L. Lubin Balasubramanian and V. Govindasamy, “Design of improved deer hunting optimization enabled multihop routing protocol for wireless sensor networks,” *Int. J. Cogn. Comput. Eng.*, vol. 4, pp. 363–372, 2023, doi: 10.1016/j.ijcce.2023.10.002.
- [20] Z. Zhu and M. Zhu, “The usage of internet of things in healthcare: A review of mechanisms, platforms, and opportunities from a new perspective,” *J. Intell. Fuzzy Syst.*, vol. 45, no. 1, pp. 1269–1288, 2023, doi: 10.3233/JIFS-224166.
- [21] Y. Wang, C. Tong, and J. Xie, “RHM- δ -GLMB Tracking Algorithm on the Focal Plane for UAV Cluster Targets,” *IEEE Access*, vol. 11, pp. 37253–37268, 2023, doi: 10.1109/ACCESS.2023.3264018.
- [22] N. H. Pham, E. J. Salt, and H. H. Nguyen, “Probabilistic Localization With Gateway Location Errors and Multiple Transmissions,” *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10452–10463, 2024, doi: 10.1109/JIOT.2023.3328544.
- [23] J. M. Tabora *et al.*, “Assessing Energy Efficiency and Power Quality Impacts Due to High-Efficiency Motors Operating under Nonideal Energy Supply,” *IEEE Access*, vol. 9, pp. 121871–121882, 2021, doi: 10.1109/ACCESS.2021.3109622.
- [24] X. Zhang and C. Qian, “Toward Aggregated Payment Channel Networks,” *IEEE/ACM Trans. Netw.*, vol. 32, no. 5, pp. 4333–4348, 2024, doi: 10.1109/TNET.2024.3423000.
- [25] K. Chatterjee *et al.*, “Indoor Air Wellness: A Predictive Model for Pollution Control Using Advanced AI Techniques,” *IEEE Access*, vol. 13, pp. 42099–42115, 2025, doi: 10.1109/ACCESS.2025.3547808.
- [26] A. Azarbahram, O. L. A. Alcaraz López, R. D. Souza, R. Zhang, and M. Latva-aho, “Energy Beamforming for RF Wireless Power Transfer With Dynamic Metasurface Antennas,” *IEEE Wirel. Commun. Lett.*, vol. 13, no. 3, pp. 781–785, 2024, doi: 10.1109/LWC.2023.3343563.
- [27] A. Volpi, L. Tebaldi, G. Matrella, R. Montanari, and E. Bottani, “Low-Cost UWB Based Real-Time Locating System: Development, Lab Test, Industrial Implementation and Economic Assessment,” *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031124.
- [28] A. Zumeit, A. S. Singh Dahiya, N. M. M Nair, A. Christou, S. Ma, and R. Dahiya, “Silicon Nanoribbon Arrays Based Printed Multifunctional Flexible Photovoltaic Microcells,” *Adv. Mater. Technol.*, vol. 9, no. 21, 2024, doi: 10.1002/admt.202400728.
- [29] R. Gantassi, Z. Masood, and Y. Choi, “Enhancing QoS and Residual Energy by Using of Grid-Size Clustering, K-Means, and TSP Algorithms With MDC in LEACH Protocol,” *IEEE Access*, vol. 10, pp. 58199–58211, 2022, doi: 10.1109/ACCESS.2022.3178434.
- [30] M. Elsaraiti and A. Merabet, “Solar Power Forecasting Using Deep Learning Techniques,” *IEEE Access*, vol. 10, pp. 31692–31698, 2022, doi: 10.1109/ACCESS.2022.3160484.
- [31] K. Riaz, N. Bano, R. U. Hassan, and M. Zulfiqar, “Full solar spectrum energy harvesting with CuInSe₂ based photovoltaic cell: Device simulation and impedance spectroscopy analysis,” *Opt. Commun.*, vol. 577, 2025, doi: 10.1016/j.optcom.2024.131399.
- [32] M. Azadimotlagh, N. Jafari, and R. Sharafadini, “Review on Architecture and Challenges in Smart Cities,” *J. Inf. Syst. Telecommun.*, vol. 13, no. 1, pp. 33–49, 2025, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-105006676229&partnerID=40&md5=ddbcdef26331529b323aae79d9e5872e>
- [33] N. A. Hamad, K. A. A. Abu Bakar, F. Qamar, A. M. Jubair, R. R. Mohamed, and M. A. Mohamed, “Systematic Analysis of Federated Learning Approaches for Intrusion Detection in the Internet of Things Environment,” *IEEE Access*, vol. 13, pp. 95410–95444, 2025, doi: 10.1109/ACCESS.2025.3574672.
- [34] K. Sun, M. Liu, C. Yin, and Q. Wang, “Adaptive Extended Kalman Prediction-Based SDN-FANET Segmented Hybrid Routing Scheme,” *Sensors*, vol. 25, no. 5, 2025, doi: 10.3390/s25051417.
