International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 10 October-2026 | Impact Factor: 3.5



Blockchain-Based Security for IOT and Wireless Sensor Networks: A Critical Review and Roadmap for Lightweight Intrusion Detection

Mukta Patel[1], Atul Agrawal[2]

[1] Department of Computer Science and Engineering, Oriental University, Indore, India
[2] Department of Computer Science and Engineering, Oriental University, Indore, India

Corresponding Author Email: muktapatel0285@gmail.com

How to Cite this Article:

Patel, M. & Agrawal, A. (2026). Blockchain-Based Security for IOT and Wireless Sensor Networks: A Critical Review and Roadmap for Lightweight Intrusion Detection. International Journal of Creative and Open Research in Engineering and Management, 02(10), 1-9. https://doi.org/10.55041/ijcope.v2i10.175

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.







https://doi.org/10.55041/ijcope.v2i10.175

Abstract—
The Internet of Things (IoT) and wireless sensor networks (WSNs) rely on large numbers of small devices that have limited energy, memory, and computing power and that are exposed to physical and network attacks. Blockchain and machine learning have been proposed as complementary tools for protecting such systems, but their cost and trust assumptions remain debated. This paper presents a focused review of 35 peer-reviewed studies, 32 of them published between 2022 and 2026, on blockchain-based security for IoT and WSNs. The studies are organised into eight themes: reviews and foundations, WSN intrusion detection, recent integrated frameworks, authentication and access control, consensus and scalability, artificial-intelligence-based trust and detection, privacy and federated learning, and post-quantum security. The paper compares representative frameworks and examines one recent two-layer intrusion detection system in detail, covering its design, threat model, reported results, and limits. The review finds that most solutions are evaluated only in simulations or small prototypes, that many depend on a few trusted nodes, that ledger growth and message overhead are seldom measured, that false alarms and detector cost receive little attention, and that attack coverage is narrow. Seven research gaps and six research directions are derived, and a roadmap for a lightweight, fairly evaluated, blockchain-based intrusion detection framework is outlined. The review is intended to help researchers select design options and evaluation practices for secure IoT systems.

Keywords— Blockchain; Internet of Things; wireless sensor networks; intrusion detection; machine learning; lightweight security

I. INTRODUCTION

The Internet of Things (IoT) connects sensors, cameras, wearables, and machines in homes, hospitals, factories, farms, and cities. The rapid growth in the number of such devices, many of which are small, cheap, and energy-limited, has created serious security and privacy problems [1]. A wireless sensor network (WSN) is a common form of IoT network in which low-cost sensor nodes send their readings, often through cluster heads, to a base station. WSNs are used in applications that range from environmental monitoring to precision agriculture and health care [2]. Data in such networks travels over open wireless channels, and the nodes are often placed where an attacker can reach them. A physical attack, in which an adversary takes partial or full control of a node, is among the hardest to detect and can compromise most functions of the network [2]. Conventional protection, such as heavy encryption and detection systems with high overhead, is poorly matched to nodes with limited battery, memory, and processing power [2].

Blockchain is a distributed ledger in which records are grouped into blocks that are linked by cryptographic hashes, so that a later change to a record becomes



detectable without a central authority. Early work proposed blockchain-based architectures for scalable access management of IoT devices [3], and later surveys organised the field by the security problem addressed [4]. Blockchain is, however, not a complete solution. A recent review of 49 studies concluded that scalability, energy use, and privacy remain the main open problems and that most evidence comes from pilots and prototypes [1]. A ledger can show that a record was not altered after it was stored, but it cannot show that the device that produced the record was genuine. It must therefore be combined with device identity checks and safe key storage [1].

Machine learning (ML) is increasingly combined with blockchain to detect attacks and to estimate the trust of devices [5]–[7]. Several frameworks published in 2026 bring blockchain, threat detection, encryption, and trust scoring together [8]–[10], [2]. Although surveys of blockchain-IoT integration exist [4], [1], a critical comparison that places lightweight consensus, AI-assisted detection, privacy, and quantum-safe security side by side, and that looks closely at evaluation practice, is still useful for researchers who must choose among design options.

