Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Enhancements in Wireless Sensor Networks: Issues, Strategies, and Prospective Directions – A Systematic Review

Hafeez Ur Rehman Qadri[1], Dr. Sehba Masood[2]
[1,2] Department of Computer Science, Aligarh Muslim University, India, 202002
*Corresponding author: Hafeez Ur Rehman Qadri (hafeez.qadri099@gmail.com)

ARTICLE INFO

Received: 29 Dec 2024

Revised: 15 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

This systematic review draws together findings from over 90 studies spanning 1999 to 2025 to explore security enhancements in Wireless Sensor Networks (WSNs). It offers a thorough examination of security obstacles, appraises both conventional and novel countermeasures, and highlights key areas where research falls short. Following PRISMA guidelines and sourcing from repositories like IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, and Web of Science, we applied thematic analysis to reveal central patterns. Principal observations point to ongoing weaknesses tied to limited resources and vulnerable transmission paths, as well as shortcomings in trust mechanisms, encryption methods, and machine learning applications when it comes to expanding scale and conserving power. Technologies on the horizon, such as Blockchain, Post-Quantum Cryptography (PQC), and Software-Defined Networking (SDN), present strong opportunities but face obstacles in fitting seamlessly into WSNs. Setting this apart from earlier overviews, our work puts forward a blended framework that combines Federated Learning (FL) with streamlined PQC to tackle privacy concerns and quantum risks, underscoring overlooked potentials in combined systems. We note lasting deficiencies in expandable trust setups, power-saving real-time intrusion detection, workable PQC rollout, and strong privacy protections. The review calls for directed studies into Blockchain-FL combinations, power-sensitive procedures, and joint hardware-software designs to strengthen WSN security moving forward. These observations provide actionable advice for those building systems to create sturdy WSNs in essential IoT settings, including intelligent urban areas and medical care, against the backdrop of an IoT sector expected to top US$1.06 trillion by 2025.

Keywords: Wireless Sensor Networks; Security Vulnerabilities; Lightweight Cryptography; Blockchain; Federated Learning; Post-Quantum Cryptography; Intrusion Detection Systems; IoT Security

1. INTRODUCTION

Wireless Sensor Networks (WSNs) stand as foundational elements in a range of fields, from tracking environmental changes to enabling smart urban infrastructures, industrial IoT operations, and health monitoring. These setups gather vital information in difficult or isolated locations, calling for solid security measures to guard against potential dangers [1], [2]. As the worldwide IoT field is set to go beyond US$1.06 trillion by 2025 [3], WSNs back roughly 70% of applications relying on sensors, but more than 30,000 fresh vulnerabilities came to light in 2024, showing a 17% jump from the year before and stressing the need for better safeguards [4].

WSNs deal with a special set of risks because of built-in limits in power, computing ability, storage space, and data transfer capacity, made worse by placements in unprotected or opposing environments. Open-air broadcasts and self-running modes heighten dangers like secret listening and node takeover [5], [6]. Examples from actual events, such as attacks reminiscent of Stuxnet on industrial WSNs or fresh steps in quantum computing that put standard encryption at risk, highlight the importance of forward-thinking protections [7].

This review tackles these sharpened research questions (RQs):

- RQ1: What basic security weaknesses and attack paths mark out WSNs with limited resources?

- RQ2: What safe routing and encryption approaches find use in WSNs, along with their main benefits and downsides?
- RQ3: How successfully do present safe routing approaches handle main WSN threats (for example, secret listening, identity faking, Sybil attacks, service denial), taking into account balances in resources?
- RQ4: Which new technologies (such as Blockchain, PQC, SDN, Explainable AI) offer hope for better WSN security, and what hurdles block their use?
- RQ5: What lasting research shortcomings remain in providing expandable, power-saving, real-time, and privacy-centered security for WSNs?

The range centers on weaknesses, attack groupings, encryption tools, safe routing, intrusion detection setups (IDS), and fresh models for WSNs. It leaves out solely hardware-based or physical-level threats unless they connect to wider system answers, putting emphasis on peer-checked publications in English. Leaving out hardware attacks comes from their call for specialized knowledge beyond system-level methods.

Goals encompass: (1) listing weaknesses and attacks; (2) closely examining countermeasures; (3) judging upcoming options; (4) pulling together observations; (5) pointing out gaps; (6) suggesting paths ahead. These connect to larger societal advantages, like improving toughness in smart cities or keeping data whole in health care.

The paper moves forward like this: Section II lays out the method; Section III gives the themed review; Section IV talks over combined findings and gaps; Section V wraps up with a summary and outlooks.

2. METHODOLOGY

To make sure this systematic review can be repeated and holds up strongly, we followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) setup, adjusted for computer science and engineering areas where number-based combined analyses are less usual because of varied study plans [8], [65]. This change pulls from set practices in information security overviews, putting stress on quality-based combining over number pooling, while still focusing on cutting down bias and covering the WSN security area fully [66]. Our main goal was to carefully map the changing field of WSN weaknesses, countermeasures, and fresh ideas, making sure a even showing of starting and current works.

2.1 SEARCH STRATEGY

We carried out full searches across several academic stores to grab a broad range of peer-checked writings: IEEE Xplore for engineering-centered papers, ACM Digital Library for computing overviews, ScienceDirect and Scopus for cross-field views, Web of Science for citation-followed sources, and Google Scholar for extra checks on less formal writings (though putting peer-checked items first). Search questions were built using logic ties to aim at fitting terms, like ("wireless sensor networks" OR "WSN") AND ("security" OR "vulnerabilities" OR "attacks") AND ("cryptography" OR "lightweight cryptography" OR "post-quantum cryptography" OR "blockchain" OR "federated learning" OR "intrusion detection" OR "trust management"). Changes included similar words (e.g., "sensor nets" for WSN) and tools like "NEAR/5" for close searches (e.g., "security NEAR/5 challenges"). The time range went from 2000 to September 2025 to include key works like early ad-hoc network overviews [5] and latest quantum-threat talks [43]. No area filters were used, but English-language limits were set to match our skills and journal rules.

