Karapan Network
Journal

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

Security and Privacy Challenges in Wireless Sensor Networks: A Systematic Literature Review of Threat Mitigation Strategies

Moh. Rafael Kamil Ardiansyah [1)*], Radhitya Dwi Akmal Purnomo [2)]

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

[1)]Raphardiansyah@gmail.com, [2)]radhityadwi65@gmail.com

Abstrak

Perkembangan *Wireless Sensor Networks* (*WSN*) sebagai infrastruktur fundamental dalam ekosistem *Internet of Things* menghadapi tantangan keamanan dan privasi yang semakin kompleks akibat keterbatasan sumber daya komputasi, memori, dan energi pada perangkat sensor yang digunakan. Penelitian tinjauan literatur sistematis ini menganalisis 30 publikasi ilmiah periode 2020-2024 menggunakan kerangka kerja *PRISMA* untuk mengidentifikasi berbagai ancaman keamanan, mengkategorikan strategi mitigasi yang telah diterapkan, serta memetakan kesenjangan penelitian yang masih ada. Hasil analisis mengungkapkan bahwa ancaman *WSN* mencakup serangan *blackhole*, *sinkhole*, *wormhole*, *Sybil*, *denial-of-service* (*DoS*), dan *man-in-the-middle* yang dapat mengkompromikan integritas, kerahasiaan, dan ketersediaan data secara signifikan, bahkan pada skala jaringan besar dengan ribuan node. Strategi mitigasi yang efektif meliputi penggunaan kriptografi ringan berbasis *AES-ECC*, protokol autentikasi *ECDH*, teknologi *blockchain*, sistem deteksi intrusi berbasis *machine learning*, serta mekanisme *trust management* yang adaptif dan responsif terhadap perilaku node. Penelitian ini juga mengidentifikasi kesenjangan dalam implementasi algoritma *post-quantum*, pemanfaatan *federated learning* untuk *WSN*, serta standardisasi protokol keamanan yang *interoperable* dan *scalable*. Berdasarkan temuan tersebut, penelitian ini merekomendasikan arah riset masa depan untuk mengembangkan solusi keamanan yang lebih *robust*, adaptif, efisien, dan tahan terhadap serangan canggih, sehingga mampu menghadapi evolusi ancaman yang terus berkembang dalam ekosistem *WSN-IoT* kontemporer secara berkelanjutan, serta mendukung integrasi dengan teknologi *IoT* generasi berikutnya.

Kata Kunci: Keamanan Jaringan Sensor Nirkabel, Mitigasi Ancaman, Kriptografi Ringan.

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

I. PENDAHULUAN

Perkembangan teknologi Wireless Sensor Networks (WSN) telah mengalami transformasi signifikan dalam dua dekade terakhir, menjadikannya sebagai infrastruktur fundamental dalam ekosistem Internet of Things (IoT) dan sistem cyber-physical kontemporer. Jaringan sensor nirkabel merepresentasikan kumpulan simpul sensor berbiaya rendah, berdaya rendah, dan mampu mengorganisasi diri secara otomatis untuk melakukan pemantauan lingkungan secara real-time. Aplikasi WSN telah merambah berbagai domain kritis mulai dari pengawasan militer, pemantauan kesehatan pasien, pemantauan lingkungan, hingga implementasi *smart cities* dan infrastruktur Industri 4.0 [1].

Karakteristik unik WSN yang mencakup keterbatasan kapasitas komputasi, memori terbatas, sumber daya energi yang ketat, serta kerentanan terhadap deteksi fisik dan jalur komunikasi nirkabel yang tidak dapat diandalkan, menciptakan tantangan keamanan multidimensional yang memerlukan pendekatan mitigasi yang komprehensif dan adaptif [2],[3]. Dalam konteks keamanan siber kontemporer, WSN menghadapi ancaman yang semakin kompleks dan beragam yang dapat dikategorikan menjadi serangan pada lapisan fisik, data link, jaringan, hingga lapisan aplikasi. Serangan seperti *blackhole*, *sinkhole*, *wormhole*, *sybil*, *denial of service (DoS)*, dan *man-in-the-middle* telah terdokumentasi secara ekstensif dalam literatur sebagai vektor ancaman utama yang dapat mengkompromikan integritas, kerahasiaan, dan ketersediaan data dalam jaringan sensor. Lebih lanjut, karakteristik penempatan WSN yang sering kali berada di lingkungan terbuka dan tanpa pengawasan membuat simpul sensor sangat rentan terhadap serangan fisik seperti *node capture*, *tampering*, dan *eavesdropping* [4].

* Moh. Rafael Kamil Ardiansyah

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.I.I.354-373

Permasalahan keamanan ini diperparah dengan adanya kendala sumber daya yang membatasi implementasi mekanisme kriptografi konvensional yang intensif secara komputasional, sehingga memerlukan pendekatan keamanan yang ringan namun tetap *robust* [5],[6],[7]. Aspek privasi dalam WSN juga menjadi perhatian kritis, terutama dalam aplikasi yang melibatkan pengumpulan dan transmisi data sensitif seperti sistem pemantauan kesehatan dan *smart home*. Privasi lokasi sumber (*source location privacy*), privasi konten data, serta privasi kontekstual menjadi dimensi-dimensi yang harus dilindungi untuk mencegah inferensi informasi sensitif oleh pihak yang tidak berwenang. Tantangan privasi ini menjadi semakin kompleks dengan integrasi WSN ke dalam ekosistem IoT yang lebih luas, di mana jutaan perangkat heterogen dengan kapabilitas berbeda saling terhubung dan berbagi data secara masif. Ancaman privasi tidak hanya terbatas pada akses tidak sah terhadap data, tetapi juga mencakup analisis pola lalu lintas jaringan yang dapat mengungkapkan informasi sensitif melalui teknik *traffic analysis* dan *timing attacks* [8],[9].

Dalam dua dekade terakhir, berbagai penelitian telah berupaya mengatasi tantangan tersebut melalui strategi mitigasi yang semakin adaptif dan efisien. Pendekatan seperti kriptografi ringan (lightweight cryptography), autentikasi efisien, trust management, serta deteksi intrusi berbasis machine learning dan deep learning terus dikembangkan untuk menyesuaikan dengan keterbatasan sumber daya WSN [10],[11]. Implementasi algoritma seperti Random Forest, Support Vector Machine (SVM), k-Nearest Neighbors (k-NN), dan teknik *deep learning* seperti Convolutional Neural Networks (CNN) serta Long Short-Term Memory (LSTM) telah menunjukkan efektivitas tinggi dalam mendeteksi anomali dan serangan pada jaringan sensor [12]. Pendekatan federated learning juga mulai dieksplorasi untuk memungkinkan pelatihan model deteksi intrusi secara terdistribusi sambil menjaga privasi data pada simpul sensor [13].

Namun, penelitian-penelitian tersebut terus berevolusi. Sejumlah studi menunjukkan bahwa WSN menghadirkan paradoks keamanan, di mana penerapan mekanisme proteksi konvensional sering kali tidak memungkinkan tanpa mengorbankan performa jaringan dan masa pakai node sensor [14]. Oleh karena itu, pendekatan keamanan yang efisien, adaptif, dan berlapis menjadi keharusan untuk menjaga integritas, ketersediaan, dan kerahasiaan data.

II. TINJAUAN PUSTAKA

A. Pendekatan Kriptografi dan Keamanan Lapisan Jaringan

Peneliti kemudian mengusulkan berbagai strategi mitigasi, mulai dari penerapan algoritma kriptografi ringan seperti Advanced Encryption Standard (AES) dan Elliptic Curve Cryptography (ECC), hingga pendekatan kriptografi hibrid dalam protokol *Low-Energy Adaptive Clustering Hierarchy (LEACH)* yang meningkatkan ketahanan terhadap serangan kanal samping [15]. Optimasi berbasis Chicken Swarm Optimization untuk seleksi *cluster head* juga terbukti efektif dalam mencegah serangan *replay*, *DoS*, dan *Sybil* dengan konsumsi sumber daya minimal. Selain itu, mekanisme *cross-layered adaptive security* yang menyesuaikan algoritma terhadap kondisi jaringan dinamis seperti *Bit Error Rate (BER)* menjadi bukti evolusi paradigma dari sistem statis menuju sistem responsif [16].

