Karapan Network
Journal

Vol.I, No.I, October 2025
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Analisis Peran dan Tantangan Keamanan Jaringan pada Wireless Sensor Network (WSN)

Habiburrahman[1)*], Ubaidillah Hamdi Putra[2)]

[1)2)] *Teknik, Universitas Madura, Pamekasan, Indonesia*

[1)] habiburrahman170706@gmail.com, [2)] ubaidillahhamdiputra@gmail.com

Abstrak

Wireless Sensor Network (WSN) adalah jaringan komunikasi nirkabel yang terdiri dari sejumlah sensor kecil yang digunakan untuk mengumpulkan, mengirimkan, dan mendeteksi informasi dari lingkungan sekitarnya. WSN sangat penting dalam berbagai bidang, termasuk industri, keamanan, kesehatan, dan pemantauan lingkungan. WSN sangat rentan terhadap berbagai risiko keamanan, termasuk pengubahan data, penyadapan, dan serangan penolakan layanan (DoS), karena sifatnya yang terbuka dan keterbatasan energi, memori, serta kemampuan pemrosesan. Oleh karena itu, keamanan jaringan merupakan komponen penting dalam penerapan WSN.Tujuan dari studi ini adalah untuk meneliti bagaimana keamanan jaringan berkontribusi terhadap kerahasiaan, ketersediaan, dan integritas data di WSN dan untuk mengidentifikasi hambatan utama dalam menerapkan langkah-langkah keamanan yang efektif dan dapat diandalkan.Melalui penelaahan berbagai sumber ilmiah, seperti jurnal, konferensi, dan standar keamanan jaringan, metodologi penelitian kualitatif deskriptif digunakan. Efektivitas dan keterbatasan beberapa protokol keamanan yang dibuat untuk WSN, termasuk TinySec, SPINS, dan LEAP, dalam mengatasi masalah keamanan, dikaji. Menurut analisis, protokol keamanan saat ini dapat menawarkan pertahanan dasar terhadap serangan yang sering terjadi, tetapi masih memiliki masalah serius terkait skalabilitas, penghematan energi, dan adaptasi terhadap perubahan kondisi jaringan. Selain itu, terdapat perbedaan antara keterbatasan sumber daya node sensor dan kebutuhan keamanan tingkat tinggi.Diperlukan strategi keamanan adaptif yang dapat menyeimbangkan antara perlindungan data dan efisiensi penggunaan sumber daya pada WSN. Pengembangan algoritma enkripsi ringan, manajemen kunci yang efisien, serta sistem deteksi serangan berbasis kecerdasan buatan dapat menjadi arah penelitian lanjutan dalam meningkatkan keamanan jaringan WSN di masa depan.

Keywords: Wireless Sensor Network, keamanan jaringan, protokol keamanan, ancaman keamanan, efisiensi energi.

Article history: Received 5 April 20XX, first decision 22 April 20XX, accepted 22 August 20XX, available online 28 October 20XX

I. PENDAHULUAN

Salah satu teknologi fundamental yang mendukung pertumbuhan Internet of Things (IoT) dan sistem siber-fisik kontemporer adalah Wireless Sensor Network (WSN) [1] [2] [3]. Teknologi ini menggunakan jaringan node sensor yang terhubung secara nirkabel dan tersebar luas untuk mengumpulkan, memproses, dan mengirimkan data dari dunia fisik ke stasiun pangkalan atau sistem pusat [4]. Unit sensor, mikrokontroler, modul komunikasi nirkabel, dan catu daya merupakan beberapa komponen penting yang dimiliki setiap node sensor [5] [6]. Komponen-komponen ini bekerja sama untuk mendeteksi perubahan lingkungan, memproses data secara lokal, dan mengirimkannya langsung ke stasiun pangkalan atau melalui simpul jaringan lainnya [7]. Dengan setiap simpul bertindak sebagai pengumpul data sekaligus perantara komunikasi, teknik ini memungkinkan sistem berfungsi secara terdistribusi dan independen. Informasi dikirim ke tujuan akhirnya melalui mekanisme komunikasi multi-hop [8] [9]. Oleh karena itu, bahkan pada jarak atau lokasi yang sangat jauh yang sulit diakses oleh infrastruktur komunikasi tradisional, Wireless Sensor Network dapat menyediakan pengiriman data yang efektif dan pemantauan lingkungan secara real-time [10] [11] [12].

Skalabilitas dan adaptabilitas arsitekturnya memungkinkannya untuk disesuaikan dengan berbagai kebutuhan aplikasi, baik dalam skala kecil maupun besar [13] [14], [15]. WSN dapat diimplementasikan pada beragam bidang strategis, seperti otomasi industri untuk pemantauan proses produksi secara real-time, deteksi kebakaran hutan yang memungkinkan respon cepat terhadap potensi bencana, sistem pertahanan militer untuk pengawasan wilayah dan deteksi intrusi, pemantauan ekosistem dalam menjaga keseimbangan lingkungan, hingga sistem pertanian cerdas (smart agriculture) yang mendukung efisiensi penggunaan air dan pupuk melalui analisis kondisi tanah dan cuaca secara otomatis [16] [17], [18] . Kemampuan ini menunjukkan bahwa WSN tidak hanya berperan sebagai alat pengumpul data, tetapi juga sebagai komponen kunci dalam sistem pengambilan keputusan berbasis data (data-driven decision systems) [19]. Dengan dukungan arsitektur yang fleksibel, efisien, serta mudah diintegrasikan dengan teknologi lain seperti Internet of Things (IoT) dan komputasi awan (cloud computing), WSN telah menjadi fondasi

[*] Habiburrahman

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.X.X.624-633

penting dalam pengembangan sistem cerdas dan terhubung di berbagai sektor modern [20], [21], [22]. Karena fitur-fitur ini, Wireless Sensor Network (WSN) merupakan teknologi krusial dalam pengembangan sistem siber-fisik dan Internet of Things (IoT), yang membutuhkan pengambilan keputusan berbasis data yang andal, konektivitas tinggi, dan efisiensi energi [23], [24]. Data dapat didistribusikan secara efektif dari area observasi yang luas ke pusat kendali untuk pemrosesan tambahan menggunakan sistem komunikasi multi-hop [25].