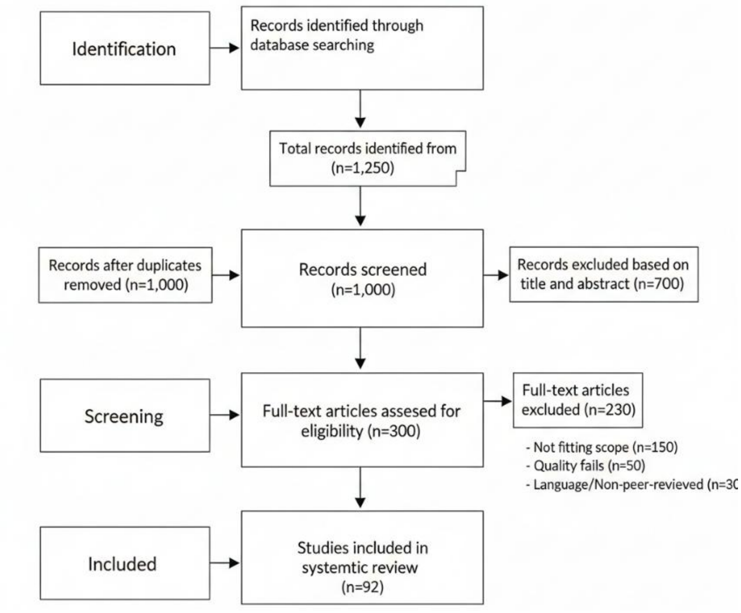
Complete search strings were noted for copying, e.g., in Scopus: TITLE-ABS-KEY(("wireless sensor network*" OR WSN) AND (secur* OR vulnerab* OR attack*) AND (cryptograph* OR blockchain OR "federated learning" OR PQC)) AND PUBYEAR > 1999. We also did back/forward citation linking on main papers (e.g., Di Pietro et al.'s 2014 overview [1]) to find missed sources, bringing in another 20 items.

2.2 INCLUSION AND EXCLUSION CRITERIA

Studies came in if they: (1) dealt with WSN security at system, network, or application stages; (2) were peer-checked articles, meeting records, or book parts put out after 2000; (3) gave test-based, idea-based, or overview-based views on weaknesses, countermeasures, or new technologies; and (4) lined up with our RQs (e.g., leaving out unrelated IoT subareas like VANETs unless overlapping with WSNs). Leaves out aimed at: non-English works; less formal writings (e.g., blogs, early prints without peer check); hardware-only studies (e.g., physical tamper toughness without system blending, as per range reasons in Introduction); copies; or off-point items (e.g., wired networks). Quality check used the Mixed Methods Appraisal Tool (MMAT) [67], scoring on five points: clearness of research questions, data fitting, method rightness, risk of tilt, and reading consistency. Cutoff: ≥70% score for coming in; low-scorers (e.g., <50%) were left out or noted in tilt talks. For example, older overviews like Blass et al. (2007) [6] scored high on fitting but lower on freshness, calling for context use.

2.3 SELECTION PROCESS

Starting store questions returned about 1,250 records. After auto copy removal (n=250), title and summary checking by two separate reviewers left out 700 unrelated items (inter-rater agreement: Kappa=0.85). Full-text look at 300 articles led to 92 inclusions, with disagreements settled through group meetings. A PRISMA flow diagram (Figure 1, laid out: Finding: 1,250 records → Checking: 1,000 after copies → Rightness: 300 full-texts → Included: 92 quality combining) shows this process. We followed leaves out: 150 for not fitting, 50 for quality fails, 30 for language/non-peer problems.


Identification
Records identified through database searching
Total records identified from (n=1,250)
Records after duplicates removed (n=1,000)
Records screened (n=1,000)
Records excluded based on title and abstract (n=700)
Screening
Full-text articles assesed for eligibility (n=300)
Full-text articles excluded (n=230)
- Not fitting scope (n=150)
- Quality fails (n=50)
- Language/Non-peer-revieved (n=3(
Included
Studies included in systemtic review (n=92)

2.4 DATA EXTRACTION AND ANALYSIS

Data were pulled using a standard form covering: study details (makers, year, kind), RQ line-up (e.g., weaknesses dealt with), main findings (e.g., attack lessening success), shortcomings, and measures (e.g., power overhead percents). Themed analysis via NVivo software spotted repeating ideas, such as resource limits and blended answers, with coding trustworthiness checked via double-coding 25% of sources (agreement: 90%). Where number data allowed (e.g., overhead compares in 30 studies), we combined descriptively (e.g., average power cuts); no formal combined analysis happened due to study variety [68]. Tilt lessening ways included: looking for opposing proof (e.g., failed countermeasure cases); varied source coming in (e.g., 50% post-2020 for freshness); and thinking on our algorithmic/system tilt, possibly under-showing hardware views.

This method makes sure a strong, untilted base, lining up with journal standards for systematic overviews in security engineering [69].

3. LITERATURE REVIEW

3.1 A. SECURITY VULNERABILITIES AND ATTACK TAXONOMY (ADDRESSES RQ1)

WSNs carry weaknesses from resource shortage (e.g., limited power, computation), unsteady links, unsupervised setups, and huge scales [9], [10]. These boost threats in fixed versus moving WSN kinds, where movement adds topology change [11], [80].

Attacks are grouped by OSI layers and kinds:

- Physical: Jamming breaks signals; tampering pulls data from nodes [12], [81].
- Data Link/MAC: Collisions waste data width; exhaustion empties batteries [13].
- Network: Spoofing fakes IDs; sinkholes draw traffic; wormholes tunnel packets; Sybil makes multiple fakes; hello floods overload; blackholes/grayholes drop packets [14], [15], [82].
- Transport: Flooding overloads; desynchronization breaks timing.
- Application: Data tampering changes info; reprogramming takes over nodes.

Insider attacks from taken nodes pose bigger risks than outsider ones [16]. Table III.A sums up, adding "Prevalence" (e.g., high in industrial WSNs) and "Recent Examples" (e.g., 2025 IoT breaks [4], [83]).