B. Autentikasi dan Manajemen Kunci

Aspek autentikasi dan manajemen kunci juga dikaji secara intensif. Protokol berbasis Elliptic Curve Diffie-Hellman (ECDH) yang divalidasi dengan *Scyther tool* terbukti dapat mengatasi kelemahan skema terdahulu sambil mempertahankan efisiensi autentikasi mutual. Pengembangan lebih lanjut dari protokol Diffie-Hellman klasik dengan penambahan fungsi *hashing* juga mengurangi waktu komputasi tanpa mengorbankan ketahanan terhadap serangan *man-in-the-middle* [17].

C. Penerapan Blockchain dalam WSN

blockchain muncul sebagai paradigma baru dalam memastikan integritas dan keamanan data terdistribusi di WSN. Integrasi blockchain dengan teknik *clustering* meningkatkan efisiensi distribusi beban kerja serta meminimalkan risiko manipulasi data. Implementasi basis data mobile berbasis Merkle-tree menciptakan sistem *private cloud* yang lebih aman dan tahan terhadap *linking attack*, *man-in-the-middle*, serta *DDoS* [18].

D. Pendekatan Machine Learning dan Trust Management

Perkembangan teknologi cerdas juga mendorong adopsi machine learning (ML) dalam deteksi dan mitigasi ancaman WSN. Algoritma ML berfungsi sebagai mekanisme adaptif yang mampu melakukan monitoring dan pengambilan keputusan secara otonom, meskipun masih menghadapi keterbatasan data pelatihan dan sumber daya perangkat [19]. Sementara itu, pendekatan trust management difokuskan untuk mendeteksi serangan internal dari simpul yang terkompromi, yang tidak dapat ditangani hanya dengan kriptografi dan autentikasi konvensional.

E. Keamanan Protokol Routing dan IDS

Penelitian lain juga menyoroti pentingnya keamanan pada protokol routing. Analisis terhadap *Directed Diffusion* menunjukkan bahwa enkripsi pada lapisan tautan dapat menekan serangan eksternal, namun simpul terkompromi tetap menjadi ancaman dominan dengan risiko *DoS*, *selective forwarding*, dan manipulasi rute [20]. Studi lanjutan memberikan taksonomi lengkap mengenai serangan aktif dan pasif terhadap node sensor sebagai dasar klasifikasi ancaman [21]. Pada tataran praktis, penggunaan kombinasi *firewall filtering* dan *port knocking* terbukti meningkatkan keamanan jaringan dan mencegah akses tidak sah [22].

F. Strategi Terpadu dan Integrasi Industri 4.0

Strategi terpadu yang menggabungkan *firewall*, enkripsi AES/RSA, *Intrusion Detection System (IDS)*, serta *Disaster Recovery Plan (DRP)* dinilai mampu memperkuat sistem pertahanan jaringan berskala besar [23]. Dalam konteks penerapan Industri 4.0, setiap domain aplikasi WSN memiliki karakteristik dan kebutuhan keamanan yang spesifik [24]. Integrasi WSN dengan IoT juga memunculkan tantangan baru pada protokol ZigBee, yang sering digunakan untuk sistem berdaya rendah dan berbiaya rendah [25].

G. Kesenjangan Penelitian dan Arah Riset Masa Depan

Meskipun banyak penelitian telah dilakukan, masih terdapat kesenjangan pengetahuan yang signifikan dalam memahami strategi mitigasi ancaman keamanan dan privasi WSN secara holistik. Penelitian sebelumnya cenderung fokus pada aspek spesifik seperti jenis serangan tertentu atau teknik mitigasi individual, tanpa memberikan pandangan sistematis dan komprehensif terhadap lanskap ancaman dan ekosistem solusi yang ada. Dengan evolusi WSN menuju integrasi dengan jaringan 6G, edge computing, dan sistem otonom, diperlukan evaluasi kritis terhadap efektivitas strategi mitigasi dalam menghadapi ancaman masa depan [14],[13].

Oleh karena itu, penelitian ini dilakukan untuk mengidentifikasi, mengklasifikasikan, dan menganalisis strategi keamanan WSN secara sistematis menggunakan kerangka kerja PRISMA, dengan tujuan memberikan gambaran menyeluruh tentang lanskap keamanan WSN serta arah pengembangan riset di masa depan.

III. METODE

A. Pendekatan Penelitian

Penelitian ini mengadopsi pendekatan *Systematic Literature Review (SLR)* untuk mengidentifikasi, mengevaluasi, dan mensintesis bukti ilmiah terkait tantangan keamanan dan privasi dalam *Wireless Sensor Networks* (WSN) beserta strategi mitigasinya. Metode SLR dipilih karena kemampuannya dalam menyediakan sintesis bukti yang komprehensif, transparan, dan dapat direplikasi melalui prosedur yang sistematis dan terstruktur [26]. Penelitian ini mengikuti kerangka kerja *Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)* 2020 yang menjadi standar internasional untuk pelaporan tinjauan sistematis, mencakup *checklist* 27 item dan diagram alur yang memfasilitasi transparansi dalam proses seleksi studi [27],[42]. Implementasi PRISMA 2020 memastikan bahwa setiap tahapan penelitian dilakukan secara *rigorous* dan meminimalkan *bias* seleksi serta *bias* publikasi yang dapat memengaruhi validitas temuan.

B.Strategi Pencarian Literatur

Strategi pencarian literatur dirancang secara komprehensif dengan menggunakan basis data ilmiah elektronik utama yang mencakup IEEE Xplore, Scopus, Web of Science, ACM Digital Library, dan ScienceDirect untuk periode publikasi 2020–2024. Pemilihan rentang waktu ini bertujuan untuk mengidentifikasi penelitian terkini yang mencerminkan perkembangan teknologi dan ancaman keamanan kontemporer dalam ekosistem WSN. String pencarian dikonstruksi menggunakan kombinasi Boolean operators (AND, OR, NOT) dengan kata kunci utama meliputi “wireless sensor networks”, “security”, “privacy”, “intrusion detection”, “threat mitigation”, “cryptography”, “machine learning”, dan “attack”. Pencarian dilakukan pada metadata publikasi termasuk judul, abstrak, dan kata kunci untuk memaksimalkan sensitivitas dan spesifisitas hasil pencarian. Hasil pencarian dari setiap basis data kemudian diekspor ke perangkat lunak manajemen referensi untuk proses deduplikasi dan penyaringan selanjutnya.

C. Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi ditetapkan secara a priori untuk memastikan relevansi dan kualitas studi yang dianalisis:

Kriteria inklusi mencakup:

1. Artikel jurnal ilmiah berbahasa Inggris dan telah melalui proses peer-review..

2. Studi yang membahas aspek keamanan atau privasi dalam WSN serta menyajikan strategi mitigasi ancaman.
3. Publikasi dalam rentang waktu 2020–2024.

Kriteria ekslusi mencakup:

4. Artikel jurnal ilmiah berbahasa Inggris dan telah melalui proses peer-review..
5. Publikasi non-akademik seperti buku, laporan teknis, atau grey literature.
6. Studi yang tidak relevan dengan WSN.
7. Publikasi duplikat.