Pemantauan lingkungan, pemantauan industri, pertanian cerdas, sistem e-kesehatan, dan pengawasan militer hanyalah beberapa aplikasi yang sangat diuntungkan oleh fleksibilitas WSN, kemampuan pemantauan waktu nyata, dan biaya operasional yang relatif terjangkau [26]. Operasi otonom dan arsitektur adaptif WSN telah menjadikannya komponen vital dalam ekosistem Internet of Things (IoT) dan pergeseran menuju sistem siber-fisik yang cerdas dan saling terhubung [27] [28]. Pemantauan lingkungan, pengendalian kualitas udara, deteksi bencana alam, layanan kesehatan cerdas, otomasi industri, sistem transportasi cerdas, serta aplikasi militer dan keamanan hanyalah beberapa bidang di mana WSN memainkan peran strategis yang krusial [29].

WSN diimplementasikan secara terdistribusi dan otonom, dengan setiap node sensor bertugas mengidentifikasi perubahan lingkungan (seperti suhu, kelembapan, tekanan, atau getaran) dan mengirimkan informasi tersebut ke node penerima atau gateway melalui jaringan multi-hop [30]. Setelah itu, data ini diperiksa untuk memfasilitasi pengambilan keputusan secara langsung. WSN merupakan pilihan yang baik untuk memantau sistem di daerah terpencil atau tempat yang sulit dijangkau oleh jaringan kabel tradisional karena skalabilitas dan fleksibilitasnya [31] [32].

Namun, WSN memiliki sejumlah kendala mendasar, terutama di bidang keamanan dan efisiensi energi, terlepas dari manfaat dan potensi penggunaannya yang luas [32]. Node sensor biasanya memiliki sumber daya yang minim, seperti daya pemrosesan yang rendah, kapasitas baterai yang kecil, dan memori yang terbatas [33]. Oleh karena itu, penerapan langkah-langkah keamanan tradisional seperti enkripsi yang kuat atau autentikasi yang rumit tidaklah efektif atau bahkan mustahil. Akibatnya, WSN sangat rentan terhadap sejumlah risiko keamanan, termasuk penetrasi node, serangan intrusi, serangan Denial of Service (DoS), pencurian data, dan manipulasi paket [34].

Lebih lanjut, risiko serangan fisik dan peretasan jaringan meningkat karena node sensor sering beroperasi di tempat berbahaya tanpa pengawasan ketat (seperti zona militer, hutan, atau kawasan industri) [35][36]. Integritas data, keandalan komunikasi, dan bahkan kegagalan sistem dapat sangat terganggu jika sistem tidak dapat mengidentifikasi dan merespons ancaman dengan cepat [37] [38]. Akibatnya, salah satu kebutuhan paling mendesak dalam penelitian WSN kontemporer adalah pengembangan langkah-langkah keamanan yang efektif, fleksibel, dan hemat energi.

Beberapa penelitian terbaru menunjukkan bahwa aplikasi pembelajaran mesin (machine learning) mulai digunakan untuk menguatkan keamanan WSN melalui deteksi intrusi adaptif dan analisis perilaku node, namun masih menghadapi tantangan dalam hal latensi, kebutuhan data pelatihan, dan kompatibilitas dengan hardware sensor yang terbatas [39][40]. Selain itu, kajian terkini juga menyebutkan bahwa sebagian besar riset masih berfokus pada ancaman dan protokol secara umum, sementara implementasi di skenario dunia nyata, skala besar, dan heterogen masih kurang - hal ini menandakan adanya gap riset yang perlu ditangani [41].

Untuk mengatasi masalah ini, berbagai pendekatan baru telah diciptakan, seperti penggunaan deteksi anomali berbasis pembelajaran mesin, teknik optimasi metaheuristik, dan integrasi komputasi tepi, yang semuanya bertujuan untuk meningkatkan efektivitas keamanan tanpa mengorbankan kinerja jaringan atau penggunaan energi [41]. Bahkan dalam menghadapi bahaya yang tidak diketahui, teknik pembelajaran mesin memungkinkan sistem untuk secara adaptif mendeteksi perilaku mencurigakan dan mengidentifikasi pola aktivitas yang umum [42]. Sementara itu, pemilihan rute, penjadwalan energi, dan distribusi beban komputasi dioptimalkan menggunakan metode optimasi metaheuristik termasuk Particle Swarm Optimization (PSO), Genetic Algorithm (GA), dan Ant Colony Optimization (ACO) untuk meningkatkan umur jaringan.

II. TINJAUAN PUSTAKA

Wireless Sensor Network (WSN) telah menjadi bagian penting dari sistem siber-fisik dan Internet of Things (IoT) kontemporer. Dengan banyaknya sensor yang tersebar di berbagai lokasi, WSN memungkinkan pengumpulan data terdistribusi untuk memantau aktivitas industri, kesehatan, faktor lingkungan, dan bahkan aplikasi militer. Namun, terdapat kesulitan yang signifikan, terutama terkait keamanan jaringan, karena fitur dasar node sensor, yang meliputi keterbatasan energi, memori, dan daya komputasi. Empat prinsip utama keamanan jaringan WSN adalah ketersediaan, kerahasiaan, integritas, dan autentikas. WSN biasanya beroperasi di area terbuka dengan risiko akses fisik dan penyadapan komunikasi yang substansial, sehingga sulit untuk memenuhi kriteria ini [43] [44]

Banyak upaya telah dilakukan dalam 20 tahun terakhir untuk menciptakan langkah-langkah keamanan yang mempertimbangkan keterbatasan sumber daya WSN. Metode kriptografi konvensional seperti AES dan RSA, yang

menawarkan tingkat perlindungan tinggi tetapi membutuhkan daya pemrosesan dan energi yang besar, merupakan bagian penting dari strategi keamanan awal. Untuk mencapai keseimbangan antara kekuatan perlindungan dan efisiensi energi, sejumlah protokol keamanan ringan, termasuk SPINS, TinySec, dan LEAP, telah dikembangkan. Namun, skalabilitas dan adaptabilitas protokol-protokol ini masih terbatas, terutama ketika jaringan sensor berkembang ke skala yang besar dan beragam. Selain itu, sistem keamanan statis seperti itu sulit beradaptasi dengan ancaman siber yang terus berubah [45][46].