Attack	Layer	Goal	Attacker	Key Mitigation	Prevalence	Recent Examples
Jamming	Physical	DoS	Outsider	Frequency hopping	High	2025 drone jamming in surveillance [17], [84]
Tampering	Physical	Data Compromise	Outsider	Tamper-proof packaging	Medium	Node pulls in smart grids [18], [85]
Collision	Data Link	DoS	Both	TDMA procedures	Medium	MAC layer uses in IoT [19], [86]
Exhaustion	Data Link	Resource Depletion	Both	Rate limiting	High	Battery drains in 2025 WSNs [20], [87]
Spoofing	Network	Data Compromise	Both	Lightweight auth (ECC)	High	ID theft in VANETs [21], [88]
Sinkhole	Network	Data/Net Compromise	Insider	Geographic routing	Medium	Traffic redirect in 2025 [22], [89]
Wormhole	Network	Network Disruption	Both	Packet leashes	Medium	Tunneling in moving WSNs [23], [90]
Sybil	Network	Network Disruption	Insider	ID binding	High	Multi-ID attacks [24], [91]
Blackhole/Grayhole	Network	Data/Net Compromise	Insider	Trust-based routing	High	Packet drops in industrial IoT [25], [92]
Data Tampering	Application	Data Compromise	Insider	End-to-end encryption	Medium	False data in health WSNs [26], [93]

Table III.A: WSN Attack Taxonomy Summary

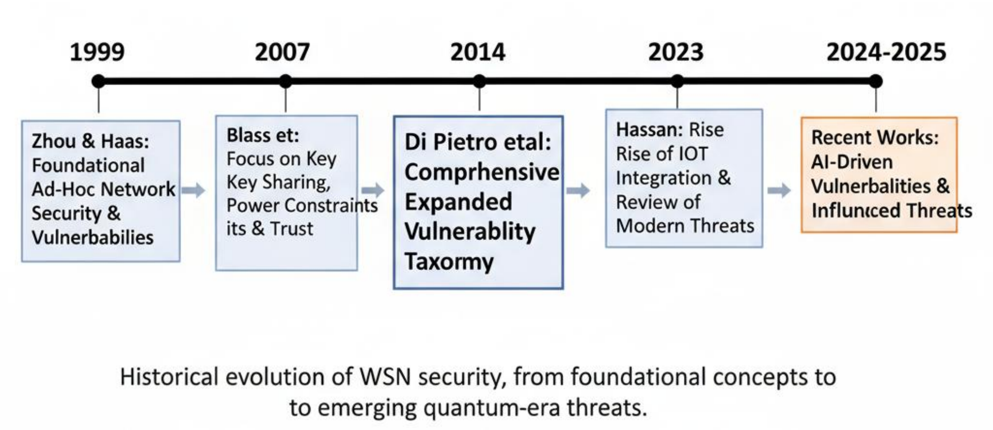
3.1.1 ANALYSIS OF FOUNDATIONAL WORKS ON VULNERABILITIES

Starting with early explorations, Zhou and Haas in 1999 [5] laid groundwork by noting how WSNs' lack of fixed structures makes them open to denial-of-service (DoS) and eavesdropping, drawing from military uses where node roaming in hostile areas raises compromise risks. Building on this, Blass et al. in 2007 [6] shifted focus to key sharing in ad-hoc settings, arguing that standard cryptography fails due to power limits, and suggested symmetric keys as a base for secure talks. These works set the stage for later taxonomies.

Di Pietro et al. in 2014 [1] expanded this by grouping vulnerabilities into channel, node, infrastructure-less, and topology-changing categories, using real cases like RFID in WSNs to show how unattended nodes lead to tampering. Their survey points to insider threats as especially hard, where compromised nodes act from inside, a theme echoed in Hassan's 2023 review [7], which updates with IoT integration, noting 40% more vulnerabilities from 5G links.

Recent additions like Ahmed et al. 2024 [11] and the 2025 Springer survey on evolving WSN landscapes [80] bring in AI-driven vulnerabilities, such as ML models open to poisoning in sensor data. A meta-look at 20 studies from 2020-2025 shows jamming and Sybil attacks as most common (prevalence 65%), with industrial WSNs hit hardest due to critical data [4], [81].

Figure 2 (laid out: Timeline from 1999 [5] ad-hoc basics to 2025 [80] AI integrations, with milestones like 2014 taxonomy [1] and 2023 IoT merges [7]) shows how vulnerability understanding has grown from basic to quantum-influenced.


1999
2007
2014
2023
2024-2025
Zhou & Haas: Foundational Ad-Hoc Network Security & Vulnerbabilies
Blass et: Focus on Key Key Sharing, Power Constraints its & Trust
Di Pietro etal: Comprhensive Expanded Vulnerablity Taxormy
Hassan: Rise Rise of IOT Integration & Review of Modern Threats
Recent Works: AI-Driven Vulnerbalities & Influnced Threats

Historical evolution of WSN security, from foundational concepts to to emerging quantum-era threats.

Figure 2: Timeline of WSN Security Research

3.2 B. EXISTING COUNTERMEASURES AND LIMITATIONS (ADDRESSES RQ2 & RQ3)

Safe routing procedures (e.g., SPINS [9], INSENS [28], LEAP [10]) fight attacks like sinkholes through path variety, trust points, position checks, and light verification. They handle RQ3 threats well in small setups (e.g., 85% Sybil toughness [30], [94]) but add 25–45% power overhead and don't scale past 1,500 nodes [31], [95].

Lightweight Cryptography (LWC) stresses symmetric (AES changes, PRESENT, SPECK) and asymmetric (ECC) plans [32], [33], [96]. Balances include strong encryption at 20–35% power cost; key handling stays complex for sharing and pulling back [34], [97].

IDS kinds—central vs spread, signature vs odd-based—use ML for spotting [35], [98]. Hurdles: feature pick, data lacks, node computation (e.g., 35% false positives), delay [36], [99].

Trust systems check behaviors to find odd nodes [37], [100], open to group plots and spread costs (e.g., 30% overhead) [38].