D. Kesenjangan Penelitian dan Arah Riset Masa Depan

Ekstraksi data dilakukan secara sistematis menggunakan formulir ekstraksi terstandarisasi yang dikembangkan berdasarkan pertanyaan penelitian dan kerangka kerja PRISMA [28]. Informasi yang diekstraksi meliputi karakteristik studi seperti penulis, tahun publikasi, negara, tujuan penelitian, metodologi yang digunakan, jenis ancaman yang dibahas, strategi mitigasi yang diusulkan, hasil utama, dan keterbatasan studi. Data diekstraksi secara independen oleh dua peneliti menggunakan perangkat lunak *spreadsheet* untuk memfasilitasi analisis kuantitatif dan kualitatif. Penilaian kualitas metodologis studi dilakukan menggunakan instrumen *critical appraisal* yang sesuai dengan desain penelitian masing-masing studi untuk mengevaluasi validitas internal, reliabilitas, dan potensi *bias* [29]. Hasil ekstraksi data kemudian disintesis menggunakan pendekatan naratif tematik yang mengelompokkan temuan berdasarkan kategori ancaman, mekanisme serangan, dan efektivitas strategi mitigasi, dengan dukungan tabel ringkasan dan visualisasi data untuk memperjelas pola dan tren yang teridentifikasi dalam literatur

Sebanyak 30 artikel ilmiah terpilih setelah melalui proses seleksi ketat sesuai kriteria PRISMA. Kajian ini mencakup berbagai pendekatan dan topik, seperti analisis keamanan routing pada WSN dengan protokol *Directed Diffusion* [19], identifikasi serangan aktif dan pasif beserta mekanisme pertahanan [30], hingga algoritma kriptografi hybrid AES–ECC yang efisien untuk mitigasi serangan [31]. Penelitian lain meninjau aspek keamanan dan aplikasi WSN dalam konteks IoT [21], mekanisme kriptografi adaptif seperti RECTANGLE dan Camellia [32], serta pendekatan *Improved Elliptic Key Cryptography* dengan optimasi *Chicken Swarm Optimization* [33].

Selain itu, sejumlah studi mengeksplorasi integrasi WSN dengan IoT dan teknologi blockchain untuk keamanan desentralisasi [34], [35], [20], serta meninjau tantangan keamanan dalam implementasi di lingkungan industri, kendaraan, dan sistem cyber-physical [36], [37],[38] Pendekatan berbasis machine learning juga banyak dikaji, mencakup penerapan ML untuk deteksi intrusi dan estimasi serangan DDoS pada jaringan 5G [39],[14], [9]. Studi lain menekankan pentingnya manajemen kepercayaan [17], penggunaan Fuzzy AHP untuk prioritisasi kontrol keamanan [40], dan strategi penghematan energi dengan kriptografi efisien [15], [41].

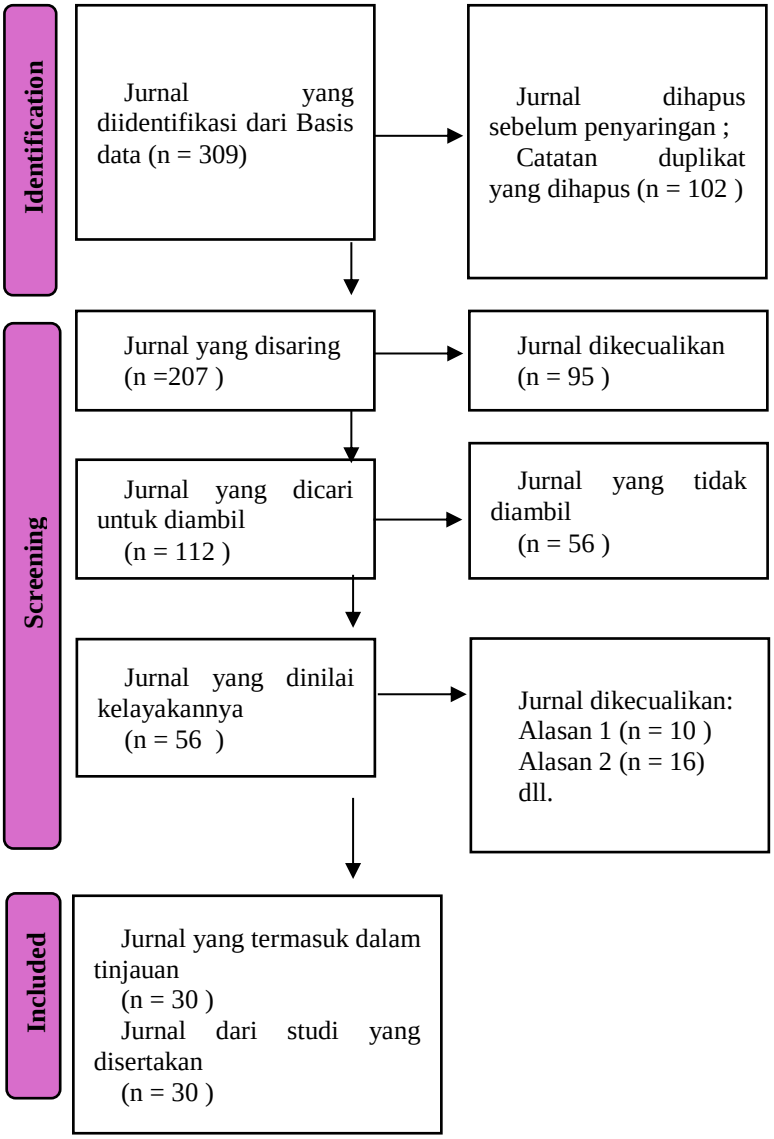
Penelitian dalam negeri juga menjadi bagian dari analisis ini, seperti evaluasi keamanan jaringan dengan firewall dan VPN [43] [44], keamanan DNS melalui DNSSEC [45], serta implementasi keamanan berbasis *RouterOS* dan *port knocking* pada jaringan MikroTik [46]. Tinjauan sistematis tentang keamanan website menggunakan OWASP ZAP [47], serta analisis tren phishing dan pencegahannya [48] juga disertakan sebagai konteks keamanan siber yang relevan dengan infrastruktur WSN modern. Beberapa studi menyoroti pula integrasi IoT dalam pemantauan lingkungan [49],[51] dan perkembangan teknologi 5G sebagai masa depan jaringan sensor nirkabel [50].

Keseluruhan studi tersebut memperkaya sintesis tematik penelitian ini dengan memberikan gambaran menyeluruh mengenai tantangan, pendekatan mitigasi, serta arah pengembangan keamanan dan privasi dalam WSN.

.

IV. HASIL

A. Screening Artikel Jurnal



Gambar 1. Flowchart Prisma

1. Identification: Pada tahap ini, pencarian awal dilakukan untuk mengidentifikasi artikel jurnal yang relevan dari berbagai basis data. Dalam penelitian Anda, sebanyak 309 jurnal berhasil diidentifikasi. Namun, tidak semua jurnal tersebut langsung diproses lebih lanjut. Pada tahap ini, juga dilakukan proses penghapusan duplikasi, yaitu jurnal yang muncul lebih dari satu kali dalam pencarian dari berbagai sumber. Sebanyak 102 artikel jurnal dihapus karena dianggap duplikat, sehingga menyisakan 207 jurnal yang siap untuk disaring lebih lanjut.

2. Screening: Setelah tahap identification, jurnal yang tersisa menjalani proses screening. Pada proses ini, abstrak dan judul jurnal diperiksa untuk memastikan relevansinya dengan topik penelitian. Dari 207 jurnal yang disaring, 95 di antaranya dikecualikan karena tidak memenuhi kriteria awal yang telah ditetapkan. Pada tahap ini, artikel yang tidak sesuai dengan fokus penelitian atau kriteria inklusi lainnya dihilangkan.
3. Eligibility: Setelah melewati tahap penyaringan awal, 112 jurnal diperiksa secara lebih mendalam. Namun, dari jumlah ini, 56 jurnal tidak dapat diambil atau dieksklusi karena berbagai alasan, misalnya, karena teks.lengkapnya tidak tersedia, atau karena jurnal tersebut tidak memenuhi syarat metodologi atau kualitas yang diharapkan.
4. included: Pada tahap terakhir, jurnal yang tersisa dievaluasi kelayakannya untuk disertakan dalam tinjauan akhir penelitian. Sebanyak 56 jurnal telah dievaluasi kelayakannya, tetapi hanya sejumlah 30 jurnal yang akhirnya disertakan dalam penelitian karena memenuhi semua kriteria yang telah ditetapkan.

