SSR Journal of Artificial Intelligence (SSRJAI)

OPEN ACCESS

Homepage: https://ssrpublisher.com/ssrjai/

Volume 3, Issue 7, 2026 ISSN: 3049-0413

# AI-Driven Intrusion Detection for the Internet of Things: A Scoping Review of Federated Learning, Privacy-Preserving Architectures, and Edge Deployability

Gilbert Imuetinyan Osaze Aimufua & Godwin Agbonkhese*

Department of Cyberspace Studies, Nasarawa State University, PMB 1022, Keffi, Nasarawa State, Nigeria

***Received:*** *05.06.2026* | ***Accepted:*** *23.07.2026* | ***Published:*** *26.07.2026*

***Corresponding author:** Godwin Agbonkhese

**DOI:** *10.5281/zenodo.21590977*

**Abstract** **Review Article**

Federated learning has emerged as the dominant architectural response to the privacy and communication constraints of centralised intrusion detection in Internet of Things environments, yet the field lacks a synthesis that maps the concurrent state of architecture diversity, privacy-preservation rigour, and edge deployability. This scoping review synthesises 99 empirical studies published between 2020 and 2026, drawn from two thematic extraction categories: federated learning-based intrusion detection for Internet of Things networks (61 studies) and deep learning-based intrusion detection with blockchain-enabled tamper-proof logging (43 studies, one shared). Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for scoping reviews, the review maps twelve confirmed architecture families, a twelve-branch privacy mechanism taxonomy, and classifies all included studies by edge evaluation type. Three gap clusters are identified. An empirical gap in deployment evaluation is the most operationally consequential: 88 per cent of included studies evaluate on server simulation only, and the study that quantifies the cost of this deferral reports a 36.5 percentage-point accuracy degradation on real-world imbalanced data. A practical-knowledge and evidence gap in privacy claims separates formal guarantees from predominant practice: 41 of 61 federated learning studies assert privacy through the federated paradigm alone, without differential privacy, homomorphic encryption, or secure aggregation. A methodological gap in evaluation reproducibility arises from incomplete federated learning configuration reporting, persistent reliance on a 2009 benchmark dataset, and unnamed datasets in recent papers. The findings provide a structured evidence base for primary research that targets these gaps.

**Keywords:** Edge deployment; Federated learning; Internet of Things; Intrusion detection systems; Privacy-preserving machine learning; Scoping review.

Copyright © 2026 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

## 1. Introduction

The Internet of Things (IoT) has expanded from an architectural concept to a global infrastructure of approximately 18 billion connected devices across industrial control systems, healthcare monitoring, vehicular networks, smart grids, and consumer environments (Anjum et al., 2025; Koroniotis et al., 2024; Devi et al., 2025). This scale has transformed the IoT attack surface into one of the most consequential security problems in contemporary computing. Distributed denial-of-service campaigns launched from compromised IoT botnets have shown the

capacity to disrupt critical infrastructure (Beshah et al., 2025; Kumar et al., 2021); data injection attacks on industrial IoT sensors have targeted operational safety systems (Tran et al., 2023; Vargas et al., 2021); and reconnaissance attacks against IoT deployments are routinely observed in healthcare, vehicular, and smart city contexts (Bhavsar et al., 2024; Liu et al., 2021; Gebresilassie et al., 2025). The detection of these threats at the network layer, before they propagate to application or physical systems, is the problem that IoT intrusion detection systems (IDS) are designed to address.