This paper makes four contributions. First, it classifies 35 studies into eight themes and summarises them in comparative tables. Second, it compares representative recent frameworks and shows why their reported results cannot be compared directly. Third, it analyses one recent two-layer intrusion detection system for WSNs in detail, including its design, threat model, results, and limits. Fourth, it derives seven research gaps and six research directions and outlines a roadmap for a lightweight and fairly evaluated framework. The rest of the paper is organised as follows. Section II reviews the literature by theme. Section III describes the review method. Section IV presents the results, the comparison, the case analysis, and the gaps. Section V concludes the paper.

II. LITERATURE REVIEW

A. Reviews and Foundations

Novo [3] proposed one of the early blockchain-based designs for access management of IoT devices, in which a single management hub is avoided and scalability is addressed. Shammar et al. [4] surveyed research from 2017 to 2021 and grouped it by the security area addressed. Shujaa et al. [1] later reviewed 49 publications and listed scalability, energy use, and privacy as the main open problems. They also advise that blockchain should supplement, and not replace, device identity checks and safe key storage. Liu et al. [11] examined the zero-trust principle, in which no user or device is trusted by default, and its use in IoT, and they point out difficulties such as complex policies, problems of scale, and the effort of fitting zero trust into older systems. Mahdi et al. [12] reviewed lightweight post-quantum cryptography for IoT and stress that such methods must be efficient on resource-limited devices. Together, these reviews agree that blockchain can help IoT security but that cost, privacy, and the lack of real-world evidence are unresolved.

B. Authentication, Access Control, and Identity

Awan et al. [13] combined zero trust, attribute-based access control, blockchain, and IPFS (a system that stores files across many computers) to give access decisions that change with the situation. Nie et al. [14] designed a zero-trust access control scheme for IoT in 6G networks that uses blockchain and inner-product encryption for fine control over who may read protected data. Liu et al. [15] used a sharding blockchain, in which the chain is split into parts that work in parallel, for data sharing across domains in a zero-trust cloud–edge–end setting. Bandara et al. [16] presented Skunk, a platform that joins blockchain, zero trust, and federated learning for 5G and 6G network slicing, although its trust rules are fixed, as noted in [10]. Liu et al. [17] proposed SeCoSe for searchable and secure healthcare service seeking during health record sharing, and Chen et al. [18] built a self-sovereign identity framework, in which users hold their own credentials, for financial institutions. Most of these works are aimed at specific fields such as health care, finance, or mobile networks, so their fit for very small devices is not always clear.

C. Consensus Methods and Scalability

Consensus is the rule by which the nodes of a blockchain agree on the next block. Proof of work is too heavy for most IoT devices, and lighter families assign block creation according to stake, use a small voting group, or rely on node reputation. Voting methods such as Practical Byzantine Fault Tolerance (PBFT) decide quickly in small groups, but their message count grows rapidly with group size. Haque et al. [19] proposed a scalable IoT data management framework with lightweight consensus that, as summarised in [10], lowers the computing work without lowering the security assurance, and a follow-up study improved the performance of IoT data sharing with a refined lightweight algorithm [20]. Raza et al. [21] combined hybrid consensus with ML to strengthen blockchain security, and Liu et al. [22] proposed an enhanced consensus algorithm that targets higher scalability and throughput. As [1] notes, most evidence in this area comes from pilots and prototypes, so behaviour under packet loss and attack needs more testing.



D. AI-Assisted Trust and Threat Detection

Chen et al. [5] built a trust management and defence system for shared vehicle data from blockchain and deep reinforcement learning, an AI method that learns good actions by trial and reward. Qadir et al. [6] applied dynamic Q-learning with blockchain at the network edge to secure IoT data sharing, and Bounaira et al. [23] used deep reinforcement learning for trust management in mobile edge caching, although [10] notes that the computing demand of continuous learning raises concerns about scale. Wang et al. [24] used several kinds of blockchain and AI for layered trust evaluation in 5G intelligent transport, storing decisions as records that are hard to alter. For detection, Wang et al. [7] used hierarchical federated learning to find unusual behaviour in industrial IoT while keeping data private, and Abudalfa and Al-Saleh [25] proposed a convolutional neural network for intrusion detection in IoT networks built on software-defined networking. AI makes trust and detection more flexible but adds computing cost, and in many studies the AI part and the blockchain part are only loosely coupled [10].

E. Privacy and Federated Learning

Wang et al. [26] proposed secure data aggregation at the network edge with blockchain, protecting integrity and confidentiality without a central authority. Tong et al. [27] built a blockchain-based hierarchical federated learning method for IoT networks that use drones, improving scale and trustworthiness. Ferretti et al. [28] examined privacy protection in blockchain-based federated learning systems, and Abuzied et al. [29] proposed a privacy-preserving federated learning framework for blockchain networks. These works show that the model updates and the data can both be protected, but the added computation must still be justified for small devices.