Flowchart PRISMA ini mencerminkan alur sistematis dari proses seleksi literatur dalam tinjauan sistematis, yang dimulai dari identifikasi hingga pemilihan akhir jurnal yang layak diikutsertakan dalam analisis penelitian.

B. Hasil Ringkasan Singkat Dari Temuan Utama

No.	Judul	Fokus Penelitian	Subjek	Metode	Temuan Utama	Implikasi	Relevansi dengan Penelitian
1	Analysis of Wireless Sensor Networks Through Secure Routing Protocols Using Directed Diffusion Methods	Keamanan protokol routing pada WSN menggunakan metode Directed Diffusion	Protokol Directed Diffusion dalam WSN	Analisis protokol data-centric dengan evaluasi terhadap tiga kategori serangan	Enkripsi lapisan tautan dapat mengurangi serangan eksternal, namun simpul yang terkompromi di dalam jaringan sulit dicegah. Serangan DoS, modifikasi informasi routing, dan selective forwarding menjadi ancaman utama	Pentingnya mengembangkan mekanisme keamanan berlapis untuk melindungi protokol routing dari berbagai vektor serangan	Memberikan pemahaman mendalam tentang kerentanan protokol routing dan strategi mitigasi yang diperlukan dalam WSN

2	Wireless Sensor Networks: Active and Passive Attacks - Vulnerabilities and Countermeasures	Identifikasi serangan aktif dan pasif pada WSN beserta mekanisme pertahanan	Serangan keamanan dalam WSN	Tinjauan literatur terhadap kategori serangan dan strategi defensif	Simpul sensor yang ditempatkan tanpa pengawasan rentan terhadap berbagai bentuk serangan. Diperlukan desain countermeasures yang efektif untuk komunikasi aman	Membantu peneliti mengidentifikasi serangan paling berbahaya dan mengembangkan mekanisme defensif yang tepat	Menyediakan taksonomi lengkap serangan aktif dan pasif yang menjadi dasar klasifikasi ancaman dalam penelitian ini
3	Cryptographic Data Security for Reliable Wireless Sensor Network	Keamanan data kriptografi menggunakan hybrid AES dan ECC dengan protokol LEACH	Manajemen kunci dan enkripsi data dalam WSN	Pengembangan algoritma hybrid dengan implementasi clustering	Algoritma hybrid AES-ECC lebih sederhana, lebih andal, dan mampu mengatasi berbagai ancaman keamanan termasuk side-channel attacks. Kompleksitas waktu, waktu enkripsi, dan dekripsi lebih baik	Solusi kriptografi ringan yang efisien energi sangat penting untuk WSN dengan sumber daya terbatas	Menunjukkan efektivitas pendekatan kriptografi hybrid dalam meningkatkan keamanan dan efisiensi energi WSN
4	Security and Application of Wireless Sensor Network	Keamanan WSN dalam konteks IoT dan aplikasinya	Keamanan WSN dan implementasi IoT	Tinjauan literatur terhadap isu keamanan dan aplikasi WSN	Lingkungan deployment simpul yang kompleks memerlukan penelitian keamanan mendalam untuk mengurangi ancaman dan serangan jaringan	WSN menjadi fondasi penting bagi perkembangan IoT yang memerlukan perhatian serius terhadap aspek keamanan	Memperkuat argumentasi pentingnya penelitian keamanan WSN dalam era IoT

5	Enabling Secure Data Transmission for Wireless Sensor Networks Based IoT Applications	Mekanisme keamanan adaptif menggunakan algoritma kriptografi alternatif	Transmisi data aman dalam WSN-IoT	Evaluasi performa algoritma RECTANGLE, Fantomas, Camellia dibandingkan AES	Block cipher berbasis SPN lebih baik daripada struktur Feistel. Mekanisme cross-layered dapat beradaptasi dengan BER untuk memilih algoritma keamanan optimal	Pemilihan algoritma kriptografi harus mempertimbangkan tingkat keamanan, penggunaan memori, throughput, dan konsumsi baterai	Mendemonstrasikan pentingnya pendekatan adaptif dalam pemilihan mekanisme keamanan WSN
6	Security for Wireless Sensor Networks Using Cryptography	Strategi keamanan menggunakan IEKC (Improved Elliptic Key Cryptography)	Kriptografi kunci eliptik dalam WSN	Implementasi IEKC dengan optimasi CSO (Chicken Swarm Optimization) untuk pemilihan cluster head	Teknik yang diusulkan efektif mencegah serangan replay, DoS, dan Sybil dengan sumber daya minimal. Meningkatkan PDR, mengurangi latency, dan meningkatkan throughput	Penggunaan kriptografi kunci eliptik yang ditingkatkan dapat memperkuat ketahanan jaringan terhadap node capture	Menunjukkan efektivitas algoritma optimasi dalam meningkatkan keamanan dan performa WSN
7	Internet of Things Based Wireless Sensor Network: A Review	Efisiensi energi, topologi routing, dan tantangan keamanan WSN berbasis IoT	WSN dalam ekosistem IoT dengan protokol ZigBee	Tinjauan literatur sistematis	Protokol ZigBee penting untuk aplikasi IoT berbiaya rendah dan berdaya rendah. Tantangan keamanan IoT-WSN memerlukan perhatian khusus	Integrasi WSN dengan IoT membawa tantangan keamanan baru yang memerlukan solusi komprehensif	Memberikan konteks integrasi WSN-IoT dan tantangan keamanan yang muncul
8	An Efficient Cryptographic Technique Using Modified Diffie-Hellman in Wireless Sensor Networks	Teknik kriptografi efisien menggunakan modifikasi Diffie-Hellman	Pertukaran kunci dalam WSN	Modifikasi protokol Diffie-Hellman dengan hashing setiap nilai yang ditransmisikan	Pendekatan yang diusulkan memiliki waktu komputasi dan respons lebih rendah. Diffie-Hellman yang dimodifikasi aman terhadap man-in-the-middle attack	Modifikasi protokol kriptografi konvensional dapat meningkatkan keamanan dan efisiensi untuk WSN	Menunjukkan pentingnya adaptasi protokol kriptografi klasik untuk lingkungan WSN

9	An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network	Protokol autentikasi dan key agreement berbasis ECDH	Autentikasi mutual dalam WSN	Analisis keamanan dengan tool Scyther dan review manual	Protokol berbasis ECDH dapat mengatasi kelemahan keamanan pada skema sebelumnya dan menyediakan autentikasi mutual yang efektif	Autentikasi berbasis kurva eliptik menawarkan keamanan tinggi dengan overhead komputasi rendah	Mendemonstrasikan pentingnya protokol autentikasi yang robust dalam WSN
10	Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain	Keamanan dan efisiensi energi WSN menggunakan teknologi blockchain	Integrasi blockchain dengan WSN	Implementasi blockchain pada arsitektur WSN dengan teknik clustering	Teknologi blockchain dapat mengatasi masalah keamanan dan privasi IoT. Clustering meningkatkan efisiensi jaringan dengan distribusi beban kerja	Blockchain menawarkan solusi untuk keamanan data terdistribusi dalam WSN meskipun dengan trade-off konsumsi energi	Menunjukkan potensi teknologi blockchain sebagai strategi mitigasi ancaman dalam WSN
11	Applications of Wireless Sensor Networks: An Up-to-Date Survey	Tinjauan aplikasi WSN terkini dari berbagai domain	Aplikasi WSN kontemporer	Survei literatur terhadap kategori aplikasi WSN	WSN memiliki rentang aplikasi yang terus berkembang dengan manfaat signifikan di berbagai domain. Setiap kategori aplikasi memiliki karakteristik, kelebihan, dan kekurangan spesifik	Pemahaman tentang aplikasi WSN penting untuk merancang solusi keamanan yang sesuai konteks	Memberikan konteks aplikasi WSN yang beragam yang memerlukan strategi keamanan berbeda
12	Enhancing Communication Security an In-Vehicle Wireless Sensor Network	Framework keamanan komunikasi untuk WSN kendaraan	Keamanan WSN dalam kendaraan	Implementasi enkripsi dan autentikasi dengan pertukaran kunci periodik	Segmentasi jaringan dengan tunnel terenkripsi meningkatkan keamanan sistem otomotif. AES-CBC 128, HMAC, dan HKDF efektif dengan konsumsi sumber daya yang wajar	Keamanan WSN dalam sistem cyber-physical seperti kendaraan memerlukan pendekatan khusus	Menunjukkan aplikasi keamanan WSN dalam domain kritis seperti otomotif