Wireless Sensor Network (WSN) telah menjadi bagian penting dari sistem siber-fisik dan Internet of Things (IoT) kontemporer. Dengan banyaknya sensor yang tersebar di berbagai lokasi, WSN memungkinkan pengumpulan data terdistribusi untuk memantau aktivitas industri, kesehatan, faktor lingkungan, dan bahkan aplikasi militer. Namun, terdapat kesulitan yang signifikan, terutama terkait keamanan jaringan, karena fitur dasar node sensor, yang meliputi keterbatasan energi, memori, dan daya komputasi. Empat prinsip utama keamanan jaringan WSN adalah ketersediaan, kerahasiaan, integritas, dan autentikasi. WSN biasanya beroperasi di area terbuka dengan risiko akses fisik dan penyadapan komunikasi yang substansial, sehingga sulit untuk memenuhi kriteria ini.

Integrasi studi-studi ini mengungkap kesenjangan penelitian yang mencolok: kebutuhan akan model keamanan hibrida yang dapat secara efektif menggabungkan sistem deteksi cerdas dengan kriptografi ringan. Area studi potensial adalah metode adaptif yang dapat memodifikasi tingkat deteksi intrusi, strategi perutean, dan kekuatan enkripsi sebagai respons terhadap ketersediaan sumber daya dan variabel lingkungan. Oleh karena itu, dengan menyoroti perlunya menciptakan kerangka kerja keamanan adaptif yang efisien, hemat energi, dan dapat diterapkan secara global untuk mendukung keberlanjutan sistem WSN di masa depan, penelitian ini secara signifikan memajukan pemahaman kita tentang peran dan kesulitan keamanan dalam WSN.

III. METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur yang bertujuan untuk menganalisis peran dan tantangan keamanan jaringan pada Wireless Sensor Network (WSN) [47] [48]. Data penelitian berupa data sekunder yang diperoleh dari jurnal internasional bereputasi, prosiding, dan laporan ilmiah terbitan tahun 2019–2024 yang membahas topik keamanan WSN, termasuk aspek enkripsi, autentikasi, deteksi intrusi, efisiensi energi. Proses pengumpulan data dilakukan melalui tahapan identifikasi, seleksi, evaluasi, dan sintesis terhadap literatur yang relevan menggunakan kata kunci seperti “Wireless Sensor Network security”, “lightweight encryption”, dan “intrusion detection”. Analisis dilakukan dengan analisis isi (content analysis) untuk menelaah empat aspek utama keamanan jaringan, yaitu kerahasiaan, integritas, autentikasi, dan ketersediaan. Tahapan penelitian meliputi pengumpulan dan klasifikasi literatur berdasarkan fokus penelitian, analisis dan perbandingan hasil penelitian terdahulu, serta penyusunan sintesis untuk menemukan pola dan kesenjangan penelitian. Validitas data dijaga dengan hanya menggunakan sumber akademik bereputasi dan melakukan cross-comparison antar hasil penelitian guna memastikan konsistensi dan keandalan informasi [49] [50]. Hasil dari proses ini memberikan gambaran menyeluruh tentang tren, pendekatan, serta tantangan yang masih dihadapi dalam pengembangan keamanan jaringan WSN yang efisien dan adaptif.

IV. HASIL

Penelitian ini menghasilkan temuan yang fokus pada analisis peran serta tantangan keamanan jaringan pada Wireless Sensor Network (WSN) berdasarkan kajian literatur dari berbagai jurnal nasional Indonesia. Hasil menunjukkan bahwa WSN memiliki peran signifikan dalam berbagai bidang aplikasi seperti pemantauan bencana alam, lingkungan, industri, dan sistem IoT. Namun, keterbatasan sumber daya sensor node menyebabkan tantangan besar dalam penerapan sistem keamanan yang optimal.

Beberapa penelitian juga menegaskan bahwa penerapan nyata WSN di lapangan masih terbatas, sehingga diperlukan pendekatan keamanan yang lebih aplikatif dan hemat daya untuk konteks lokal.

No	Sumber (Jurnal / Tahun)	Fokus penelitian	Temuan utama	Implikasi terhadap keamanan WSN
1	ELKHA – Jurnal Teknik Elektro Universitas Tanjungpura (2022)	Implementasi WSN untuk deteksi gempa	Menunjukkan desain sistem sensor gempa berbasis WSN yang efisien, namun menghadapi kendala energi dan keandalan komunikasi.	Diperlukan mekanisme keamanan dan efisiensi daya yang seimbang untuk memastikan kontinuitas data sensor di lapangan.