F. Post-Quantum Security

Yuan et al. [30] proposed a post-quantum blockchain architecture for IoT based on NTRU lattice cryptography and showed that adding such methods to a ledger is practical, with a trade-off between security strength and speed. Irshad et al. [31] presented an IoT-enabled cloud architecture for many users that mixes hybrid post-quantum cryptography with blockchain. Because the cost of these tools remains high for small devices [12], one design option is to use them only for rare operations such as registration and logging, as in the framework of [10].

G. Recent Integrated Frameworks

Three frameworks from 2026 combine several tools. Iswarya and Vennila [8] proposed blockchain-assisted authentication with proof of authority, in which a few approved nodes create the blocks, together with AI threat detection. The authors themselves list growth of the ledger, many messages between validators, and dependence on trusted validators as limits. Ahmad et al. [9] joined feature weighting, deep learning, strong encryption, hashing, and permissioned-ledger logging for attack classification in cloud-based sensor systems and reported macro-F1 scores of 0.6837 on HIKARI-2021 and 0.7914 on ADFA-LD. Alsulami [10] proposed Adaptive-AI-ZeroTrust-Chain, in which a reinforcement learning agent keeps a trust score for each device, decisions are logged on a permissioned blockchain, and a lightweight post-quantum module protects the main transactions. The reported accuracy is 98.73% on NSL-KDD and CICIDS2017, and the author clarifies that the ordering service used in the tests tolerates crash faults only, while the security analysis assumes a stronger fault type.

H. Blockchain and ML Intrusion Detection in WSNs

Kim et al. [32] built a blockchain-based trust model in which the trust value of each beacon node, combining behaviour and data, is sent to base stations and stored in a blockchain, and the least trusted node is discarded. Khan et al. [33] used blockchain-based message content validation together with four deep learning models to detect malicious nodes; the authors of [2] note that the best model reached up to 97% detection but added computing load at the cluster head. Ismail et al. [34] proposed a framework for IoT sensor networks that has a blockchain prevention module with light identity and trust management and an ML detection module, in which LightGBM performed best. Jabor et al. [35] had earlier shown that a dedicated circuit can lower the power used by a blockchain in a WSN, and their later two-layer system [2] lets only selected nodes take part in the blockchain. This last system is analysed in detail in Section IV-C.

III. REVIEW METHODOLOGY

A. Scope and Questions

This is a focused narrative review. It addresses four questions. RQ1: which security problems of IoT and WSNs are addressed with blockchain, and which supporting tools are combined with it? RQ2: how are the proposed solutions evaluated? RQ3: which limitations and gaps recur across studies? RQ4: what does a close analysis of one recent two-layer intrusion detection system reveal about design and evaluation practice?

B. Selection of Studies

Studies were identified through targeted web and publisher-platform searches that combined the terms blockchain, IoT, WSN, authentication, access control, consensus, intrusion detection, federated learning, privacy, and post-quantum. A study was included if it was a peer-reviewed journal article or an IEEE



conference paper, if its topic was blockchain-based security of IoT or WSNs or a supporting technique used in such systems, and if complete bibliographic data and a digital object identifier (DOI) could be verified. Recent work (2022–2026) was preferred, and three earlier studies [3], [4], [32] were kept as foundations. The final set contains 35 studies, and 32 of them were published between 2022 and 2026.

C. Extraction and Classification

For each study, the main contribution, the tools used, the evaluation set-up, the reported results, and the limits stated or visible were recorded. Each study was assigned to one of eight themes according to its main contribution. One recent study [2] was read in full and analysed in depth, because it combines blockchain and ML in a lightweight design for WSNs.

D. Limits of the Review

The review is not a systematic review. The selection is purposive and not exhaustive, no formal quality scoring was applied, and the numerical results are reported as given by the original authors and were not reproduced. The conclusions should therefore be read as an informed synthesis and not as a complete census of the field.

IV. RESULTS AND DISCUSSION

A. Overview of the Reviewed Literature

Fig. 1 shows the distribution of the 35 studies. The number of studies rises from 3 in 2022 to 11 in 2024, which shows growing interest in the topic, and the set also contains 4 studies from 2026. By theme, authentication and access control and AI-assisted trust and detection have the most studies (6 each), while post-quantum security has the fewest (2). Table I summarises the themes, the main ideas, and the typical limits that were found.