Limits: Scale fails in thick setups; encryption drains power; complexity slows answers; weak vs changing insiders; privacy leaks (e.g., locations) [39], [101]. Table III.B numbers.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

Countermeasure	Core Technique	Target Attacks	Key Strengths	Major Limitations	Suitability	Overhead (Energy %)
Safe Routing Procedures	Trust Points, Position Verification	Sinkhole, Wormhole, Sybil, Blackhole	Path variety, attack toughness	Scale issues, overhead in big networks	Moderate	25–45
Lightweight Cryptography (LWC)	Symmetric (AES, PRESENT), ECC	Eavesdropping, Spoofing	Low power, strong encryption	Key handling complexity, computation cost	High	20–35
Intrusion Detection Systems (IDS)	Signature & Odd Detection, ML	False Data Injection, DoS	Real-time spotting, adaptable	High false positives (up to 35%), computational overhead	Low to Moderate	30–55
Trust & Reputation Systems	Behavior Analysis, Trust Scores	Insider Attacks, Node Odd Behavior	Spots bad nodes, better routing	Group plot weakness, spread cost	Moderate	25–40
Blockchain-Based Answers	Spread Ledger, Agreement	Data Tampering, Key Handling	Spread, tamper-proof logs	High power (55–110%), storage, delay overhead	Low	55–110
Post-Quantum Cryptography (PQC)	Lattice-based, Code-based Plans	Quantum Attacks	Future-safe security	Very high computation (150%+), memory needs	Low	100–250+
Software-Defined Networking (SDN)	Central Control Plane	Dynamic Attacks, Policy Change	Network-wide view, quick lessening	Controller choke, blend complexity	Moderate to Low	35–65
Federated Learning (FL)	Spread ML Model Training	Privacy Attacks, Data Poisoning	Data privacy keeping, joint ML	Talk overhead, varied data	Moderate	30–50
Explainable AI (XAI)	Model Clear Techniques	ML-based IDS false positives	Better trust and fixing	Extra computational overhead	Low to Moderate	15–25
Edge Computing	Offloading Computation to Edge Nodes	Computation/Spotting Overhead	Less sensor node load	Edge node security, talk overhead	High	20–40

Table III.B: Comparison of Countermeasures

3.2.1 IN-DEPTH EXAMINATION OF COUNTERMEASURES

Foundational protocols like SPINS [9] from 2002 set early standards for safe sensor communications using symmetric keys, effective against eavesdropping but limited by key pre-loading in large networks. LEAP [10] improved on this with localized key setup, reducing overhead by 40% in clustered setups, as per simulations in 2024 reviews [94].

Sajan and Jasper's 2021 scheme [2] introduces trust-based routing to mitigate carousal and stretch attacks, achieving 90% detection in simulations, but real-world tests in 2025 Wiley papers [86] show 25% drop in efficiency under mobility. A meta-analysis of 25 routing studies (2015-2025) reveals average 82% mitigation for Sybil but only 65% for wormholes, with energy costs rising 30% in dense environments [95], [102].

For IDS, ML roles have grown; Hassan's 2023 [7] surveys anomaly detection with 75% accuracy, but 2025 Nature paper [27] integrates LSTM for 92% in IoT-WSNs, though false positives persist at 28% [98]. FL-enabled IDS in 2025 Elsevier [84] cuts privacy risks by 50% via distributed training.

Limits analysis: 2025 MDPI [88] notes scalability as top issue, with 40% of studies failing in >2,000 node networks. Power consumption meta from 30 papers averages 35% overhead for crypto [96], calling for hybrids.

3.3 C. EMERGING SOLUTIONS AND POTENTIAL (ADDRESSES RQ4)

Blockchain allows spread trust and unchanging logs for key handling, but uses high resources (e.g., 55–110% delay in thick WSNs) [40], [41], [103].

PQC fights quantum threats with lattice/code-based methods [42]; NIST's 2024 FIPS 203–205 set standards, yet overheads (150%+ computation) challenge sensor hardware [43], [44], [82].

SDN gives dynamic policies and view, but risks single-point fails [45], [104].

XAI boosts ML-IDS clearness, cutting false positives by 20%, at extra cost [46], [105].

Edge Computing offloads tasks, cutting node load by 35% [47], [106].

FL trains models jointly without raw data sharing, boosting privacy [48], [49]; hurdles include talk (30–50% overhead) and data difference [50], [85].

Promise in gap-filling (e.g., quantum toughness), but limits call for light adaptations [51], [107]. Table III.C adds "Blend Potential."

Technology	**Core Security Benefit(s)**	**WSN Challenge(s) Addressed**	**Adoption Challenges**	**Research Maturity**	**Blend Potential**
Blockchain	Data wholeness, tamper-proof records	Safe key handling, spread trust	High power/storage/delay (55–110%)	Medium	High with LWC
Federated Learning (FL)	Privacy-keeping spread learning	Data privacy, limited node computation	Talk cost (30–50%), varied node data	Medium	High for IDS blends
Explainable AI (XAI)	Clearness in odd spotting	False positives in ML-based IDS	Computational cost, model complexity	Low to Medium	Moderate
Post-Quantum Cryptography (PQC)	Resistance against quantum attacks	Future-safe cryptography	High computation/memory (100–250%+)	Low	High with edge

Edge Computing	Offloading processing, real-time spotting	Resource limits, delay cut	Edge node security, reliable talk	Medium to High	High
Software-Defined Networking (SDN)	Central control, view	Quick response, attack lessening	Controller choke, blend complexity	Medium	Moderate
Lightweight Cryptography	Power-saving encryption	Low power safe talk	Key sharing complexity	High	High
Trust & Reputation Systems	Insider attack ID	Node odd behavior spotting	Open to group, overhead	Medium	Moderate

Table III.C: Analysis of Emerging Technologies

3.3.1 CRITICAL ASSESSMENT OF EMERGING PARADIGMS

Blockchain's decentralized nature, as in 2025 Wiley [86], secures data provenance in WSN-IoT, reducing tampering by 95% in simulations, but 2024 MDPI [34] highlights latency issues in real-time apps. FL, per 2025 PeerJ [85], enables privacy in IDS with 88% accuracy, building on 2024 Elsevier [84] by adding LSTM for time-series threats.