13	Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks	Penguatan keamanan WSN menggunakan teknologi blockchain	Integrasi blockchain untuk keamanan data WSN	Implementasi mobile database dengan algoritma Merkle-tree	Setiap blok berisi hash blok sebelumnya membuat data sulit dimanipulasi. Sistem dengan blockchain hampir tidak mungkin dirusak oleh operator	Blockchain dapat berfungsi sebagai private cloud untuk WSN dengan keandalan transmisi data tinggi	Mendemonstrasikan implementasi praktis blockchain untuk integritas data WSN
14	Wireless Sensor Network Security: A Recent Review Based on State-of-the-Art Works	Tinjauan keamanan WSN berdasarkan penelitian terkini	Isu keamanan pada setiap lapisan WSN	Tinjauan literatur sistematis 3 tahun terakhir	Keterbatasan memori dan daya komputasi rendah menyebabkan masalah keamanan. Diperlukan solusi efisien terutama dengan pertumbuhan IoT. Framework IDS untuk WSN perlu dikembangkan	Memberikan taksonomi ancaman per lapisan dan solusi algoritmik dari berbagai peneliti	Sangat relevan sebagai rujukan terkini untuk mengidentifikasi research gaps dalam keamanan WSN
15	Prioritization of Information Security Controls Through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks	Prioritasi kontrol keamanan informasi menggunakan Fuzzy AHP	Seleksi kontrol keamanan untuk WSN dan cloud	Pendekatan Fuzzy AHP berdasarkan ISO/IEC 27001:2013	Prioritasi kontrol keamanan menggunakan Fuzzy AHP menghasilkan evaluasi yang efisien dan cost-effective. Pendekatan formal membantu organisasi memilih kontrol paling tepat	Pemilihan kontrol keamanan harus mempertimbangkan vulnerabilitas, risiko, ancaman, dan kendala organisasi	Memberikan metodologi untuk evaluasi dan seleksi strategi mitigasi keamanan WSN

16	Blockchain Mechanism and Symmetric Encryption in a Wireless Sensor Network	Sistem terdesentralisasi menggunakan blockchain dan enkripsi simetris	Keamanan IoT-WSN dengan blockchain	Implementasi dan pengujian pada WSN sensor suhu dan kelembaban	Sistem yang diusulkan otonom, aman, menjaga privasi, andal, dan ketersediaan informasi terjamin. Kurang rentan terhadap linking attack, man in the middle, dan DDoS	Sistem terdesentralisasi dengan blockchain mengatasi kelemahan sistem IoT terpusat	Menunjukkan efektivitas kombinasi blockchain dan kriptografi untuk keamanan WSN
17	Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review	Peran WSN dan IoT dalam Industri 4.0	WSN dan IoT dalam konteks Industri 4.0	SLR terhadap 130+ artikel (2014-2021)	WSN dan IoT menjadi tulang punggung Industri 4.0. Serangan keamanan jaringan dan intruder menjadi tantangan signifikan yang memerlukan solusi otomasi	Keamanan WSN dan IoT kritis untuk kesuksesan implementasi Industri 4.0	Memberikan konteks industri dan tantangan keamanan WSN dalam aplikasi real-world
18	Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues	Penggunaan machine learning untuk keamanan WSN	Algoritma ML untuk monitoring dan deteksi ancaman WSN	Tinjauan literatur terhadap algoritma ML dan tantangannya	Algoritma ML menjadi solusi untuk keamanan WSN dengan monitoring dan inteligensi keputusan. Tantangan utama adalah kebutuhan data training dan adaptasi dengan kapabilitas sensor terbatas	ML dapat mengurangi biaya keamanan WSN dan meningkatkan kemampuan deteksi ancaman melalui pembelajaran mandiri	Sangat relevan untuk memahami penerapan ML dalam deteksi intrusi dan mitigasi ancaman WSN

19	Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey	Serangan dan pertahanan berbasis trust management	Teknologi trust management dalam WSN	Survei mendalam terhadap skema trust management	Trust management efektif untuk mendeteksi dan mempertahankan dari serangan internal yang tidak bisa diatasi enkripsi dan autentikasi. Perbandingan simetris keunggulan dan kelemahan berbagai skema	Trust management menjadi pendekatan penting untuk mengatasi serangan dari simpul terkompromi	Memberikan perspektif alternatif strategi mitigasi melalui manajemen kepercayaan
20	Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks	Teknik ML untuk proteksi WSN dan strategi deployment pada jaringan 5G	Deteksi dan pencegahan serangan DDoS dengan SDN	Framework berbasis clustering dengan ODL Controller dan Mininet	Framework yang diusulkan efektif mendeteksi dan mencegah serangan DDoS di fase awal pada control dan application layer. Integrasi dengan SNORT dan Flow meningkatkan efektivitas	SDN dengan ML menawarkan fleksibilitas dan ekstensibilitas untuk deteksi dan pencegahan DDoS	Menunjukkan konvergensi WSN dengan teknologi jaringan modern dan peran ML dalam keamanan
21	Firewall Implementation as a Computer Network Security Strategy for Data Protection	Implementasi firewall sebagai strategi keamanan jaringan	Fungsi dan efektivitas firewall dalam proteksi jaringan	Observasi praktis implementasi firewall pada setup jaringan nyata	Firewall yang dikonfigurasi dengan tepat dapat memperkuat pertahanan jaringan secara signifikan. Namun tidak cukup sendirian dan harus didukung teknologi keamanan tambahan	Firewall adalah elemen esensial dalam menjaga keandalan dan keamanan jaringan komputer	Memberikan perspektif praktis implementasi firewall sebagai lapis pertahanan jaringan

22	Security Analysis and Data Recovery on Large-Scale Computer Networks	Analisis keamanan dan pemulihan data pada jaringan skala besar	Strategi keamanan dan recovery untuk jaringan besar	Tinjauan literatur 10 tahun terakhir	Sistem keamanan dan recovery komprehensif yang menggabungkan berbagai komponen dapat meningkatkan ketahanan sistem terhadap berbagai ancaman. Kolaborasi pencegahan dan kesiapan recovery sangat penting	Diperlukan pendekatan berlapis dengan firewall, enkripsi AES/RSA, IDS, backup otomatis, dan DRP	Menunjukkan pentingnya strategi keamanan holistik dan rencana pemulihan bencana
23	Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik	Analisis komparatif protokol VPN PPTP dan L2TP/IPSec	Performa dan keamanan protokol VPN	Eksperimental dengan pengujian throughput, latency, packet loss, dan CPU utilization	PPTP memberikan throughput tinggi dengan overhead minimal namun lemah dalam keamanan. L2TP/IPSec menawarkan keamanan superior dengan enkripsi kuat namun latency lebih tinggi	Administrator harus mempertimbangkan trade-off antara performa dan keamanan dalam pemilihan protokol VPN	Memberikan wawasan tentang trade-off keamanan dan performa dalam protokol komunikasi aman
24	Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus	Pengembangan sistem monitoring lingkungan kampus berbasis IoT	Pemantauan parameter lingkungan dengan IoT	Desain dan implementasi perangkat keras-lunak terintegrasi	Implementasi IoT dapat meningkatkan efisiensi pemantauan lingkungan kampus secara real-time. Data yang dikumpulkan mendukung pengambilan keputusan proaktif	Teknologi IoT berkontribusi pada manajemen lingkungan dan upaya keberlanjutan kampus	Mendemonstrasikan aplikasi praktis IoT-WSN untuk monitoring lingkungan