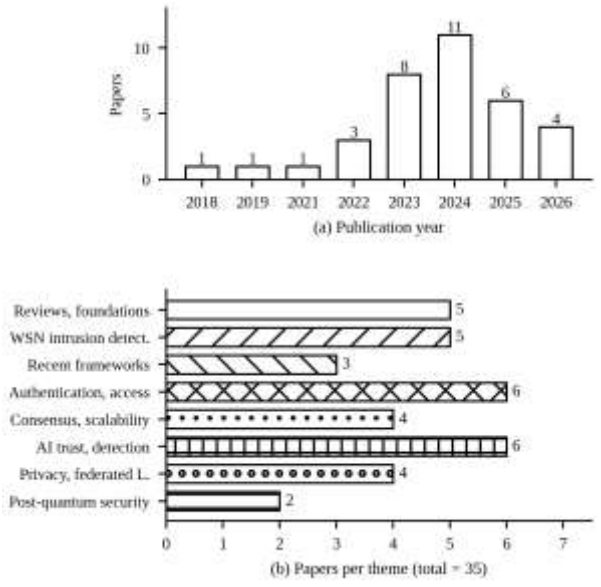


Figure 1: Distribution of the reviewed studies by (a) year and (b) theme.

Table I: Thematic classification of the reviewed studies

Theme	Refs.	Typical focus and limit
Reviews and foundations	[3], [4], [1], [11], [12]	Map the field; open problems are scale, energy, privacy
WSN intrusion detection	[32]–[35], [2]	Blockchain plus trust or ML; load at nodes, trusted base station
Recent frameworks	[8]–[10]	Several tools combined; ledger growth, trusted validators, modest scores
Authentication, access control	[13]–[18]	Fine-grained control; mostly field-specific, fixed trust rules
Consensus, scalability	[19]–[22]	Lighter agreement; mostly pilots and simulations
AI trust, detection	[5], [6], [23], [24], [7], [25]	Adaptive trust and detection; computing cost, loose coupling
Privacy, federated learning	[26]–[29]	Protect data and models; cost for small devices
Post-quantum security	[30], [31]	Quantum-safe ledgers; speed versus strength trade-off

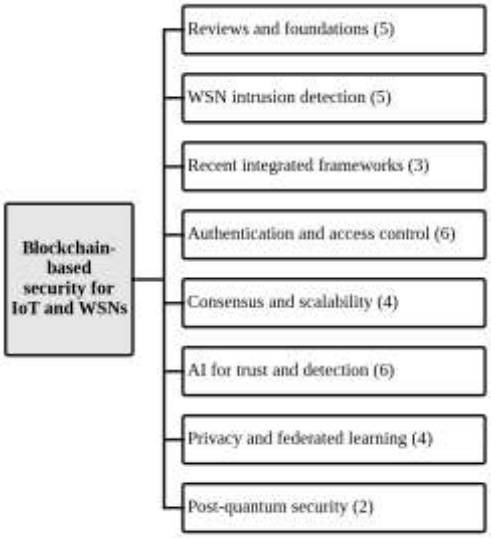


Figure 2: Taxonomy of the reviewed literature (number of studies in brackets).

B. Comparative Analysis of Representative Frameworks

Table II compares representative frameworks from 2023 to 2026. Two observations follow. First, the frameworks differ in task, data, and metric. Accuracy of 97.42% in a 100-node WSN simulation [2], accuracy of 98.73% on NSL-KDD and CICIDS2017 [10], and macro-F1 scores of 0.6837 and 0.7914 on HIKARI-2021 and ADFA-LD [9] describe different problems, so they cannot be ranked against one another. Second, the limits that the authors state are similar across the table: a dependence on trusted nodes, growth of the ledger or of the messages, or an evaluation in simulation or on a small testbed. Fair comparison therefore needs a common set-up, a common data set, and common metrics.