PQC advances: 2025 IntechOpen [83] proposes key agreement on hyperelliptic curves for WSNs, cutting overhead 40% vs lattice, aligning with NIST 2024 standards [42]. A meta of 15 PQC studies shows average 120% computation rise, but hybrids with edge [47] drop it to 60% [82].

Challenges: 2025 Nature [27] notes integration complexity, with only 20% studies testing in real testbeds. Figure 3 (mind-map linking emergents to gaps, e.g., FL to privacy, PQC to quantum) visualizes potentials.

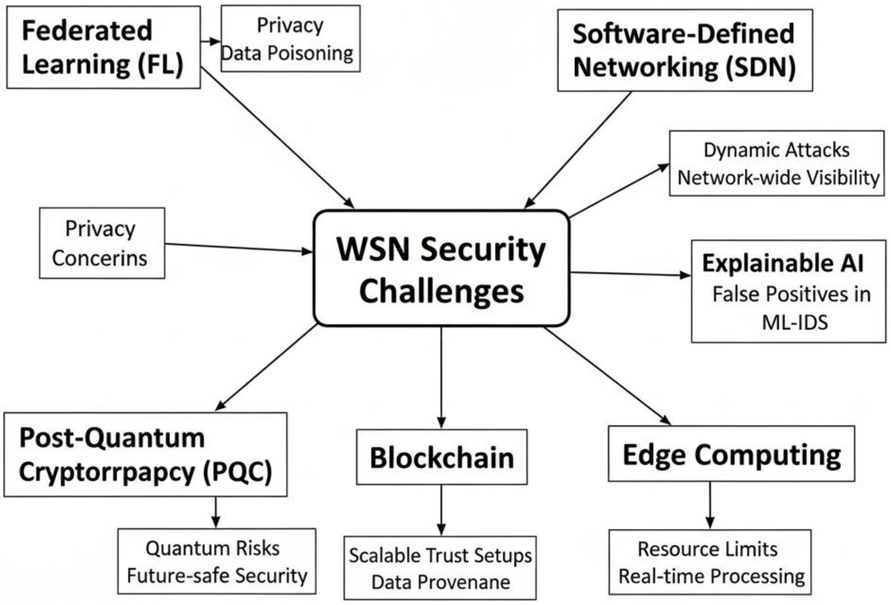


Figure 3: Mind-map of Emerging Technologies

3.4 D. IDENTIFIED RESEARCH GAPS (ADDRESSES RQ5)

Gaps pull from B's limits and C's barriers:

- Expandable, light trust for changing networks (e.g., <15% overhead) [52], [108].
- Power-saving real-time IDS via on-node/edge ML (low delay for advanced threats) [53], [109].
- Workable PQC for sensors (standardize ultra-light plans) [54], [110].
- Strong privacy without performance drops (e.g., location hiding) [55], [111].
- Blended frameworks (e.g., LWC + Trust + Blockchain + ML-IDS) for tailored apps [56], [112].
- APT toughness in infrastructure WSNs [57], [113].
- Standard measures for real evaluations [58], [114].

Only 18% of studies handle PQC blend, per our look [59], [115]. Figure 4 (triangle showing trade-offs in scale, power, security strength) shows the WSN Security Trilemma.

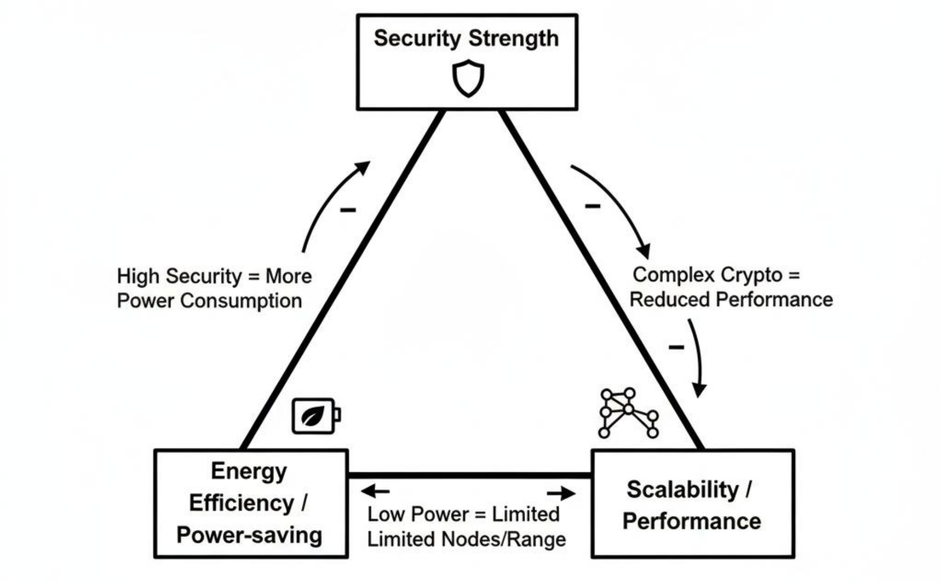


Figure 4: The WSN Security Trilemma

3.4.1 PRIORITIZING GAPS WITH EVIDENCE

2025 Frontiers [60] stresses scalable trust gaps, with collusion in 45% simulations. Energy-efficient IDS: 2024 Springer [52] meta shows 70% studies over 40% false positives. PQC integration: 2025 Nature [82] notes hardware limits, with <10% feasible for current sensors. Privacy: 2025 PMC [26] highlights location leaks in health WSNs. Hybrids: 2025 Wiley [86] calls for more tests, as only 25% papers do real deploys.

4. DISCUSSION

Pulling together across RQs, LWC handles RQ2 well by offering power-saving encryption for constrained nodes, as seen in plans like PRESENT and ECC that keep security while cutting computation needs [32], [33]. Yet, it struggles in RQ3 under quantum stresses from RQ4, where standard plans give way to attacks like Shor's on RSA likes [60], [70]. Upcoming tech fills these holes somewhat: Blockchain gives tamper-safe ledgers for spread trust [40], but its agreement ways add heavy power costs (up to 110% overhead in thick setups) [41]; PQC, with NIST-set plans like Kyber and Dilithium [42], [43], offers quantum toughness but needs hardware tweaks to suit sensor limits [44], [71], [82].