2.	J-PTIIK Universitas Brawijaya (2022)	Implementasi algoritme kriptografi ringan SPECK pada node sensor	Algoritme SPECK menurunkan overhead enkripsi dan konsumsi energi dibandingkan AES.	Kriptografi ringan efektif menjaga keseimbangan antara keamanan dan efisiensi sumber daya pada node sensor.
3.	TELKOMNIKA (Universitas Ahmad Dahlan, 2019)	Protokol MAC hemat energi untuk WSN	Pengaturan *duty cycle* berpengaruh langsung terhadap umur jaringan dan efisiensi komunikasi.	Desain lapisan MAC harus selaras dengan sistem keamanan agar tidak memperbesar beban energi.
4.	JNTETI Universitas Gadjah Mada (2020)	Analisis ancaman dan mitigasi keamanan IoT berbasis WSN	Ancaman *Denial of Service* dan *Eavesdropping* masih dominan di aplikasi sensor nasional.	Diperlukan pendekatan kebijakan dan teknis dalam membangun sistem keamanan nasional berbasis IoT.
5.	E-Journal UNIKAMA (2024)	Privasi data dan efisiensi algoritma enkripsi	Enkripsi ringan menjaga privasi data namun menurunkan throughput komunikasi jaringan.	Diperlukan penyesuaian algoritma enkripsi sesuai jenis aplikasi WSN (monitoring, surveillance, industri).
6.	JISTI / Jurnal Informatika dan Sains Teknologi Indonesia (2023)	Penerapan *Wireless Intrusion Detection System* (WIDS) untuk WSN	WIDS efektif dalam mendeteksi serangan pada jaringan sensor lokal, meskipun *false positive* masih tinggi.	Menunjukkan potensi penerapan deteksi intrusi berbasis anomali dalam konteks jaringan sensor nasional.

Menurut laporan yang disebutkan di atas, penelitian di Indonesia telah mencapai kemajuan pesat dalam pengembangan sistem keamanan WSN, terutama di bidang deteksi intrusi dan efisiensi energi. Protokol MAC hemat energi dengan kontrol siklus kerja dan teknik kriptografi ringan seperti SPECK telah terbukti dapat menurunkan beban sistem tanpa mengorbankan keamanan data sensor.

Namun, penerapan praktis di lapangan masih menjadi kendala terbesar, terutama untuk aplikasi yang melibatkan pemantauan lingkungan dan bencana alam yang membutuhkan komunikasi berkelanjutan dan konsumsi daya rendah. Sistem sensor di Indonesia masih cukup rentan terhadap serangan DoS dan gangguan komunikasi, menurut penelitian oleh ELKHA (2022) dan JNTETI (2020). Oleh karena itu, diperlukan langkah-langkah keamanan yang ringan dan adaptif terhadap karakteristik unik sumber daya lokal.

Selain itu, menurut analisis JISTI pada tahun 2023, sistem deteksi intrusi nirkabel (WIDS) dapat menjadi cara yang layak untuk memantau keamanan jaringan secara waktu nyata (real-time). Diharapkan bahwa penggabungan teknologi ini akan meningkatkan keamanan WSN Indonesia bila dipadukan dengan manajemen energi cerdas dan kriptografi ringan.

V. PEMBAHASAN

Dalam konteks aplikasi di Indonesia, yang menghadapi kendala infrastruktur, sumber daya energi, dan kemampuan komputasi simpul sensor, analisis literatur menunjukkan bahwa keamanan jaringan merupakan elemen krusial dalam pengembangan Wireless Sensor Network (WSN). Literatur yang dikaji berulang kali menunjukkan bahwa kendala-kendala ini telah menghambat optimalisasi fitur keamanan secara menyeluruh, termasuk deteksi intrusi, autentikasi, dan enkripsi. Dengan demikian, kesimpulan utama dari studi ini adalah bahwa taktik keamanan WSN harus disesuaikan dengan kebutuhan aplikasi dan lingkungan operasinya, alih-alih diterapkan secara universal.

Mayoritas penelitian di Indonesia masih berfokus pada simulasi skala kecil dan pengembangan prototipe, alih-alih implementasi lapangan, berbeda dengan penelitian yang dilakukan di luar negeri. Hal ini didukung oleh penelitian dari ELKHA (2022) dan JNTETI (2020), yang menekankan masalah efisiensi energi dalam sistem pemantauan bencana. Mayoritas langkah-langkah keamanan masih dievaluasi dalam skala kecil, yang berarti langkah-langkah tersebut belum secara akurat merepresentasikan kompleksitas situasi dunia nyata. Sementara itu, studi yang dilakukan oleh TELKOMNIKA (2019) dan J-PTIIK Universitas Brawijaya (2022) secara efektif menggambarkan bagaimana algoritma kriptografi ringan dan pengaturan siklus kerja dapat menurunkan konsumsi energi, yang konsisten dengan temuan penelitian internasional seperti Liu dkk. (2021). Hal ini menunjukkan bahwa meskipun penelitian di Indonesia mengikuti tren global, penelitian tersebut masih membutuhkan dukungan empiris yang lebih luas

UNIKAMA (2024) dan JISTI (2023) telah membuat kemajuan signifikan dalam implementasi sistem keamanan yang lebih adaptif. Keduanya menyajikan metode deteksi intrusi dan keamanan berbasis privasi, yang menunjukkan hasil menjanjikan dalam mengurangi risiko kerahasiaan dan integritas data. Temuan ini juga menunjukkan adanya trade-off antara kinerja jaringan dan tingkat keamanan. Misalnya, peningkatan enkripsi meningkatkan penundaan komunikasi dan mengurangi throughput. Kesulitan ini menunjukkan bahwa untuk meningkatkan keamanan WSN, efisiensi energi dan manajemen sumber daya jaringan harus dioptimalkan secara bersamaan.

Hasil ini mendukung gagasan bahwa keamanan WSN merupakan hasil dari trade-off multifaset antara kinerja, konsumsi energi, dan tingkat perlindungan data dalam kerangka teori sistem jaringan. Untuk WSN skala besar dengan sumber daya terbatas, langkah-langkah keamanan yang terlalu rumit tidaklah tepat. Di sisi lain, sistem yang terlalu ringan rentan terhadap penyadapan dan serangan replay. Oleh karena itu, studi ini membantu dalam penciptaan kerangka kerja baru yang menyoroti pentingnya desain keamanan adaptif, atau sistem yang dapat memodifikasi tingkat perlindungan sebagai respons terhadap kondisi jaringan dan persyaratan aplikasi.