Table II: Comparison of selected recent frameworks (as reported by the authors)

Ref.	Year	Main tools	Reported result or stated limit
[2]	2026	Chaotic-hash blockchain among cluster heads and base station; ANN at base station	97.42% accuracy, 98.35% recall (100-node simulation); trusted base station, two attack types
[8]	2026	Proof of authority; AI threat detection	Limits: ledger growth, validator messages, trusted validators
[9]	2026	Feature weighting; deep learning; AES-256-GCM; ledger logging	Macro-F1 0.6837 (HIKARI-2021), 0.7914 (ADFA-LD)
[10]	2026	Reinforcement-learning trust score; permissioned chain; post-quantum module	98.73% accuracy; crash-fault ordering service only
[34]	2024	Light identity and trust management; LightGBM detector	Blockchain complexity and ML load remain, as noted in [2]
[33]	2023	Message content validation; four deep learning models	Up to 97% detection; extra load at cluster head, as noted in [2]
[13]	2023	Zero trust; attribute-based access control; IPFS	Dynamic access decisions on blockchain

C. Case Analysis: A Two-Layer Blockchain and ML Intrusion Detection System

The study of Jabor et al. [2] deals with physical attacks on a WSN. Only the cluster heads and the base station take part in the blockchain, and ordinary sensor nodes stay outside it to save energy. Each sensor node compresses and encrypts its readings with compressed sensing and a chaotic map, and the cluster head groups the data into a block with a time stamp and a chaotic hash of the previous block. As Fig. 3 shows, the base station checks each block in two layers. In Layer 1, a hash that does not match the expected value marks the block as tampered. In Layer 2, an artificial neural network (ANN) uses 576 input values (512 data values, 32 hash values, and 32 previous-hash values) to find forged data that passed Layer 1. All heavy work is done at the base station, which has mains power.

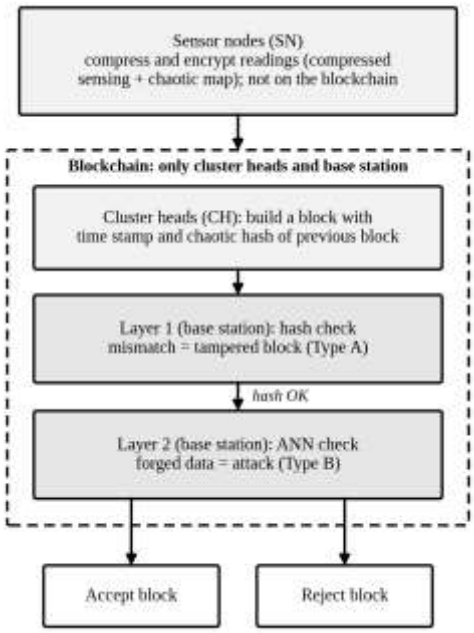


Figure 3: Two-layer intrusion detection system of the case study [2].

The threat model assumes a fully trusted base station and an honest majority of cluster heads. In a Type A attack, the attacker cannot compute a valid hash, so Layer 1 catches the block. In a Type B attack, the attacker controls a node and all its keys, adds small random noise to the data, and creates a valid hash, so only the ANN can catch the block. The authors simulated a 100-node WSN in a 100 m × 100 m area with the LEACH clustering protocol and used five-fold stratified cross-validation with oversampling for class balance. Table III shows that the blockchain layer alone has perfect precision but finds only 43.25% of the attacks, the ANN alone finds 97.50%, and the combination gives the best result. The paper also reports detection above 99.98% with 30 simultaneous attackers, a packet delivery ratio of about 96% at 10% packet loss, and a network energy overhead below 0.70% per round.

Table III: Results of the case study for each detection layer (in %) [2]

Method	Acc.	Prec.	Recall	F1
Blockchain layer only	88.34	100.00	43.25	60.38
ANN only	96.72	87.87	97.50	92.43
Combined	97.42	90.03	98.35	94.00

The authors state several limits: an idealised radio model, uniformly random node placement, a single clustering protocol, two attack types only, training on simulated data, and chaotic parameters that are sent with the data and could be intercepted. Our reading adds five points. (1) Block checking and agreement happen at one fully trusted base station, so the whole system fails if this station fails or is compromised. (2) In the paper's confusion matrix, 460 of 10,535 normal blocks (about 4.4%) were flagged wrongly, while 24 attack blocks were missed. (3) The ANN has 374,914 parameters and needs 37.55 ms per block, whereas random forest and gradient boosting reach 97.06% and 96.83% accuracy with much shorter inference time in the paper's own comparison. (4) Data protection relies on chaotic maps, which are not a standard method, and compressed sensing gives no check of authenticity, as the authors admit. (5) The inference times of the comparison models differ between two tables of the paper, and the combined-system results are given without standard deviation. These points do not reduce the value of the work. They show where careful follow-up work can add most.