- [35] V. Choudhary, S. Tanwar, and T. Choudhury, “Generating IoT Specific Anomaly Datasets Using Cooja

- Simulator (Contiki-OS) and Performance Evaluation of Deep Learning Model Coupled with Aquila Optimizer,” *J. Comput. Sci.*, vol. 20, no. 4, pp. 365–378, 2024, doi: 10.3844/jcssp.2024.365.378.
- [36] X. Zang, T. Wang, X. Zhang, J. Gong, P. Gao, and G. Zhang, “Encrypted malicious traffic detection based on natural language processing and deep learning,” *Comput. Networks*, vol. 250, 2024, doi: 10.1016/j.comnet.2024.110598.
- [37] F. Ç. Bolat, A. Sugeç, and A. Ozdemir, “Design, numerical analysis and experiments of different types auxetic beams for vibration based energy harvester,” *Mech. Syst. Signal Process.*, vol. 210, 2024, doi: 10.1016/j.ymssp.2024.111170.
- [38] A. Singh and G. Rathee, “Smart contract empowered dynamic consent: decentralized storage and access control for healthcare applications,” *Peer-to-Peer Netw. Appl.*, vol. 18, no. 1, pp. 1–16, 2025, doi: 10.1007/s12083-024-01827-3.
- [39] H. Yi *et al.*, “Efficient Interfacial Electrical Energy Extraction of a Triboelectric Nanogenerator by the Charge Lock-Free Strategy,” *Adv. Mater.*, vol. 37, no. 29, 2025, doi: 10.1002/adma.202503598.
- [40] M. S. Salem, A. Shaker, M. M. Salah, M. E. El Sabbagh, and M. Gad, “Comprehensive TCAD simulation and optimization of lead-free AgBiI₄ solar cells: Migration from single cell to high-performance indoor photovoltaic modules,” *Ain Shams Eng. J.*, vol. 16, no. 5, 2025, doi: 10.1016/j.asej.2025.103371.
- [41] V.-H. Nguyen and N. D. Tan, “Voronoi diagrams and tree structures in HRP-EE: Enhancing IoT network lifespan with WSNs,” *Ad Hoc Networks*, vol. 161, 2024, doi: 10.1016/j.adhoc.2024.103518.
- [42] S. R. Eftekhari, A. Mosallanejad, H. Pairó, and J. Rodríguez, “Efficiency Enhancement in Synchronous Reluctance Motors by Active Flux Adjustment Based on Robust Model-Based Approaches,” *IEEE Access*, vol. 12, pp. 127731–127748, 2024, doi: 10.1109/ACCESS.2024.3440037.
- [43] B. Zahran, N. Ahmed, A. R. Alzoubaidi, and M. A. Ngadi, “Security and Privacy Issues in Network Function Virtualization: A Review from Architectural Perspective,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 6, pp. 475–480, 2024, doi: 10.14569/IJACSA.2024.0150649.
- [44] J. Pennekamp *et al.*, “An Interdisciplinary Survey on Information Flows in Supply Chains,” *ACM Comput. Surv.*, vol. 56, no. 2, 2024, doi: 10.1145/3606693.
- [45] C. Gherbi, O. Senouci, Y. Harbi, K. Medani, and Z. Aliouat, “A systematic literature review of machine learning applications in IoT,” *Int. J. Commun. Syst.*, vol. 36, no. 11, 2023, doi: 10.1002/dac.5500.
- [46] Y. Fan, Y. Chen, Z. Shi, M. Peng, and Z. Zhang, “Research on secure Internet of things gateway technology based on multi-communication methods,” *Appl. Math. Nonlinear Sci.*, vol. 8, no. 2, pp. 1401–1414, 2023, doi: 10.2478/amns.2023.1.00043.
- [47] Y. Zhou and A. N. Ahmed, “Cryptocurrency and digital currency based on blockchain-enabled IoT: a bibliometric literature review,” *Multimed. Tools Appl.*, vol. 83, no. 12, pp. 35583–35606, 2024, doi: 10.1007/s11042-023-16726-7.
- [48] Y. Liu, “Blockchain and Machine Learning for Communications and Networking Systems,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020, doi: 10.1109/COMST.2020.2975911.
- [49] D. A. Abdul Kareem and D. Rajesh, “Enhancing WBAN Performance with Cluster-Based Routing Protocol Using Black Widow Optimization for Healthcare Application,” *J. Intell. Syst. Internet Things*, vol. 14, no. 1, pp. 45–58, 2025, doi: 10.54216/JISIoT.140104.
- [50] S. Boulfekhar and D. Aissani, “C-QoS-RP: Cluster Based QoS-Routing Protocol for VANET in Highway Environment,” *Autom. Control Comput. Sci.*, vol. 58, no. 3, pp. 313–325, 2024, doi: 10.3103/S0146411624700196.