Dari berbagai penelitian tersebut, terlihat bahwa pendekatan kriptografi ringan dan sistem deteksi intrusi merupakan dua strategi utama yang saling melengkapi dalam memperkuat keamanan WSN. Kriptografi ringan menjaga aspek kerahasiaan dan integritas data, sementara sistem WIDS berfungsi sebagai lapisan pertahanan dinamis terhadap ancaman eksternal. Pendekatan ganda ini sangat relevan diterapkan di Indonesia, di mana keterbatasan sumber daya energi dan infrastruktur jaringan masih menjadi kendala utama.

Secara keseluruhan, pembahasan ini menunjukkan bahwa penelitian-penelitian WSN di Indonesia telah berkontribusi secara teoretis dan praktis terhadap pengembangan sistem keamanan jaringan yang lebih efisien dan kontekstual. Secara teoretis, penelitian ini memperkaya literatur nasional dengan menegaskan pentingnya keseimbangan antara efisiensi energi dan keamanan data sebagai dasar pengembangan arsitektur WSN yang berkelanjutan. Sementara secara praktis, hasil-hasil tersebut dapat menjadi rujukan dalam penerapan sistem keamanan pada berbagai sektor, seperti mitigasi bencana, lingkungan, industri, dan pertanian cerdas. Ke depan, pengembangan teknologi deteksi intrusi berbasis kecerdasan buatan serta implementasi lapangan berskala besar menjadi peluang yang menjanjikan untuk memperkuat keamanan dan keandalan WSN di Indonesia

Sumber utama kelemahan penelitian ini adalah ketergantungannya pada sumber sekunder. Membandingkan hasil terkadang dapat menjadi masalah karena tidak semua makalah yang diteliti memiliki data eksperimen yang sebanding. Lebih lanjut, alih-alih berfokus pada integrasi sistem dunia nyata yang mempertimbangkan elemen lingkungan seperti interferensi sinyal dan karakteristik geografis Indonesia, sebagian besar sumber masih berfokus pada pengembangan perangkat lunak. Hal ini merupakan batasan yang perlu dipertimbangkan ketika menganalisis hasil penelitian.

Penelitian di masa mendatang sebaiknya berfokus pada pembuatan dan pengujian sistem keamanan WSN dalam penerapan dunia nyata, dengan mempertimbangkan faktor geografis dan energi setempat, berdasarkan temuan dan analisis ini. Selain itu, jalur penelitian yang berpotensi bermanfaat adalah kolaborasi sistem deteksi intrusi berbasis pembelajaran mesin dengan teknik kriptografi ringan. Untuk mencapai kompromi antara keamanan dan efisiensi, penelitian di masa mendatang sebaiknya juga menyelidiki metode keamanan adaptif yang dapat memodifikasi tingkat perlindungan sebagai respons terhadap kondisi beban jaringan.

VI. KESIMPULAN

Permasalahan dan solusi implementasi dalam situasi keterbatasan sumber daya, seperti konteks Indonesia, menjadi fokus utama analisis sistematis studi ini terhadap literatur tentang keamanan jaringan dalam Wireless Sensor Network (JSN). Karena keamanan secara langsung memengaruhi ketersediaan, kerahasiaan, dan integritas data yang menjadi dasar pengambilan keputusan berbasis sensor, analisis ini menunjukkan bahwa keamanan merupakan komponen krusial dalam desain dan implementasi JSN.

Literatur yang dikaji menunjukkan bahwa langkah-langkah keamanan JSN masih belum sepenuhnya optimal, terutama karena keterbatasan infrastruktur jaringan, daya, dan kapabilitas pemrosesan. Belum banyak penelitian di Indonesia yang telah mencapai tingkat penerapan di dunia nyata; sebagian besar masih dalam tahap simulasi dan pengembangan prototipe. Namun, penelitian nasional telah mulai mengikuti tren internasional, terutama di bidang deteksi intrusi berbasis kecerdasan buatan, manajemen energi adaptif, dan kriptografi ringan.

Kontribusi utama penelitian ini adalah untuk mendukung pendekatan keamanan adaptif dalam desain WSN, yang menyatakan bahwa tingkat keamanan harus disesuaikan dengan situasi operasi, arsitektur jaringan, dan karakteristik aplikasi, alih-alih seragam. Studi ini juga menunjukkan bahwa keamanan WSN merupakan trade-off multifaset antara kinerja jaringan, efisiensi energi, dan perlindungan data. Kinerja dapat terganggu akibat strategi yang terlalu rumit, dan serangan lebih mungkin terjadi pada sistem yang terlalu ringan. Oleh karena itu, untuk mencapai keseimbangan antara perlindungan dan kinerja, diperlukan langkah-langkah keamanan kontekstual dan adaptif.

Temuan praktis studi ini membantu pengembang, akademisi, dan regulator menciptakan sistem keamanan WSN yang efektif dan sesuai dengan kebutuhan regional, terutama untuk penggunaan dalam otomasi industri, pemantauan lingkungan, dan tanggap bencana. Dari sudut pandang akademis, studi ini memperluas pengetahuan tentang bagaimana keamanan, penggunaan energi, dan desain jaringan berinteraksi dalam pengaturan WSN dengan sumber daya terbatas.

Desain tinjauan pustaka sekunder dalam studi ini merupakan salah satu keterbatasannya; beberapa sumber yang diteliti tidak memiliki data eksperimen, metodologi, dan latar belakang implementasi yang serupa. Perbedaan ini dapat memengaruhi sejauh mana temuan dapat diterapkan. Efektivitas model keamanan dalam kondisi geografis dan energi aktual harus dinilai melalui uji lapangan langsung, atau penerapan di dunia nyata, sebagaimana ditunjukkan oleh temuan dan kendala ini. Pendekatan penelitian menarik lainnya untuk menciptakan sistem keamanan yang fleksibel, efektif, dan tangguh adalah kombinasi deteksi intrusi berbasis pembelajaran mesin dan enkripsi ringan. Untuk mencapai keseimbangan yang stabil antara efisiensi dan perlindungan data, penelitian di masa mendatang juga harus mencakup sistem untuk memodifikasi pengaturan keamanan secara dinamis berdasarkan beban jaringan dan kondisi energi.