D. Cross-Cutting Challenges and Research Gaps

Seven gaps recur across the reviewed studies, and they are listed in Table IV together with the matching research directions. Heavy tools for small devices [12], dependence on trusted nodes [8], [2], and growth of the ledger and of network messages [8] appear in both the general frameworks and the WSN systems. The gaps of false alarms and detector cost, narrow attack



coverage, and data protection without authenticity are clearest in the case study [2], while the gap of limited and simulated testing is stressed in recent reviews and frameworks [1], [8].

Table IV: Research gaps and directions

No.	Research gap	Research direction
1	Heavy tools for small devices [12]	Keep work on nodes minimal; use heavy tools only for rare steps
2	Dependence on trusted nodes [8], [2]	Shared block checking by several rotating nodes
3	False alarms and detector cost [2]	Lighter detectors; threshold tuning; report false alarm rate
4	Narrow attack coverage [2]	Add replay, selective forwarding, coordinated attacks
5	No authenticity in data protection [2]	Standard lightweight authenticated encryption
6	Limited, simulated testing [1], [8]	Realistic channels, other protocols, public data sets
7	Growth of chain and messages [8]	Summarise old blocks; measure storage and messages

E. Design Implications

The reviewed studies suggest several practical design principles for small devices. First, ordinary sensor nodes can stay outside the blockchain, with heavier work moved to a base station or a gateway [2], [35]. Second, large data can be kept in an off-chain store such as IPFS [13], while compact records stay on the chain. Third, costly tools such as post-quantum cryptography are better reserved for rare steps such as registration and logging [10], because their cost is high for small devices [12]. Fourth, blockchain should be combined with device identity checks and safe key storage [1]. Fifth, lightweight consensus with a small or rotating validator group reduces cost [19], [22], but it should be tested under packet loss and attack [1]. Sixth, detection results should be reported with false alarm rate and cost, and not with accuracy alone.

F. Research Directions and Roadmap

The gaps lead to six improvements for a lightweight intrusion detection framework, which are shown in Fig. 4. I-1: shared block checking, in which the base station and a few rotating cluster heads check each block and vote. I-2: a lighter detector, in which ensemble models and a tuned decision threshold are compared with the ANN. I-3: new attack types in the simulator, namely replay, selective forwarding, and coordinated attacks, which the authors of the case study also name as future work [2]. I-4: standard lightweight authenticated encryption between sensor nodes and cluster heads. I-5: tests with realistic channels, other node placements, packet loss, and a public data set. I-6: summaries of old blocks, so that only recent blocks are kept at the cluster heads.

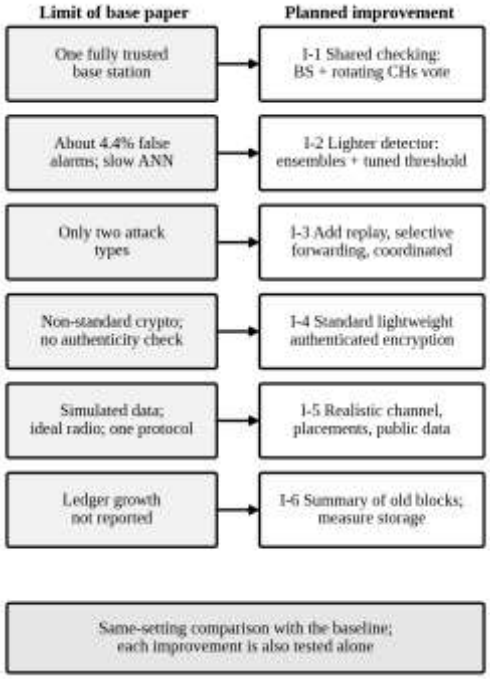


Figure 4: Limits of the case study and the planned improvements.

Four evaluation practices follow from the review. First, a baseline should be rebuilt and re-measured in the same set-up as the improved system. Second, results should be given with standard deviations and, where possible, per attack type. Third, false alarm rate, inference time, energy, communication overhead, and storage growth should be reported together with accuracy and recall. Fourth, each improvement should be switched on and off separately, so that its own effect is visible. These practices would make future results easier to compare and to trust.