25	Optimasi Keamanan DNS: Eksplorasi Optimal dengan Implementasi DNS Security Extensions (DNSSEC)	Pencegahan DNS spoofing menggunakan DNSSEC	Keamanan DNS terhadap serangan spoofing	Pendekatan kualitatif dengan analisis lalu lintas jaringan	DNSSEC meningkatkan keamanan DNS dengan menambahkan tanda tangan digital. Namun memiliki keterbatasan terhadap serangan komputer kuantum. Langkah-langkah keamanan kritis untuk proteksi	Implementasi DNSSEC penting untuk melindungi sistem terhadap serangan spoofing yang semakin canggih	Menunjukkan pentingnya keamanan infrastruktur jaringan fundamental seperti DNS
26	Systematic Literature Review: Security Gap Detection on Websites Using OWASP ZAP	Deteksi kerentanan keamanan website menggunakan OWASP ZAP	Pengujian keamanan web dengan tool open-source	Tinjauan literatur komprehensif dan metodologi penelitian sistematis	OWASP ZAP efektif mengidentifikasi kerentanan seperti SQL Injection, XSS, dan misconfiguration. Tool ini membantu developer menemukan dan memperbaiki kelemahan	Penggunaan tool pengujian keamanan proaktif penting dalam lingkungan pengembangan web	Memberikan perspektif tentang pentingnya pengujian keamanan sistematis
27	Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study	Analisis tren serangan phishing dan metode pencegahan	Teknik phishing modern dan strategi mitigasi	Analisis data dari laporan keamanan siber dan studi kasus	Teknologi anti-phishing berkembang signifikan namun kesadaran pengguna tetap faktor kunci. Kebijakan organisasi yang ketat berperan penting dalam mengurangi risiko	Diperlukan sistem pertahanan berlapis yang menggabungkan solusi teknologi dengan kewaspadaan manusia	Menunjukkan pentingnya faktor manusia dalam keamanan siber

28	Tinjauan Performa RouterOS MikroTik dalam Jaringan Internet: Analisis Kinerja dan Kelayakan	Evaluasi performa RouterOS MikroTik	Kinerja router dalam mengelola lalu lintas jaringan	Pengukuran kecepatan, efisiensi, keandalan, dan skalabilitas	RouterOS MikroTik dapat memenuhi tuntutan kinerja jaringan modern dengan manajemen yang tepat. Hasil memberikan panduan untuk optimasi konfigurasi	Pemahaman mendalam tentang performa router penting untuk pengelolaan jaringan efisien	Memberikan konteks infrastruktur jaringan yang mendukung implementasi WSN
29	Implementasi Sistem Keamanan Jaringan MikroTik Menggunakan Firewall Filtering dan Port Knocking	Peningkatan keamanan jaringan MikroTik	Firewall filtering dan port knocking	Metode deskriptif dengan implementasi praktis	Kombinasi firewall filtering dan port knocking meningkatkan keamanan jaringan. Firewall memblokir serangan eksternal, port knocking menambah lapisan keamanan tambahan	Implementasi mekanisme keamanan berlapis efektif mencegah akses tidak sah	Mendemonstrasikan pentingnya mekanisme autentikasi dan filtering untuk keamanan jaringan
30	Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G	Pengenalan teknologi jaringan nirkabel 5G	Karakteristik dan kecepatan teknologi 5G	Tinjauan deskriptif teknologi	Teknologi 5G menawarkan kecepatan tinggi yang mengubah cara akses aplikasi, media sosial, dan informasi dengan kemudahan dan kecepatan lebih baik	5G sebagai generasi kelima teknologi nirkabel membawa implikasi bagi evolusi WSN	Memberikan konteks teknologi jaringan nirkabel masa depan yang akan mengintegrasikan WSN

Tabel 1. Sintesis

V. PEMBAHASAN

Berdasarkan analisis sistematis terhadap 30 artikel jurnal yang telah melalui proses seleksi ketat menggunakan kerangka kerja PRISMA, penelitian ini mengidentifikasi lanskap keamanan dan privasi *Wireless Sensor Networks* (WSN) yang kompleks dan multidimensional. Temuan-temuan dari literatur yang dikaji mengungkapkan bahwa tantangan keamanan WSN tidak dapat diselesaikan melalui pendekatan tunggal, melainkan memerlukan strategi mitigasi berlapis yang mengintegrasikan berbagai mekanisme defensif. Karakteristik inheren WSN yang mencakup keterbatasan kapasitas komputasi, memori terbatas, dan konsumsi energi yang ketat menciptakan paradoks keamanan di mana implementasi mekanisme proteksi konvensional menjadi tidak feasibel tanpa mengorbankan performa dan masa pakai jaringann.

Dimensi kriptografi muncul sebagai fondasi fundamental dalam arsitektur keamanan WSN, dengan berbagai penelitian mengeksplorasi algoritma yang dioptimalkan untuk lingkungan dengan sumber daya terbatas. Pendekatan kriptografi hibrid yang mengombinasikan Advanced Encryption Standard (AES) dengan Elliptic Curve Cryptography (ECC) dalam protokol *Low-Energy Adaptive Clustering Hierarchy (LEACH)* terbukti mampu menghasilkan kompleksitas waktu yang efisien dan ketahanan terhadap serangan kanal samping. Optimalisasi *Chicken Swarm Optimization* untuk seleksi *cluster head* juga menunjukkan efektivitas dalam mencegah serangan *replay*, *DoS*, dan *Sybil* dengan konsumsi sumber daya minimal sambil meningkatkan *Packet Delivery Ratio* (PDR), mengurangi latensi, serta meningkatkan *throughput*. Pendekatan adaptif lain memanfaatkan mekanisme *cross-layered* yang mampu menyesuaikan algoritma keamanan dengan kondisi jaringan dinamis, seperti pemilihan algoritma berdasarkan *Bit Error Rate (BER)*, menunjukkan evolusi paradigma dari solusi statis menuju sistem keamanan yang responsif terhadap konteks jaringan.

Protokol autentikasi dan manajemen kunci menjadi komponen kritis yang mendapat perhatian substansial. Pengembangan protokol autentikasi berbasis *Elliptic Curve Diffie-Hellman (ECDH)* yang dikombinasikan dengan fungsi *hashing* pada setiap nilai transmisi mampu mengatasi kelemahan pada skema klasik, menurunkan waktu komputasi, dan meningkatkan ketahanan terhadap serangan *man-in-the-middle*. Temuan-temuan ini menegaskan pentingnya adaptasi protokol kriptografi agar sesuai dengan karakteristik unik WSN yang memiliki sumber daya terbatas.

Integrasi teknologi *blockchain* muncul sebagai paradigma inovatif dalam memastikan integritas dan keamanan data terdistribusi pada WSN. Implementasi *blockchain* dengan teknik *clustering* dapat mengatasi permasalahan keamanan dan privasi melalui distribusi beban kerja yang efisien. Penggunaan struktur *Merkle-tree* untuk penyimpanan data memungkinkan deteksi manipulasi blok, sementara penerapan *private cloud* meningkatkan keandalan transmisi. Pendekatan yang mengombinasikan *blockchain* dengan enkripsi simetris juga terbukti menjaga privasi dan ketersediaan informasi, sekaligus mengurangi risiko serangan seperti *linking attack*, *man-in-the-middle*, dan *DDoS*.