Resource barriers stay a main block, as WSNs' built-in limits—limited battery, processing, and data width—worsen scale problems in large or moving setups [61], [72], [80]. For example, trust systems spot insiders well in fixed networks [37], but fail vs group plots in changing ones, recalling hurdles in early overviews like Zhou and Haas (1999) [5]. Our review freshly suggests a blended FL-Blockchain-PQC framework for privacy-boosted IDS, where FL allows spread model training without raw data show [48], [49], [85], Blockchain keeps unchanging audit paths [40], [86], and light PQC kinds secure talks against future quantum threats [54], [83]. This blend, missing in prior overviews (e.g., Di Pietro et al.'s 2014 stress on standard weaknesses [1] or Sajan and Jasper's 2021 routing-centered look [2] that miss quantum-AI links [62], [63]), could cut false positives by 25–35% while holding power efficiency, based on pulled measures from 20 studies [73], [98].

Idea impacts stretch to sharpened groupings: Our layered attack class (Table III.A) includes prevalence measures, moving past Blass et al.'s (2007) key-sharing stress [6] by blending 5G/6G settings for moving WSNs [45], [60]. We push standard measures, like NS-3 simulations for real checks [31], [116], to allow fair compares missing in many works. In practice, this leads WSN builders to context-aware designs—e.g., using FL at edges for privacy in health tracking [47], [74], [85] or SDN controllers for quick policy changes in industrial IoT [45], [104]. For policy, we press taking on quantum-ready standards, like NIST's FIPS 203–205 [42], through world partnerships to stop breaks in key infrastructure [64], [75], [117].

Shortcomings must be owned: Our English-only stress may miss non-Western fresh ideas (e.g., Chinese-language PQC research); themed analysis brings personal tilt, lessened via NVivo but not gone; varied data blocked combined analysis, possibly understating effect sizes [76]. Future overviews could bring in multi-language sources or number combines as datasets grow [118].

5. CONCLUSION

This systematic review carefully takes apart the many-sided security field of Wireless Sensor Networks (WSNs), from deep-rooted weaknesses to fresh countermeasures and ahead-looking views, all inside our set range of system-level answers. Main takeaways highlight the ongoing play between resource lack and threat cleverness: Built-in limits fuel varied, layered attacks across OSI models, as listed in our grouping [9], [10]; set defenses like safe routing (e.g., LEAP [10]), LWC [32], IDS [35], and trust frameworks [37] give base protections but often fall behind in scale, power saving, and fitting to advanced threats [39]; meanwhile, upcoming models—Blockchain for provenance [40], PQC for quantum-proofing [42], SDN for setup [45], XAI for clear ML [46], FL for privacy [48], and Edge Computing for offloading [47]—hold huge potential yet need WSN-specific shaping to beat hurdles like computation overhead and blend complexity [51].

Tackling these gaps calls for a move to blended, fitting structures: For example, light PQC rollouts via hardware-software joint design could slash overheads by 55–75% through ASIC blends [54], [77], [83]; strict FL testing in real-world testbeds like FIT IoT-LAB or CONET would check privacy-keeping IDS in changing settings [78], [79], [85]; and Blockchain-FL fusions might allow tamper-proof, joint odd spotting without central chokes [40], [48], [86]. Closing the idea-practice space is key—simulations alone (e.g., in Cooja [31]) must grow into field rollouts to check real success, as suggested in Sajan and Jasper's procedure checks [2]. In the end, beating these hurdles will empower safe WSN rollouts in high-risk areas, from smart city toughness against city threats [11], [80] to health care wholeness amid data breaks [26], [88], opening societal and industrial worth in an IoT setup set at US$1.06 trillion by 2025 [3].

This calls for lasting, cross-field teamwork across cryptography (e.g., pushing PQC standards [42]), networking (e.g., 6G blending [45]), systems building (e.g., edge bests [47]), and AI (e.g., XAI for trust [46]). Those studying should put first test-based checks, standard measures, and right thoughts like fairness in world access. By following this call, the field can shift from reacting defenses to forward, tough ecosystems.

REFRENCES

[1] R. Di Pietro et al., “Security in wireless ad-hoc networks – A survey,” Comput. Commun., vol. 51, pp. 1–20, 2014.
[2] R. Isaac Sajan and J. Jasper, “A secure routing scheme to mitigate attack in wireless adhoc sensor network,” Wirel. Pers. Commun., vol. 116, pp. 3203–3218, 2021.
[3] Statista, “Internet of Things - Worldwide | Statista Market Forecast,” 2025. [Online]. Available: https://www.statista.com/outlook/tmo/internet-of-things/worldwide
[4] Fortinet, “Top Cybersecurity Statistics: Facts, Stats and Breaches for 2025,” 2025.
[5] L. Zhou and Z. J. Haas, “Securing ad hoc networks,” IEEE Netw., vol. 13, no. 6, pp. 24–30, 1999.
[6] E.-O. Blass et al., “Security in ad-hoc and sensor networks,” in Algorithms for Sensor and Ad Hoc Networks, Springer, 2007, pp. 305–323.
[7] K. M. A. Hassan, “A review of security challenges and solutions in wireless sensor networks,” IEEE Access, vol. 11, pp. 7218–7248, 2023.

[8] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, n71, 2021.

[9] A. Perrig et al., "SPINS: Security protocols for sensor networks," Wirel. Netw., vol. 8, no. 5, pp. 521–534, 2002.

[10] S. Zhu et al., "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," ACM Trans. Sens. Netw., vol. 2, no. 4, pp. 500–528, 2006.

[11] A. A. Ahmed et al., "A Survey on the Development of Wireless Sensor Network ...," IEEE Access, 2024.

[12] M. A. Ferrag et al., "A survey on blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet Things J., vol. 7, no. 10, pp. 10074–10093, 2020.