Machine learning (ML) and deep learning (DL) methods have become the dominant approach to IoT IDS; high detection accuracy on controlled benchmarks is widely reported (Soomro et al., 2024; Chaurasia et al., 2024; Lekssays et al., 2021; Ullah et al., 2025; Srinivasan and Senthilkumar, 2025; Manzano et al., 2025). The established approach trains a centralised model on aggregated network traffic data and deploys it for inference at the network perimeter or on a monitoring server. In IoT environments, however, centralised training is constrained by three structural problems. First, IoT traffic data frequently contains sensitive device-level or user-level information; transmitting raw traffic logs to a central server for training creates a data privacy risk that is both a regulatory concern and a practical attack surface (Ruzafa-Alcázar et al., 2023; Islam et al., 2025). Second, the communication overhead of transmitting high-volume traffic data from thousands of constrained IoT devices to a central training server is prohibitive under typical IoT network conditions (Issa et al., 2026; Al Tfaily et al., 2025). Third, IoT deployments are characterised by severe data heterogeneity: traffic distributions vary across device types, manufacturers, firmware versions, and deployment contexts in ways that a single centralised model trained on pooled data cannot adequately capture (Mhawish et al., 2026; Mukisa et al., 2025; Luo et al., 2025).

Federated learning (FL) (McMahan et al., 2017) addresses these three constraints by training the global detection model across distributed IoT nodes without transmitting raw data to a central server. Each participating device trains a local model on its own traffic data and transmits only model updates to a central aggregation server, which combines them via McMahan et al. (2017) or a variant into a global model redistributed to clients. Research activity in FL-based IoT IDS has accelerated substantially since 2022. Architecture diversity has expanded from CNN and LSTM variants to graph neural networks (Al Tfaily et al., 2025; Liu et al., 2021), knowledge distillation chains (Ma et al., 2025; Peng et al., 2025), Vision Ma et al. (2025), and LLM-integrated models (AlHayan and Al-Muhtadi, 2026). Aggregation algorithms have proliferated to address non-IID data heterogeneity (Mhawish et al., 2026; Mukisa et al., 2025), adversarial robustness (Sanjalawe et al., 2025; Ullah et al., 2026), communication overhead (Alqazzaz, 2025a; Issa et al., 2026), and client trust management (Alabdulatif, 2025; Nakayiza et al., 2026). A parallel literature has coupled FL with blockchain to provide tamper-proof logging of model updates and detection outcomes (Lilhore et al., 2026; Ibrahim et al., 2026a,b; Alharthi et al., 2025; Luo et al., 2025; Khonde and Ulagamuthalvi, 2022; Arazzi et al., 2023; Swarnalatha et al., 2026).

Privacy preservation within this literature takes three distinct forms. The majority of FL-IDS papers treat the federated paradigm itself as the privacy mechanism; the absence of raw data sharing is taken as equivalent to privacy preservation. A smaller group applies formal differential privacy (Ruzafa-Alcázar et al., 2023; Danquah et al., 2025; Islam et al., 2025; Praveen et al., 2025; Ullah et al., 2026) or homomorphic encryption (Alqazzaz, 2025b; Nakayiza et al., 2026; Arazzi et al., 2023) to bound information leakage from gradient updates. The DL-Blockchain category uses blockchain consensus and immutable ledgers as the primary integrity mechanism (Sengan et al., 2026; Parashar et al., 2026; Alkhonaini et al., 2025; Gebresilassie et al., 2025; Srinivasan and Senthilkumar, 2025; Vargas et al., 2021; Khraisat et al., 2025a; Manzano et al., 2025; Ullah et al., 2025). These three approaches address different threat models and produce results that are difficult to compare directly.

Edge deployability is the third dimension of the problem. An FL-IDS that achieves high accuracy in server simulation but cannot execute inference

within the memory and latency budget of a constrained IoT device is not deployable. Constrained-hardware evaluations are rare across the combined landscape (Chen et al., 2020; Huong et al., 2022; Bhavsar et al., 2024; Al Mazroa, 2025; Albanbay et al., 2025), and the study that most directly measures the cost of deferring this step reports a 36.5 percentage-point accuracy degradation on real-world imbalanced data (Ranpara et al., 2025).

Despite the volume of primary research across these three dimensions, no prior review has mapped their intersection concurrently. Using the research gap taxonomy of Miles (2017), this review identifies three gap clusters: an empirical gap in deployment evaluation, a practical-knowledge and evidence gap in privacy claims, and a methodological gap in evaluation reproducibility.