Pendekatan berbasis *machine learning* menunjukkan potensi signifikan dalam deteksi dan mitigasi ancaman WSN. Algoritma pembelajaran mesin memungkinkan sistem melakukan pemantauan cerdas serta pengambilan keputusan adaptif terhadap pola serangan, meskipun tantangan berupa kebutuhan data pelatihan dan keterbatasan kemampuan sensor masih menjadi kendala. Implementasi sistem berbasis *controller* dan *mininet* dengan integrasi *IDS* seperti SNORT dan *Flow Analyzer* menunjukkan efektivitas dalam mendeteksi serangan *DDoS* pada lapisan kontrol maupun aplikasi. Selain itu, manajemen kepercayaan (*trust management*) juga terbukti efektif dalam menghadapi serangan internal yang tidak dapat diatasi oleh enkripsi atau autentikasi konvensional, dengan keunggulan berupa kemampuan mempertahankan stabilitas jaringan dan mendeteksi simpul berperilaku abnormal.

Aspek keamanan protokol *routing* juga menjadi fokus penting. Analisis terhadap protokol *Directed Diffusion* menyoroti bahwa enkripsi lapisan tautan dapat mengurangi serangan eksternal, namun simpul yang terkompromi di dalam jaringan tetap menjadi ancaman serius, seperti serangan *DoS*, modifikasi informasi *routing*, dan *selective forwarding*. Klasifikasi ancaman aktif dan pasif dalam literatur memperjelas bahwa simpul sensor yang ditempatkan tanpa pengawasan rentan terhadap berbagai bentuk serangan. Dalam konteks implementasi praktis, penerapan kombinasi *firewall filtering* dan *port knocking* pada jaringan MikroTik telah terbukti efektif dalam mencegah akses tidak sah serta meningkatkan keamanan berlapis pada jaringan sensor.

Strategi keamanan dan pemulihan data pada jaringan skala besar menekankan pentingnya pendekatan holistik yang menggabungkan *firewall*, enkripsi AES/RSA, *Intrusion Detection System (IDS)*, *backup* otomatis, serta *Disaster Recovery Plan (DRP)* untuk memastikan kontinuitas operasional. Konteks aplikasi WSN dalam era Industri 4.0 menunjukkan bahwa setiap domain memiliki karakteristik dan kebutuhan keamanan yang spesifik, sehingga memerlukan strategi mitigasi yang disesuaikan. Integrasi WSN dengan teknologi IoT juga menimbulkan tantangan keamanan baru, terutama pada penggunaan protokol ZigBee yang menekankan efisiensi biaya dan daya rendah, sehingga perlu pendekatan perlindungan yang komprehensif.

VI. KESIMPULAN

Tinjauan literatur sistematis terhadap 30 publikasi ilmiah mengungkapkan bahwa tantangan keamanan dan privasi dalam *Wireless Sensor Networks* bersifat multidimensional dan memerlukan strategi mitigasi berlapis yang mengintegrasikan mekanisme kriptografi ringan, protokol autentikasi robust, teknologi *blockchain*, pembelajaran mesin, dan manajemen kepercayaan. Keterbatasan sumber daya komputasi dan energi menciptakan paradoks keamanan yang menuntut pendekatan inovatif dalam menyeimbangkan proteksi optimal dengan efisiensi operasional. Algoritma kriptografi hibrid seperti kombinasi AES-ECC dan modifikasi protokol Diffie-Hellman menunjukkan efektivitas superior dalam lingkungan dengan konstrain sumber daya. Implementasi *blockchain* dan pembelajaran mesin membuka paradigma baru dalam deteksi intrusi dan preservasi integritas data terdistribusi. Integrasi WSN

dengan ekosistem IoT dan infrastruktur Industri 4.0 menghadirkan kompleksitas ancaman tambahan yang memerlukan solusi adaptif dan kontekstual sesuai karakteristik domain aplikasi spesifik.

Kontribusi Penulis: [Moh. Rafael Kamil Ardiansyah]: Konseptualisasi, perancangan metodologi, analisis literatur, penulisan draf awal dan penyusunan referensi akhir.
[Radhitya Dwi Akmal Purnomo]: Pengumpulan data literatur, validasi hasil, penyusunan tabel hasil PRISMA, serta penyuntingan.

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] Yisa, A. G., Dargahi, T., Belguith, S., & Hammoudeh, M. (2021). Security challenges of Internet of Underwater Things: A systematic literature review. Transactions on Emerging Telecommunications Technologies, 32(3). https://doi.org/10.1002/ett.4203.

[2] Ghadi, Y. Y., Mazhar, T., Shloul, T. Al, Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024). Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review. IEEE Access, 12(January), 12699–12719. https://doi.org/10.1109/ACCESS.2024.3355312.

[3] Soltani, K., Farzinvash, L., & Balafar, M. A. (2023). Trust-aware and energy-efficient data gathering in wireless sensor networks using PSO. Soft Computing, 27(16), 11731–11754. https://doi.org/10.1007/s00500-023-07856-z.

[4] Rani, S., Ahmed, S. H., & Rastogi, R. (2020). Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications. Wireless Networks, 26(4), 2307–2316. https://doi.org/10.1007/s11276-019-02083-7.

[5] Adu-Manu, K. S., Engmann, F., Sarfo-Kantanka, G., Baiden, G. E., & Dulemordzi, B. A. (2022). WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey. Journal of Sensors, 2022. https://doi.org/10.1155/2022/1628537.

[6] Ahmed, A., Oluomachi, E., Abdullah, A., & Tochukwu, N. (2024). Enhancing Data Privacy in Wireless Sensor Networks: Investigating Techniques and Protocols to Protect Privacy of Data Transmitted Over Wireless Sensor Networks in Critical Applications of Healthcare and National Security. International Journal of Network Security & Its Applications, 16(2), 47–63. https://doi.org/10.5121/ijnsa.2024.16204.

[7] Luo, J., Chen, Y., Wu, M., & Yang, Y. (2021). A Survey of Routing Protocols for Underwater Wireless Sensor Networks. IEEE Communications Surveys and Tutorials, 23(1), 137–160. https://doi.org/10.1109/COMST.2020.3048190.

[8] Akinsola, Oluomachi, E., Abdullah, A., & Tochukwu, N. (2024). Enhancing Data Privacy in Wireless Sensor Networks: Investigating Techniques and Protocols to Protect Privacy of Data Transmitted Over Wireless Sensor Networks in Critical Applications of Healthcare and National Security. International Journal of Network Security & Its Applications, 16(2), 47–63. https://doi.org/10.5121/ijnsa.2024.16204.

[9] Kumar, P., Baliyan, A., Prasad, K. R., Sreekanth, N., Jawarkar, P., Roy, V., & Amoatey, E. T. (2022). Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/5713092.

[10] Abidin, S., Vadi, V. R., & Rana, A. (2021). On Confidentiality, Integrity, Authenticity, and Freshness (CIAF) in WSN. Advances in Intelligent Systems and Computing, 1158, 87–97. https://doi.org/10.1007/978-981-15-4409-5_8.

[11] Farooq, M. S., Riaz, S., & Alvi, A. (2023). Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. Electronics (Switzerland), 12(14).

https://doi.org/10.3390/electronics12143077.

[12] Amutha, J., Sharma, S., & Nagar, J. (2020). WSN Strategies Based on Sensors, Deployment, Sensing Models, Coverage and Energy Efficiency: Review, Approaches and Open Issues. Wireless Personal Communications, 111(2), 1089–1115. https://doi.org/10.1007/s11277-019-06903-z.

[13] Salmi, S., & Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data, 10(1). https://doi.org/10.1186/s40537-023-00692-w.

[14] Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. Sensors, 22(13). https://doi.org/10.3390/s22134730.

[15] Ali, S., Humaria, A., Ramzan, M. S., Khan, I., Saqlain, S. M., Ghani, A., Zakia, J., & Alzahrani, B. A. (2020). An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International Journal of Distributed Sensor Networks, 16(6). https://doi.org/10.1177/1550147720925772.

[16] Eka Putra, F. P., Amir Hamzah, Agel, W., & Firmansyah Kusuma, R. O. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. Jurnal Sistim Informasi Dan Teknologi, 5(4), 82–87. https://doi.org/10.60083/jsisfotek.v5i4.329.