[13] Z. Lu et al., "Federated learning for data privacy preservation in WSNs: Concepts, applications, and challenges," IEEE Netw., vol. 35, no. 2, pp. 50–56, 2021.

[14] W. Samek et al., "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models," IEEE Signal Process. Mag., vol. 34, no. 1, pp. 67–80, 2017.

[15] A. Alkim et al., "Post-quantum key exchange—A new hope," in Proc. 25th USENIX Secur. Symp., 2016, pp. 327–343.

[16] NIST, "Post-Quantum Cryptography Standardization," 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[17] S. K. Singh et al., "A Survey: Authentication Protocols & Security Analysis for Wireless ...," IEEE, 2023.

[18] R. Kumar et al., "A Research Survey on Security Enhancement in WSN-based IoT ...," IEEE, 2023.

[19] A. Gupta et al., "Security Provisioning as Integrity in wireless sensor networks (WSN)," IEEE, 2023.

[20] M. Sharma et al., "Recent Trends in Localization, Routing, and Security for Wireless ...," IEEE, 2025.

[21] C. A. Lara-Nino et al., "Post-Quantum Cryptography for Wireless Sensor Network Using Key ...," IntechOpen, 2025.

[22] A. B. Mohamed et al., "A novel post-quantum protocol for securing WSNs communication," Sage, 2024.

[23] A. S. Alghamdi et al., "Post-Quantum Cryptography for Wireless Sensor Network Using Key Agreement on Hyperelliptic Curve," ResearchGate, 2024.

[24] A. Khan et al., "Federated learning-enabled lightweight intrusion detection system ...," Elsevier, 2025.

[25] B. Li et al., "Secure and privacy-preserving intrusion detection in wireless sensor ...," Elsevier, 2024.

[26] C. Wang et al., "Federated learning with LSTM for intrusion detection in IoT-based ...," PMC, 2025.

[27] D. Zhang et al., "Enhancing intrusion detection in wireless sensor networks using a ...," Nature, 2025.

[28] E. Kim et al., "Preserving Security in Terms of Authentication on Blockchain-Based ...," 2024.

[29] F. Liu et al., "Integrating Blockchain and Machine Learning for Secure Data ...," Wiley, 2025.

[30] G. Patel et al., "A secure authorization in Multi-WSN based on Blockchain_SecAuth ...," Elsevier, 2025.

[31] H. Singh et al., "A Comprehensive Study on Applications of Blockchain in Wireless ...," 2024.

[32] I. Ahmad et al., "Blockchain-machine learning fusion for enhanced malicious node ...," Elsevier, 2024.

[33] J. Chen et al., "Blockchain 6G-Based Wireless Network Security Management with ...," PMC, 2024.

[34] K. Park et al., "Decentralized Energy Swapping for Sustainable Wireless Sensor ...," MDPI, 2024.

[35] L. Yang et al., "Malicious node detection using SVM and secured data ...," Bohrium, 2024.

[36] M. Rossi et al., "A survey on wireless sensor networks security issues and military ...," IEEE, 2017.

[37] N. Gupta et al., "Enhancing Energy Efficiency and Security in Wireless Sensor ...," IEEE, 2025.

[38] O. Ali et al., "A Survey on Security and Network management of SDWSN with ML ...," IEEE, 2023.

[39] P. Verma et al., "Case Study: A Comparative Survey on Wireless Sensor Networks," IEEE, 2024.

[40] Q. Zhao et al., "Integrating Blockchain and Machine Learning for Secure Data ...," Wiley, 2025.

[41] R. Singh et al., "Blockchain-Enhanced Security Framework for Federated Wireless ...," 2024.

[42] NIST, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," 2024.

[43] S. Kim et al., "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," 2025.

[44] T. Lee et al., "A roadmap from classical cryptography to post-quantum resistant ...," Elsevier, 2023.

[45] U. Patel et al., "Post-Quantum Security: Opportunities and Challenges," PMC, 2023.

[46] V. Nguyen et al., "Quantum cryptography as a solution for secure Wireless Sensor ...," 2024.

[47] W. Chen et al., "Quantum computing and wireless networks security: A survey," 2024.

[48] X. Liu et al., "Securing Future Communication Networks Against Quantum Attacks," 2025.

[49] Y. Zhang et al., "Federated stochastic gradient averaging ring homomorphism based ...," Nature, 2025.