This paper presents a scoping review of AI-driven intrusion detection for IoT, following the framework of Arksey and O'Malley (2005) as extended by Levac et al. (2010), and reported per Tricco et al. (2018). The review synthesises 99 included studies across two thematic extraction categories. The remainder of the paper is organised as follows. Section 2 describes the review methodology. Section 3 reports findings by research question. Section 4 characterises the three gap clusters and states the review's limitations. Section 5 draws conclusions and identifies directions for primary research.

## 2. Methods

### 2.1 Review Design and Protocol Registration

This study was conducted as a scoping review following the methodological framework of Arksey and O'Malley (2005), as extended by Levac et al. (2010). Reporting conforms to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for scoping reviews (PRISMA-ScR) (Tricco et al., 2018). The scoping design was selected over a systematic review with meta-analysis for three reasons. First, the review spans three methodologically distinct sub-literatures (federated learning for IoT intrusion detection, blockchain-enabled tamper-proof logging, and edge-deployable AI security systems), and their concurrent coverage requires a breadth of scope that a narrow PICO question cannot accommodate. Second, the included studies report detection performance across incompatible metrics and benchmarks; meta-analytic pooling across this heterogeneity is not methodologically defensible. Third, the sub-field has been active for approximately six years; the scoping review is therefore the appropriate instrument to map what exists, characterise what is missing, and direct the design of future primary studies.

A protocol was prepared prior to data extraction covering the Population–Concept–Context (PCC) framework, research questions, corpus architecture, eligibility criteria, search strategy, screening procedure, extraction framework, and synthesis themes. The protocol is available from the corresponding author on reasonable request.

### 2.2 PCC Framework and Research Questions

The Population–Concept–Context (PCC) framework was adopted in place of PICO, per PRISMA-ScR convention for scoping reviews (Tricco et al., 2018). The population is defined as IoT devices and networks (industrial IoT (IIoT), vehicular IoT (IoV), smart grid systems, healthcare IoT, smart cities, wireless sensor networks, and connected consumer devices) in which intrusion or anomaly detection is the security objective. The concept covers AI-driven intrusion detection systems incorporating at least one of three features: federated learning as the training or inference paradigm; privacy-preserving mechanisms targeting data or gradient confidentiality, including differential privacy, homomorphic encryption, secure aggregation, or blockchain-based tamper-proof logging; or edge deployment as an explicit design objective or evaluation target. The context is peer-reviewed empirical research published between 2020 and 2026 in which the IoT environment is the primary deployment setting and intrusion or anomaly detection is the primary security task.

Four research questions (RQs) were derived from the PCC framework:

- **RQ1:** What AI and deep learning architectures are employed for IoT intrusion detection within federated learning frameworks, and what detection performance do they achieve across reported metrics and datasets?
- **RQ2:** How are privacy-preservation requirements addressed in AI-driven IoT IDS across the spectrum from structural FL claims through formal differential privacy, homomorphic encryption, secure aggregation, and blockchain-based auditability, and how rigorously is privacy evaluated?
- **RQ3:** To what extent do included studies evaluate AI-driven IoT IDS under hardware-realistic edge conditions, and what is the gap between claimed and demonstrated deployability?
- **RQ4:** What IoT application domains and threat classes are addressed by the included literature, and what methodological gaps in evaluation rigour, reproducibility, and deployment realism are unresolved?

### 2.3 Corpus Architecture and Source Corpora

The evidence base for this review is organised into two thematic extraction categories that cover complementary dimensions of the literature. The first category addresses federated learning architectures for IoT threat detection; it draws on seven databases (IEEE Xplore, Springer Link, ScienceDirect, PubMed, Frontiers, Scientific Reports, and ACM) over 2020–2026 and includes 61 papers after PRISMA 2020 screening. The second category addresses deep learning-based intrusion detection with blockchain-enabled tamper-proof logging; it draws on six databases (IEEE Xplore, Springer Link, ScienceDirect, PubMed, Frontiers, and ACM) over 2021–2026 and includes 43 papers.