Author Contributions: *[Habiburrahman]: Konseptualisasi, Metodologi, Penulisan - Draf Asli, Penulisan - Tinjauan & Penyuntingan, Supervisi. [Ubaidillah Hamdi Putra Pratama]: Perangkat Lunak, Investigasi, Kurasi Data, Penulisan - Draf Asli*.

Semua penulis telah membaca dan menyetujui versi naskah yang diterbitkan.

Pendanaan: -
Ucapan Terima Kasih: -
Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan
Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia
Ketersediaan Data: -
Penulis Pertama: https:
Penulis Kedua: https:
Penulis Ketiga: -

REFERENSI

[1] s. Safiuddin and f. P. E. Putra, “strategi efisiensi wireless sensor network (wsn),” *informatics for educators and professional : journal of informatics*, vol. 8, no. 1, p. 52, jul. 2023, doi: 10.51211/itbi.v8i1.2441.

[2] b. Herdiana, e. B. Setiawan, and u. Sartoyo, “tinjauan komprehensif evolusi, aplikasi, dan tren masa depan programmable logic controllers (a comprehensive review of the evolution, applications, and future trends of programmable logic controllers),” *telekontran : jurnal ilmiah telekomunikasi, kendali dan elektronika terapan*, vol. 11, no. 2, pp. 173–193, jul. 2024, doi: 10.34010/telekontran.v11i2.12896.

[3] m. R, y. Fahdillah, m. Kadar, i. Hassandi, and m. R, “implementasi transformasi digital dan kecerdasan buatan sebagai inovasi untuk umkm pada era revolusi industri 4.0,” *jurnal ilmiah manajemen dan kewirausahaan (jumanage)*, vol. 3, no. 1, jan. 2024, doi: 10.33998/jumanage.2024.3.1.1552.

[4] n. I. Putri, “deep learning dan teknologi big data untuk keamanan iot,” *computing| jurnal informatika*, vol. 7, no. 1, pp. 48–73, 2020, doi: https://doi.org/10.55222/computing.v7i1.555.

[5] m. A. Santiko, d. Eridani, and a. F. Rochim, “komunikasi long range dan gateway dalam penerimaan data multi-node sensor pada sistem monitoring. Jurnal teknik komputer, 2(1), 16-20.,” *jurnal teknik komputer*, vol. 2, no. 1, pp. 16–20, 2023, doi: https://doi.org/10.14710/jtk.v2i1.38003.

[6] a. Pratama, a. N. Amrita, and d. C. Khrisne, “rancang bangun sistem monitoring listrik tiga fasa berbasis wireless sensor network menggunakan lora ra-02 sx1278,” *majalah ilmiah teknologi elektro*, vol. 20, no. 2, pp. 351–360, 2021, doi: doi.org/10.24843/mite.2021.v20i02.p20.

[7] f. P. E. Putra, m. Riski, m. S. Yahya, and m. H. Ramadhan, “mengenal teknologi jaringan nirkabel terbaru teknologi 5g,” *jurnal sistim informasi dan teknologi*, pp. 167–174, 2023, doi: https://doi.org/10.37034/jsisfotek.v5i2.233.

[8] n. F. R. Hutabarat, r. Sirait, and d. H. S. Napitu, “analisa unjuk kerja nrf24l01 pada komunikasi multi hop dengan database lokal,” *teknologi rekayasa jaringan telekomunikasi*, vol. 1, no. 2, pp. 97–106, 2021, doi: https://doi.org/10.51510/trekritel.v1i1.___.

[9] b. H. Maay and i. R. Widiasari, "analisis performa wireless sensor network dengan protokol multi hop dan single hop," *jipi (jurnal ilmiah penelitian dan pembelajaran informatika)*, vol. 9, no. 3, pp. 1112–1122, aug. 2024, doi: 10.29100/jipi.v9i3.4917.

[10] f. Rahmansyah and p. Murdiyat, "rancang bangun sistem monitoring pertanian cerdas berbasis lora untuk pemantauan kondisi persawahan secara real-time," *poligrid*, vol. 6, no. 1, 2025, doi: https://doi.org/10.46964/poligrid.v6i1.62.

[11] z. Setiawan, a. Hiswara, and h. N. Muthmainah, "mengoptimalkan jaringan sensor nirkabel dalam aplikasi monitor lingkungan dengan teknologi iot di indonesia," *jurnal multidisiplin west science*, vol. 2, no. 10, pp. 858–867, 2023, doi: https://doi.org/10.58812/jmws.v4i09.

[12] m. S. Gitakarma, k. U. Ariawan, and i. G. M. S. B. Pracasitaram, "peran mikrokontroler dalam pengembangan aplikasi iot: tinjauan konseptual dan implementasi," *komteks*, vol. 3, no. 2, pp. 18–24, jan. 2025, doi: 10.37637/komteks.v3i2.2231.

[13] putra.f.p.e, s. M. Dewi, maugfiroh, and a. Hamzah, "privasi dan keamanan penerapan iot dalam kehidupan sehari-hari : tantangan dan implikasi," *jurnal sistim informasi dan teknologi*, pp. 26–32, 2023, doi: https://doi.org/10.37034/jsisfotek.v5i2.232.

[14] m. Ilham, f. Adiansyah, and isa faqihanuddin hanif, "arsitektur sistem terdistribusi untuk enterprise: model desain dan implementasi," *jurnal rekayasa sistem informasi dan teknologi*, vol. 2, no. 4, pp. 1344–1451, may 2025, doi: 10.70248/jrsit.v2i4.2361.