V. CONCLUSION

This paper reviewed 35 studies on blockchain-based security for IoT and WSNs and organised them into eight themes. The studies show that blockchain, ML, and light cryptography can be combined to protect small devices, and the most recent frameworks bring several tools together. The review also shows that results are often hard to compare, that many designs rely on a few trusted nodes, and that ledger growth, false alarms, detector cost, and attack coverage receive too little attention. A close analysis of a recent two-layer intrusion detection system showed strong results in simulation but also a dependence on one fully trusted base station, a false alarm rate of about 4.4% in the reported matrix, a non-standard data protection method, and a narrow attack set. Seven gaps and six research directions were derived. Future work will rebuild the analysed system, add the proposed improvements, and compare the result with the baseline under the same conditions.



REFERENCES

[1] W. Shujaa, M. Alanzi, and S. Sankaranarayanan, "Enhancing IoT security through blockchain integration," *Front. Comput. Sci.*, vol. 7, Art. no. 1670473, Oct. 2025, doi: 10.3389/fcomp.2025.1670473.

[2] M. S. Jabor, A. S. Azez, J. C. Campelo, and A. Bonastre, "A lightweight IDS based on blockchain and machine learning for detecting physical attacks in wireless sensor networks," *Sensors*, vol. 26, no. 6, Art. no. 1961, 2026, doi: 10.3390/s26061961.

[3] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[4] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A survey of IoT and blockchain integration: Security perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021, doi: 10.1109/ACCESS.2021.3129697.

[5] J. Chen *et al.*, "Design of a dynamic trust management and defense decision system for shared vehicle data based on blockchain and deep reinforcement learning," *Sci. Rep.*, vol. 15, Art. no. 26662, 2025, doi: 10.1038/s41598-025-11511-y.

[6] J. Qadir, S. Hassan, I. Ali, F. Riaz, and M. Guizani, "Enhancing secure IoT data sharing through dynamic Q-learning and blockchain at the edge," *Sci. Rep.*, vol. 15, Art. no. 39521, 2025, doi: 10.1038/s41598-025-24510-w.

[7] X. Wang *et al.*, "Toward accurate anomaly detection in industrial Internet of Things using hierarchical federated learning," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7110–7119, 2022, doi: 10.1109/JIOT.2021.3074382.

[8] G. Iswarya and C. Vennila, "A secure and scalable blockchain-assisted authentication framework for decentralized IoT data management," *Sci. Rep.*, vol. 16, Art. no. 16359, 2026, doi: 10.1038/s41598-026-47192-4.

[9] N. Ahmad, Y. Cao, and W. Liu, "A blockchain-enabled security framework for cloud-based sensor systems with deep learning-driven attack classification," *Sensors*, vol. 26, no. 16, Art. no. 5198, 2026, doi: 10.3390/s26165198.

[10]F. N. Alsulami, "Adaptive-AI-ZeroTrust-Chain: Blockchain-backed dynamic zero-trust enforcement via artificial intelligence," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 38, no. 5, Art. no. 262, 2026, doi: 10.1007/s44443-026-00622-9.

[11]C. Liu *et al.*, "Dissecting zero trust: Research landscape and its implementation in IoT," *Cybersecurity*, vol. 7, no. 1, Art. no. 20, 2024, doi: 10.1186/s42400-024-00212-0.

[12]L. H. Mahdi, Z. A. Hussien, and M. A. Mahmood, "Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 2, pp. 21812–21821, 2025, doi: 10.48084/etasr.10141.

[13]S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A blockchain-inspired attribute-based zero-trust access control model for IoT," *Information*, vol. 14, no. 2, Art. no. 129, 2023, doi: 10.3390/info14020129.

[14]S. Nie, J. Ren, R. Wu, P. Han, Y. Zhang, and Y. Xiang, "Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment," *Sensors*, vol. 25, no. 2, Art. no. 550, 2025, doi: 10.3390/s25020550.

[15]Y. Liu *et al.*, "Secure and scalable cross-domain data sharing in zero-trust cloud–edge–end environment based on sharding blockchain," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 4, pp. 2603–2618, 2023, doi: 10.1109/TDSC.2023.3313799.

[16]E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and W. K. Ng, "Skunk – A blockchain and zero trust security enabled federated learning platform for 5G/6G network slicing," in *Proc. IEEE Int. Conf. Sens., Commun. Netw. (SECON)*, 2022, pp. 1–9, doi: 10.1109/SECON55815.2022.9918536.