Three conditions justify this pre-extraction corpus architecture:

1. Both extraction categories follow PRISMA 2020 screening and extraction protocols with documented, reproducible eligibility criteria and search strings.
2. Both categories address the same population (IoT security environments) and overlapping concepts (AI-driven IDS, privacy mechanisms, and edge deployment); cross-category synthesis is therefore methodologically coherent.
3. The breadth of the scoping research questions exceeds what either category covers individually, and the combined corpus provides the evidence base required to address all four RQs.

Table 1: Inclusion and Exclusion Criteria

| Dimension | Inclusion | Exclusion |
|---|---|---|
| **Population** | IoT or IIoT networks as the primary deployment environment (industrial, vehicular, smart grid, healthcare, smart city, WSN, 5G/6G-enabled IoT, consumer devices) | Single-device or non-IoT environments (enterprise LAN, general cloud) where IoT context is absent |
| **AI/ML concept** | At least one ML or DL method applied to intrusion, anomaly, or threat detection as the primary security task | FL for non-security tasks only; non-FL distributed learning without a named privacy |

| Dimension | Inclusion | Exclusion |
|---|---|---|
| | | mechanism |
| **FL or privacy concept** | At least one of: FL as the training paradigm; a named privacy mechanism (DP, HE, secure aggregation, blockchain); edge deployment as an explicit design or evaluation objective | Papers in which neither FL nor a named privacy mechanism nor an edge deployment objective is present |
| **Outcome** | At least one quantitative detection metric reported (accuracy, F1-score, precision, recall, AUC-ROC, FPR, or equivalent) | Purely conceptual or architectural papers with no quantitative evaluation |
| **Study design** | Original empirical study with experimental evaluation; peer-reviewed journal or conference paper | Surveys, meta-analyses, scoping reviews, editorials, grey literature, preprints without peer-reviewed publication |
| **Language** | English | Non-English |
| **Date** | 2020–2026 inclusive | Pre-2020 or post-June 2026 |

*DP: differential privacy; HE: homomorphic encryption; WSN: wireless sensor network; FPR: false positive rate.*

### 2.4 Eligibility Criteria

Eligibility was determined against pre-specified inclusion and exclusion criteria, presented in Table 1. Seven dimensions were assessed at screening: population, AI/ML concept, FL or privacy concept, outcome reporting, study design, language, date range, and publication type. Studies were included only when all inclusion criteria were met and no exclusion criterion applied.

### 2.5 Search Strategy

Each extraction category was searched independently using structured Boolean queries across multiple databases. The first category combined four concept blocks: federated learning variants; IoT and IIoT environment terms; intrusion, anomaly, and threat detection terms; and privacy and security terms. The search covered IEEE Xplore, Springer Link, ScienceDirect, PubMed, Frontiers, Scientific Reports, and ACM, and was conducted in July 2026. The second category combined three concept blocks: deep learning and machine learning variants; blockchain and tamper-proof logging terms; and IoT intrusion detection and security terms. The search covered IEEE Xplore, Springer Link, ScienceDirect, PubMed, Frontiers, and ACM, and was conducted over 2025–2026. Full search strings for both categories are preserved in the respective extraction archives and are available from the corresponding author on reasonable request.

A supplementary intersection search targeting papers at the junction of all three title pillars was

not conducted within the submission timeline. The two extraction categories are considered sufficient to address all four RQs, and this deviation is documented in the protocol deviations log.

### 2.6 Screening and Harmonisation Procedure

Papers appearing in both extraction categories were identified by DOI matching. Where a duplicate was found, the extraction record from the category in which the paper was a primary inclusion was retained. Source corpus papers were admitted to the synthesis without re-screening, as each had already passed full-text eligibility assessment in its respective extraction process.