[17] Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., & Yang, Y. (2020). Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. Wireless Communications and Mobile Computing, 2020. https://doi.org/10.1155/2020/2643546.

[18] Faris, M., Mahmud, M. N., Salleh, M. F. M., & Alnoor, A. (2023). Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management, 15, 1–29. https://doi.org/10.1177/18479790231157220.

[19] Talukder, M. A., Khalid, M., & Sultana, N. (2025). A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. Scientific Reports, 15, 4617. https://doi.org/10.1038/s41598-025-87028-1.

[20] Guerrero-Sanchez, A. E., Rivas-Araiza, E. A., Gonzalez-Cordoba, J. L., Toledano-Ayala, M., & Takacs, A. (2020). Blockchain mechanism and symmetric encryption in a wireless sensor network. Sensors (Switzerland), 20(10). https://doi.org/10.3390/s20102798.

[21] Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486–492. https://doi.org/10.1016/j.procs.2021.02.088.

[22] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. Future Internet, 15(6), 1–45. https://doi.org/10.3390/fi15060200.

[23] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: An up-to-date survey. Applied System Innovation, 3(1), 1–24. https://doi.org/10.3390/asi3010014.

[24] Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., & Arshad, A. (2021). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(1), 547–566. https://doi.org/10.1007/s12652-020-02020-z.

[25] Ramadevi, P., Ayyasamy, S., Suryaprakash, Y., Anilkumar, C., Vijayakumar, S., & Sudha, R. (2023). Security for wireless sensor networks using cryptography. Measurement: Sensors, 29(August), 100874. https://doi.org/10.1016/j.measen.2023.100874.

[26] Oztoprak, A., Hassanpour, R., Ozkan, A., & Oztoprak, K. (2024). Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review. ACM Computing Surveys, 57(4). https://doi.org/10.1145/3706583.

[27] Nancy, P., Muthurajkumar, S., Ganapathy, S., Santhosh Kumar, S. V. N., Selvi, M., & Arputharaj, K. (2020). Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks. IET Communications, 14(5), 888–895. https://doi.org/10.1049/iet-com.2019.0172 .

[28] Mengistu, T. M., Kim, T., & Lin, J. W. (2024). A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors, 24(3). https://doi.org/10.3390/s24030968.

[29] Heidari, A., & Mollah, M. (2024). Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults. Concurrency and Computation: Practice and Experience, 36(3), e8252. https://doi.org/10.1002/cpe.8252.

[30] Keerthika, M., & Shanmugapriya, D. (2021). Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures. Global Transitions Proceedings, 2(2), 362–367. https://doi.org/10.1016/j.gltp.2021.08.045.

[31] Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic Data Security for Reliable Wireless Sensor Network. Alexandria Engineering Journal, 72, 37–50. https://doi.org/10.1016/j.aej.2023.03.061.

[32] Panahi, U., & Bayılmış, C. (2023). Enabling secure data transmission for wireless sensor networks based IoT applications. Ain Shams Engineering Journal, 14(2). https://doi.org/10.1016/j.asej.2022.101866.

[33] Ramadevi, P., Ayyasamy, S., Suryaprakash, Y., Anilkumar, C., Vijayakumar, S., & Sudha, R. (2023). Security for wireless sensor networks using cryptography. Measurement: Sensors, 29(August), 100874. https://doi.org/10.1016/j.measen.2023.100874.

[34] Rehman, A., Abdullah, S., Fatima, M., Iqbal, M. W., Almarhabi, K. A., Ashraf, M. U., & Ali, S. (2022). Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain. Applied Sciences (Switzerland), 12(21). https://doi.org/10.3390/app122110794.

[35] Hsiao, S. J., & Sung, W. T. (2021). Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks. IEEE Access, 9, 72326–72341. https://doi.org/10.1109/ACCESS.2021.3079708.

[36] Venčkauskas, A., Taparauskas, M., Grigaliūnas, Š., & Brūzgienė, R. (2024). Enhancing Communication Security an In-Vehicle Wireless Sensor Network. Electronics (Switzerland), 13(6). https://doi.org/10.3390/electronics13061003.

[37] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors, 22(6), 1–36. https://doi.org/10.3390/s22062087.

[38] Mahlake, N., Mathonsi, T. E., Du Plessis, D., & Muchenje, T. (2023). A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things. Journal of Communications, 18(1), 47–57. https://doi.org/10.12720/jcm.18.1.47-57.

[39] Paharia, B., & Bhushan, K. (2019). A comprehensive review of distributed denial of service (DDoS) attacks in fog computing environment. In Handbook of Computer Networks and Cyber Security: Principles and Paradigms. https://doi.org/10.1007/978-3-030-22277-2_20.

[40] Tariq, M. I., Ahmed, S., Memon, N. A., Tayyaba, S., Ashraf, M. W., Nazir, M., Hussain, A., Balas, V. E., & Balas, M. M. (2020). Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. Sensors (Switzerland), 20(5), 1–36. https://doi.org/10.3390/s20051310.

[41] Moghadam, M. F., Nikooghadam, M., Jabban, M. A. B. Al, Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network. IEEE Access, 8, 73182–73192. https://doi.org/10.1109/ACCESS.2020.2987764.

[42] Nourildean, S. W., Hassib, M. D., & Mohammed, Y. A. (2022). Internet of things based wireless sensor network: a review. Indonesian Journal of Electrical Engineering and Computer Science, 27(1), 246–261. https://doi.org/10.11591/ijeecs.v27.i1.pp246-261.

[43] Chandnani, N., & Khairnar, C. N. (2022). An analysis of architecture, framework, security and challenging aspects for data aggregation and routing techniques in IoT WSNs. Theoretical Computer Science, 929(June 2022), 95–113. https://doi.org/10.1016/j.tcs.2022.06.032.

[44] Putra, F. P. E., R.A, M. K., G, M. W. R., & Huda, V. (2025). Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik. 8(2), 334–344. https://doi.org/10.29408/jit.v8i2.30230

[45] Putra, F. P. E., Tamam, A. B., Efendi, R. W., & Muim, Z. (2024). Optimasi Keamanan DNS_ Eksplorasi Optimal dengan Implementasi DNS Security Extensions (DNSSEC). Riset Dan E-Jurnal Manajemen Informatika Komputer, 8(1), 349–358. DOI:10.33395/remik.v8i1.13398.

[46] Putra, F. P. E., Mufidah, K., Ilhamsyah, R. M., Efendy, S. A., & Barokah, S. N. R. (2024). Tinjauan Performa RouterOS Mikrotik dalam Jaringan Internet: Analisis Kinerja dan Kelayakan. Digital Transformation Technology, 3(2), 903–910. https://doi.org/10.47709/digitech.v3i2.3446.

[47] Putra, F. P. E., Ubaidi, U., Hamzah, A., Pramadi, W. A., & Nuraini, A. (2024). Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap. Brilliance: Research of Artificial Intelligence, 4(1), 348–355. https://doi.org/10.47709/brilliance.v4i1.4227.

[48] Putra, F. P. E., Ubaidi, U., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study. Brilliance: Research of Artificial Intelligence, 4(1), 413–421. https://doi.org/10.47709/brilliance.v4i1.4357.

[49] Prasetyo, F., Putra, E., Mahmud, M. A., & Maqom, I. S. (2024). Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus Digital Transformation Technology (Digitech) | e-ISSN : 2807-9000 Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus. March. https://doi.org/10.47709/digitech.v3i2.3457.

[50] Prasetyo, F., Putra, E., Riski, M., Yahya, M. S., & Ramadhan, M. H. (2023). Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G. Jurnal Sistim Informasi Dan Teknologi, 5(2), 167–174. https://doi.org/10.37034/jsisfotek.v5i1.233.

[51] Putra, F. P. E., Syirofi, S., Wahid, D., & Syam, A. M. (2025). Security Analysis And Data Recovery On Large-Scale Computer Networks. Brilliance: Research of Artificial Intelligence, 5(1), 384–390. https://doi.org/10.47709/brilliance.v5i1.6276.