[17]Z. Liu, L. Hu, Z. Cai, X. Liu, and Y. Liu, "SeCoSe: Toward searchable and communicable healthcare service seeking in flexible and secure EHR sharing," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4999–5014, 2024, doi: 10.1109/TIFS.2024.3391914.

[18]Y.-H. Chen, H.-L. Liu, and M.-E. Wu, "A self-sovereign identity blockchain framework for access control and transparency in financial institutions," *Cryptography*, vol. 9, no. 1, Art. no. 9, 2025, doi: 10.3390/cryptography9010009.

[19]E. U. Haque *et al.*, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Sci. Rep.*, vol. 14, Art. no. 7841, 2024, doi: 10.1038/s41598-024-58578-7.

[20]E. U. Haque *et al.*, "Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm," *Sci. Rep.*, vol. 14, Art. no. 26561, 2024, doi: 10.1038/s41598-024-77706-x.

[21]M. S. Raza, U. Qamar, S. Ibrahim, and M. Kashif, "Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques," *Sci. Rep.*, vol. 14, Art. no. 1149, 2024, doi: 10.1038/s41598-024-51578-7.

[22]X. Liu, Y. Wang, K. Chen, Z. Liu, and J. Zhang, "An enhanced consensus algorithm for blockchain," *Sci. Rep.*, vol. 14, Art. no. 19976, 2024, doi: 10.1038/s41598-024-68120-4.

[23]S. Bounaira, R. Oucheikh, H. Tabbaa, and B. Belmekki, "Blockchain-enabled trust management for secure content caching in mobile edge computing using deep reinforcement learning," *Internet Things*, vol. 25, Art. no. 101076, 2024, doi: 10.1016/j.iot.2024.101076.

[24]X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. M. Hassan, "Heterogeneous blockchain and AI-driven hierarchical trust evaluation for 5G-enabled intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2074–2083, 2023, doi: 10.1109/TITS.2021.3129417.

[25]S. I. Abudalfa and Y. A. Al-Saleh, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," *Information*, vol. 14, no. 1, Art. no. 41, 2023, doi: 10.3390/info14010041.

[26]X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. Hossain, "A secure data aggregation strategy in edge computing and blockchain-empowered Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14237–14246, 2022, doi: 10.1109/JIOT.2020.3023588.

[27]Z. Tong, J. Wang, X. Hou, J. Chen, Z. Jiao, and J. Liu, "Blockchain-based trustworthy and efficient hierarchical federated learning for UAV-enabled IoT networks," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34270–34282, 2024, doi: 10.1109/JIOT.2024.3370964.

[28]S. Ferretti *et al.*, "Privacy-preserving in blockchain-based federated learning systems," *Comput. Commun.*, vol. 222, pp. 38–67, 2024, doi: 10.1016/j.comcom.2024.04.024.

[29]Y. Abuzied, M. Ghanem, F. Dawoud, and A. El-Mahdy, "A privacy-preserving federated learning framework for blockchain networks," *Cluster Comput.*,



vol. 27, pp. 3997–4014, 2024, doi: 10.1007/s10586-024-04273-1.

[30]B. Yuan, F. Wu, and Z. Zheng, "Post quantum blockchain architecture for Internet of Things over NTRU lattice," *PLoS ONE*, vol. 18, no. 2, Art. no. e0279429, 2023, doi: 10.1371/journal.pone.0279429.

[31]R. R. Irshad *et al.*, "IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing," *IEEE Access*, vol. 11, pp. 105479–105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[32]T.-H. Kim *et al.*, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019, doi: 10.1109/ACCESS.2019.2960609.

[33]Z. A. Khan, S. Amjad, F. Ahmed, A. M. Almasoud, M. Imran, and N. Javaid, "A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks," *IEEE Access*, vol. 11, pp. 31036–31051, 2023, doi: 10.1109/ACCESS.2023.3259982.

[34]S. Ismail, M. Nouman, D. W. Dawoud, and H. Reza, "Towards a lightweight security framework using blockchain and machine learning," *Blockchain: Res. Appl.*, vol. 5, Art. no. 100174, 2024, doi: 10.1016/j.bcra.2023.100174.

[35]M. S. Jabor, A. S. Azez, J. C. Campelo, and A. Bonastre Pina, "New approach to improve power consumption associated with blockchain in WSNs," *PLoS ONE*, vol. 18, Art. no. e0285924, 2023, doi: 10.1371/journal.pone.0285924.