Harmonisation was applied to reconcile the partially overlapping eligibility criteria of the two extraction categories. Two adjustments were made:

1. Papers that did not satisfy the broader PCC scope of this review (addressing non-IoT network environments) were excluded at harmonisation and documented in the PRISMA-ScR flow.
2. Papers coded as Weak quality in either category were retained in the synthesis but restricted to gap analysis and pattern-level claims; they were not cited for specific performance figures.

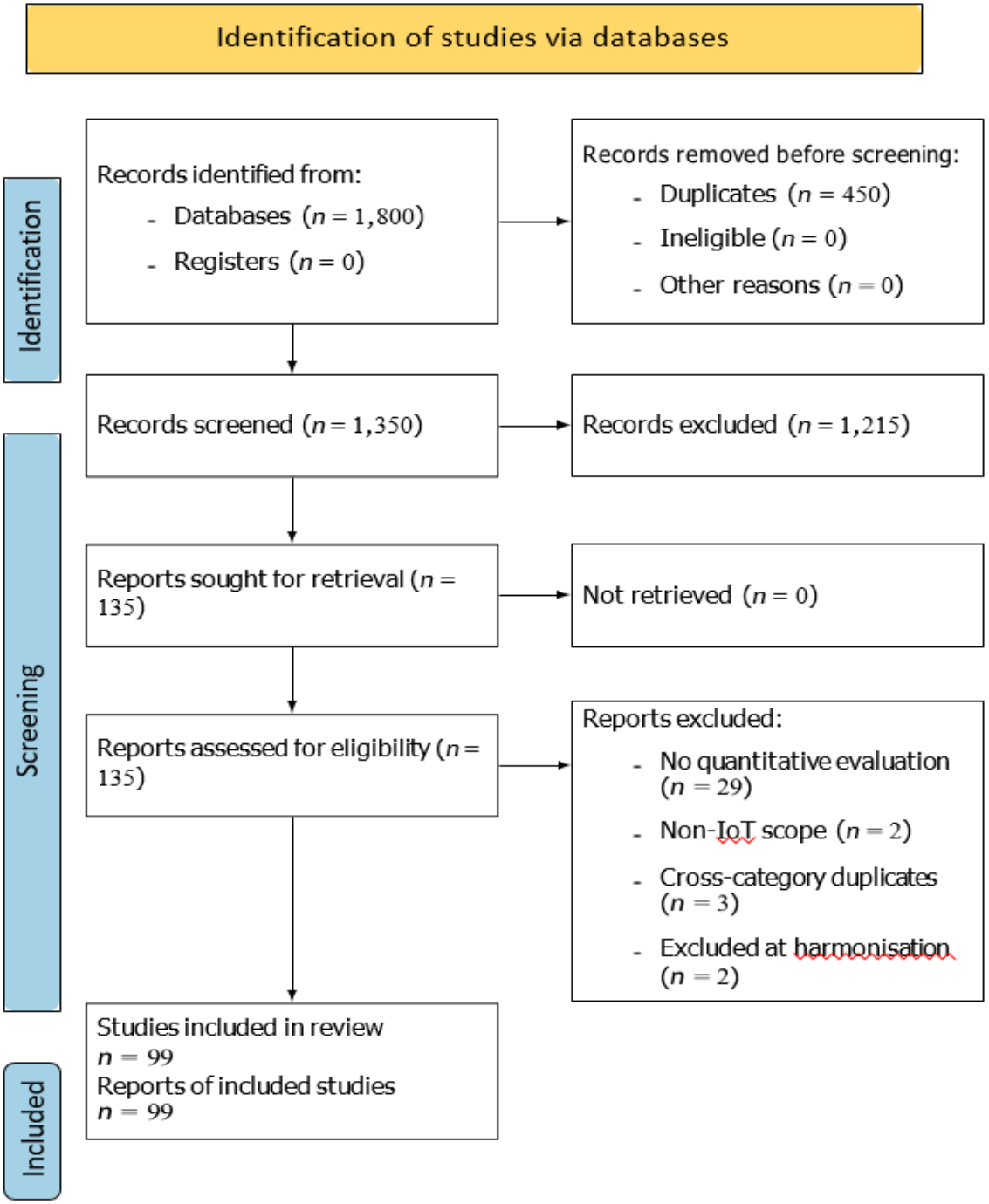
### 2.7 Data Extraction and Synthesis Approach