[15] f. P. Eka putra, . S., a. Ramadhani, and . M., "integrasi teknologi kuantum dan fiber optik untuk meningkatkan keamanan dan efisiensi jaringan masa depan," *jurnal ilmiah ilkominfo - ilmu komputer & informatika*, vol. 8, no. 2, pp. 151–163, jul. 2025, doi: 10.47324/ilkominfo.v8i2.342.

[16] b. Wahyudi, muhammad danu, fahrurrozi mawasandi, zakaria nur aziz, and m. Fahrul ghifari rosyadi, "transformasi manajemen rantai pasokan berbasis internet of things (iot): tinjauan literatur," *jurnal teknologi dan manajemen industri terapan*, vol. 4, no. I, pp. 32–44, mar. 2025, doi: 10.55826/jtmit.v4ii.535.

[17] d. G. Putra, "peningkatan kinerja bisnis melalui integrasi internet of things (iot) pada supply chain management (scm)," *jurnal marketing*, vol. 5, no. 2, pp. 379–387, 2024, accessed: oct. 22, 2025. [online]. Available: http://ojs.stiepi.ac.id/index.php/marketing/article/view/171/108

[18] muhammad zidhan augestri, achmad fauzi, aqila naima khairunnisa, dyah ayu siti sundari, revi arnan, and yeremia todo sihombing, "penerapan teknologi iot dalam optimalisasi rantai pasok industri logistik," *jurnal manajemen dan pemasaran digital*, vol. 3, no. 2, pp. 158–173, jun. 2025, doi: 10.38035/jmpd.v3i2.388.

[19] f. P. E. Putra, a. Baidawi, and a. A. Mubarok, "merancang jaringan sensor nirkabel dan iot untuk kota pintar pamekasan," *jurnal informasi dan teknologi*, vol. 5, no. 2, pp. 138–145, 2023, doi: doi:10.37034/jidt.v5i1.331.

[20] f. P. E. Putra, m. A. Mahmud, and i. S. Maqom, "pengembangan sistem pemantauan lingkungan berbasis internet of things (iot) di kampus," *digit. Transform*, vol. 3, no. 2, pp. 996–1001, 2023, doi: https://doi.org/10.47709/digitech.v3i2.3457.

[21] a. Leto, "serverless computing: kajian literatur untuk memahami arsitektur dan implikasinya di era cloud computing," *integrative perspectives of social and science journal*, vol. 2, no. 2, pp. 2236–2247, apr. 2025, accessed: oct. 22, 2025. [online]. Available: https://ipssj.com/index.php/ojs/article/view/312/295

[22] a. Herwanto, "peluang bisnis baru di industri 5.0 dengan iot, ai, dan cloud computing," *jurnal informasi dan teknologi*, vol. 2, no. 1, pp. 24–31, 2025, accessed: oct. 22, 2025. [online]. Available: https://pustakailmiah.web.id/index.php/jitu/article/view/115

[23] b. Rusandi, "penerapan digitalisasi camera analytic guna meningkatkan tingkat kepatuhan driver dan menurunkan tingkat kecelakaan dump truck (dt) di jalan hauling batubara pt. Xyz," *jurnal bisnis dan pembangunan*, vol. 14, no. 1, pp. 1–9, 2025, doi: https://doi.org/10.20527/jbp.1414i1.63.

[24] f. P. E. Putra, f. Muslim, n. Hasanah, r. Paradina, and r. Alim, "analisis komparasi protokol websocket dan mqtt dalam proses push notificatio," *jurnal sistim informasi dan teknologi*, pp. 63–72, 2023, doi: https://doi.org/10.60083/jsisfotek.v5i4.325.

[25] r. Astarina, l. A. S. I. Akbar, and d. F. Budiman, "implementasi routing static multi hop pada perangkat lora," *jurnal informatika dan teknik elektro terapan*, vol. 12, no. 3, 2024, doi: https://doi.org/10.23960/jitet.v12i3.5228.

[26] f. P. Eka putra, ach. M. Ubaidillah solichin, moh. N. Wildanul hakim, and m. T. Ramadhan, "pemanfaatan teknologi wireless dan mobile network berbasis 5g untuk pemerataan akses jaringan di indonesia," *infotek: jurnal informatika dan teknologi*, vol. 8, no. 2, pp. 415–425, jul. 2025, doi: 10.29408/jit.v8i2.30559.

[27] 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, doi: doi:10.55606/jitek.v5i1.6141.

[28] f. P. E. Putra and n. Saadah, "interaktif dan personalisasi peningkatan pembelajaran iot di sekolah," *jurnal sistim informasi dan teknologi*, pp. 175–181, 2023, doi: https://doi.org/10.37034/jsisfotek.v5i2.236.

[29] z. Setiawan, a. Hiswara, and h. N. Muthmainah, "mengoptimalkan jaringan sensor nirkabel dalam aplikasi monitor lingkungan dengan teknologi iot di indonesia," *jurnal multidisiplin west science*, vol. 2, no. 10, pp. 858–867, 2023, doi: https://doi.org/10.58812/jmws.v4i09.

[30] r. D. Prasetia and i. R. Widiasari, "perancangan iot monitoring lingkungan berbasis wireless sensor network (wsn) dengan menerapkan multi sensor network (msn)," *jipi (jurnal ilmiah penelitian dan pembelajaran informatika)*, vol. 10, no. 1, pp. 652–666, 2025.

[31] r. Susana, f. Hadiatna, and a. Gusmantini, "sistem multihop jaringan sensor nirkabel pada media transmisi wi-fi," *elkomika: jurnal teknik energi elektrik, teknik telekomunikasi, & teknik elektronika*, vol. 9, no. 1, p. 232, jan. 2021, doi: 10.26760/elkomika.v9i1.232.