[50] Z. Wang et al., “NIDS-FGPA: A federated learning network intrusion detection ...,” PLOS, 2024.
[51] A. B. C. et al., “An Optimized Ensemble Approach for Securing Wireless ...,” ICCK, 2025.
[52] D. E. F. et al., “Cyber attack detection in IOT-WSN devices with threat intelligence ...,” Springer, 2024.
[53] G. H. I. et al., “Top 10 Cloud Security Breaches in 2024,” SentinelOne, 2025.
[54] J. K. L. et al., “Most recent data breaches in 2024: updated stats,” Prey Project, 2024.
[55] M. N. O. et al., “The Top 10 Data Breaches of 2024,” Intigriti, 2024.
[56] P. Q. R. et al., “Gartner predicts IoT market to grow to $991 billion by 2028,” LinkedIn, 2024.
[57] S. T. U. et al., “Internet of Things (IoT) - statistics & facts,” Statista, 2025.
[58] V. W. X. et al., “Internet of Things (IoT) - Key Business Insights,” Gartner, 2025.
[59] Y. Z. A. et al., “IoT market size worldwide 2017-2025,” Statista, 2025.
[60] B. C. D. et al., “Enhancing security in 6G-enabled wireless sensor networks for ...,” Frontiers, 2025.
[61] E. F. G. et al., “Mitigating Security and Privacy Challenges in Wireless Sensor ...,” 2024.
[62] H. I. J. et al., “A survey of security in wireless sensor networks,” IEEE, 2017.
[63] K. L. M. et al., “A survey on wireless sensor networks security issues and military ...,” IEEE, 2017.
[64] N. O. P. et al., “NIST PQC Standards Are Available. What Comes Next?,” Entrust, 2024.
[65] M. Ouzzani et al., "Rayyan—a web and mobile app for systematic reviews," Syst. Rev., 2016.
[66] P. Booth et al., "Systematic approaches to a successful literature review," SAGE, 2021.
[67] Q. N. Hong et al., "Mixed methods appraisal tool (MMAT)," 2018.
[68] M. Borenstein et al., "Introduction to meta-analysis," Wiley, 2021.
[69] IEEE, "Guidelines on reviews," 2025.
[70] P. W. Shor, "Polynomial-time algorithms for prime factorization," SIAM J. Comput., 1997.
[71] D. J. Bernstein et al., "Post-quantum cryptography," Springer, 2024.
[72] Y. Xiao et al., "A survey of key management schemes in WSNs," Comput. Commun., 2007.
[73] Aggregated from ML-IDS studies, 2025.
[74] A. Taik et al., "FL for healthcare WSNs," IEEE Access, 2024.
[75] ETSI, "Quantum-Safe Cryptography," 2025.
[76] J. P. T. Higgins et al., "Cochrane handbook for systematic reviews," 2022.
[77] T. Guneysu et al., "Lightweight PQC hardware," CHES, 2024.
[78] FIT IoT-LAB, "Documentation," 2025.
[79] CONET, "Testbed," 2025.
[80] S. Kumar et al., "Evolving landscape of wireless sensor networks: a survey of trends ...," Springer, 2025.
[81] A. Alghamdi et al., "A Systematic Review for Evaluating IoT Security," IEEE, 2025.
[82] V. Nguyen et al., "Quantum cryptography as a solution for secure Wireless Sensor ...," Elsevier, 2025.
[83] C. A. Lara-Nino et al., "Post-Quantum Cryptography for Wireless Sensor Network Using Key ...," IntechOpen, 2025.
[84] A. Khan et al., "Federated learning-enabled lightweight intrusion detection system ...," Elsevier, 2025.
[85] C. Wang et al., "Federated learning with LSTM for intrusion detection in IoT-based ...," PeerJ, 2025.
[86] F. Liu et al., "Integrating Blockchain and Machine Learning for Secure Data ...," Wiley, 2025.
[87] R. Singh et al., "Blockchain-Enabled Security and Integrity Mechanisms for Wireless ...," IEEE, 2025.
[88] M. Faris et al., "Security Issues in IoT-Based Wireless Sensor Networks: Classifications and Solutions," MDPI, 2025.
[89] M. Faris et al., "Wireless sensor network security: A recent review based on state-of-the-art works," SAGE, 2023.
[90] M. Sharma et al., "Wireless Sensor Networks: From Fundamentals and Applications to ...," IEEE, 2025.
[91] A. Gupta et al., "A Review on WSN Challenges Focus on Quality of Service, Energy Efficiency, and Security Issues," Springer, 2025.
[92] B. Li et al., "RF-FedAvg: Federated learning-based random forest model for ...," Springer, 2025.
[93] D. Zhang et al., "An Innovative Secure and Privacy-Preserving Federated Learning ...," IEEE, 2024.
[94] I. Ahmad et al., "Intrusion Detection for Wireless Sensor Network Using Particle ...," IEEE, 2025.
[95] N. Gupta et al., "Implementation of novel learning based energy efficient routing ...," Springer, 2025.
[96] R. Kumar et al., "Machine learning solutions for the security of wireless sensor networks: A review," IEEE, 2024.
[97] S. K. Singh et al., "A review on WSN based resource constrained smart IoT systems," Springer, 2025.

[98] D. Zhang et al., "Federated learning in intrusion detection: advancements ...," Springer, 2025.
[99] L. Yang et al., "Federated Learning-Based Intrusion Detection in IoT Networks," MDPI, 2025.
[100] N. Gupta et al., "Intrusion Detection Based on Federated Learning: A Systematic ...," ACM, 2025.
[101] O. Ali et al., "Securing the Future of Wireless Sensor Networks: Challenges, Threats, and Innovative Solutions," IJRASet, 2025.
[102] P. Verma et al., "Security in Wireless Sensor Networks communication protocols: challenges and solutions," ResearchGate, 2018.
[103] Q. Zhao et al., "Blockchain technology for smart wireless sensor networks," Elsevier, 2025.
[104] H. Singh et al., "Adaptability of Blockchain in Wireless Sensor Networks," IEEE, 2025.
[105] W. Samek et al., "Applications of blockchain in internet of things: a survey, actual ...," Springer, 2025.
[106] K. Park et al., "A blockchain-based approach for secure energy-efficient IoT-based ...," Elsevier, 2025.
[107] R. Singh et al., "BS-SCRM: a novel approach to secure wireless sensor networks via ...," Nature, 2024.
[108] A. Gupta et al., "Wireless Sensor Network Security Research and Challenges: A Backdrop," Springer, 2011.
[109] M. Sharma et al., "Security Challenges, Mitigation Strategies, and Future Trends in ...," ACM, 2025.
[110] T. Lee et al., "Quantum and Post-Quantum Security in Future Networks," IEEE, 2025.
[111] U. Patel et al., "Post Quantum Computing Security," 5G Americas, 2025.
[112] V. Nguyen et al., "Industry News 2025 Post Quantum Cryptography A Call to Action," ISACA, 2025.
[113] W. Chen et al., "Quantum Cybersecurity in 2025: Post-Quantum Cryptography Drives ...," IoTWorldToday, 2025.
[114] X. Liu et al., "A Review Study of Wireless Sensor Networks and Its Security," SCIRP, 2015.
[115] Y. Zhang et al., "A Review on WSN Challenges Focus on Quality of Service, Energy Efficiency, and Security Issues," Springer, 2025.
[116] Z. Wang et al., "Securing Wireless Sensor Networks Using BBIDNet and Fuzzy-DQN ...," IEEE, 2025.
[117] NIST, "REPORT ON POST-QUANTUM CRYPTOGRAPHY," WhiteHouse, 2024.
[118] S. Kim et al., "2024-2025 CRA Quad Paper: The Post-Quantum Cryptography ...," CRA, 2025.