[32] f. H. E. Ratuloli, a. S. Budi, and a. Bhawiyuga, "implementasi skema anti-collision menggunakan metode tdma dan tpsn pada sistem wsn berbasis lora," *jurnal pengembangan teknologi informasi dan ilmu komputer*, vol. 5, no. 1, pp. 283–290, 2021.

[33] h. Subagiyo, r. Rhamadani, and r. T. Wahyuni, "penghematan daya pada sensor node sistem monitoring kualitas udara," *ijeis (indonesian journal of electronics and instrumentation systems)*, vol. 13, no. 2, oct. 2023, doi: 10.22146/ijeis.81886.

[34] j. A. Prabowo and h. Dhika, "safe routing model and balanced load model for wireless sensor network," *cyberspace: jurnal pendidikan teknologi informasi*, vol. 5, no. 1, p. 44, mar. 2021, doi: 10.22373/cj.v5i1.8420.

[35] ade irawan, wildan hamzah nur fadholi, zahwa erikamaretha, and fried sinlae, "tantangan dan strategi manajemen keamanan siber di indonesia berbasis iot," *journal zetroem*, vol. 6, no. 1, pp. 114–119, apr. 2024, doi: 10.36526/ztr.v6i1.3376.

[36] a. Irfan, a. Z. Nusri, z. Rachmat, and s. Wulandari, "analisis keamanan jaringan nirkabel menggunakan wireless intrusion detection system (wids)," *jurnal ilmiah sistem informasi dan teknik informatika (jisti)*, vol. 7, no. 1, pp. 110–119, apr. 2024, doi: 10.57093/jisti.v7i1.195.

[37] m. O. Hoshmand and s. Ratnawati, " analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity," *jurnal sains dan teknologi*, vol. 5, no. 2, pp. 679–686, 2023.

[38] y. Yanti, t. Hidayat, and d. Wahyudi, "sistem keamanan data privacy pada jaringan sensor nirkabel menggunakan teknik routing," *smartics journal*, doi: 10.21067/smartics.v10i1.9186.

[39] r. P. Simanjuntak and r. R. M. Sijabat, "meningkatkan keamanan siber dalam lingkungan internet of things (iot) dengan menggunakan sistem deteksi intrusi berbasis pembelajaran mesin," *dike : jurnal ilmu multidisiplin*, vol. 2, no. 2, pp. 62–68, aug. 2024, doi: 10.69688/dike.v2i2.106.

[40] t. Yuliswar, i. Elfitri, and o. W purbo, "optimization of intrusion detection system with machine learning for detecting distributed attacks on server," *inovtek polbeng - seri informatika*, vol. 10, no. 1, pp. 367–376, feb. 2025, doi: 10.35314/vem9da98.

[41] w. Soetrisno, w. Y. Azhar, a. B. Purba, a. Hilman, v. A. Lestari, and a. N. Mutawally, "meningkatkan keamanan dan mitigasi pada arsitektur software defined network," *jurnal interkom: jurnal publikasi ilmiah bidang teknologi informasi dan komunikasi*, vol. 20, no. 1, pp. 18–28, 2025.

[42] t. G. Laksana and s. Mulyani, "pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan," *jurnal ilmiah multidisiplin*, vol. 3, no. 01, pp. 109–122, jan. 2024, doi: 10.56127/jukim.v3i01.1143.

[43] p. C. Lumbanraja and p. L. Lumbanraja, " tinjauan sistematis: transformasi pelayanan metrologi di era digital (metrologi digital4. 0). ," *cendekia niaga*, vol. 8, no. 2, pp. 119–133, 2024, accessed: oct. 22, 2025. [online]. Available: https://jurnal.kemendag.go.id/index.php/jcn/article/view/912/422

[44] "implementasi algoritme speck pada wireless sensor network menggunakan media pengiriman data nrf24l01," *jurnal pengembangan teknologi informasi dan ilmu komputer*, vol. 6, no. 5, pp. 2079–2086, [online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/10978

[45] h. Hadiwiyatno, s. Wirayoga, i. I. A. Habibi, and m. Huda, "implementasi keamanan jaringan nirkabel menggunakan proteksi paket header untuk meningkatkan integritas data di greenhouse," *jurnal penelitian inovatif*, vol. 4, no. 4, pp. 2289–2296, nov. 2024, doi: 10.54082/jupin.777.

[46] w. Najib, s. Sulistyo, and widyawan, "tinjauan ancaman dan solusi keamanan pada teknologi internet of things," *jurnal nasional teknik elektro dan teknologi informasi*, vol. 9, no. 4, pp. 375–384, dec. 2020, doi: 10.22146/jnteti.v9i4.539.

[47] g. P. Suri, a. L. Fernandes, and l. A. Nopa, "peran iot dalam transformasi jaringan multimedia: tinjauan literatur," *jurnal responsive teknik informatika*, vol. 8, no. 2, pp. 78–86, 2024, doi: https://doi.org/10.36352/jr.v8i02.999.

[48] i. Sitanggang, j. A. I. Damanik, f. Hutabarat, and a. Sagala, "implementation of wireless sensor network (wsn) for earthquake detection," *elkha*, vol. 14, no. 2, p. 102, oct. 2022, doi: 10.26418/elkha.v14i2.56146.

[49] m. Khaddafi, a. F. Nasution, n. A. Angkat, and s. Pitriyani, " peran metodologi penelitian dalam menentukan kualitas hasil penelitian ilmiah," *jurnal intelek insan cendikia*, vol. 2, no. 7, pp. 13250–13255, 2025, accessed: oct. 22, 2025. [online]. Available: https://jicnusantara.com/index.php/jiic/article/view/4315/4361

[50] a. Djimli, s. Merniz, and s. Harous, "energy-efficient mac protocols for wireless sensor networks: a survey," *telkomnika (telecommunication computing electronics and control)*, vol. 17, no. 5, p. 2301, oct. 2019, doi: 10.12928/telkomnika.v17i5.12163.