Extraction data were drawn directly from the two source corpus extraction files; no re-extraction from primary papers was conducted. Sixteen fields were mapped from source extraction records to a unified synthesis framework, covering study identification, bibliographic metadata, IoT domain, AI architecture family, FL aggregation algorithm, FL client count, privacy mechanism and rigour classification, edge evaluation type, hardware platform, primary dataset, detection metrics, best reported performance, quality rating, and borderline code. Quality was assessed using a three-tier rubric applied consistently across both extraction categories. Strong papers provide tabulated, extractable quantitative results with FL configuration fully reported, dataset clearly identified, and privacy mechanism evaluated rather than merely described. Adequate papers satisfy these criteria partially, with results tabulated but incomplete or with FL configuration only partially reported. Weak papers present no extractable quantitative results, with FL not empirically implemented, dataset unnamed or non-IoT, or privacy mechanism purely conceptual. Quality ratings governed synthesis weighting: Strong papers were cited for specific performance figures; Adequate papers for architecture and pattern claims; Weak papers for gap analysis only.

Synthesis was organised around four pre-defined themes corresponding to the four RQs. Theme 1 maps AI architecture families and aggregation algorithms and characterises detection performance envelopes by dataset. Theme 2 classifies privacy mechanisms across a twelve-branch taxonomy for the FL-IoT category and a blockchain-as-auditability taxonomy for the DL-Blockchain category, with formal and claimed-only privacy evaluated separately. Theme 3 classifies all papers by edge evaluation type and maps hardware evidence to platform. Theme 4 characterises IoT domain coverage and threat class distribution across the combined corpus.

## 3. Results

The screening and harmonisation procedure yielded 99 studies for inclusion in the final synthesis. Figure 1 presents the PRISMA-ScR flow diagram detailing identification, screening, and inclusion at each stage. Characteristics of all included studies are summarised in Table 2, organised by extraction category, AI architecture family, privacy mechanism, edge evaluation type, and quality rating. The following sub-sections report findings by research question.




*(Figure 1: PRISMA-ScR flow diagram for the scoping review.)*

Table 2: Characteristics of included studies (n = 99).

*Privacy rigour in parentheses: F = Formal; C = Claimed-only; S = Structural FL only.* Non-IoT surrogate dataset.

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| **FL-IoT extraction category (61 studies)** | | | | | | |
| Chen et al. (2020) | Wireless edge | GRU-SVM | FedAGRU | Struct. FL (S) | Physical (RPi) | CICIDS2017; WSN-DS |
| Attota et al. (2021) | IoT general | ANN | FedAvg | Struct. FL (S) | Server sim. | MQTT-IoT |
| Huong et al. (2022) | ICS/SCADA | CNN | FedAvg | Struct. FL (S) | Physical (RPi) | HAI; SWaT |
| Driss et al. (2022) | IoV | GRU | FedAvg | Struct. FL (S) | Server sim. | Car-Hacking |
| Ruzafa-Alcázar et al. (2023) | IIoT | LR | FedAvg | DP (F) | Not stated | CIC-ToN-IoT |
| Jithish et al. (2023) | Smart grid | CNN | FedAvg | Struct. FL (S) | Server sim. | CICIDS2017 |
| Tran et al. (2023) | Smart grid | CNN | FedAvg | Encryption (S) | Server sim. | SimBench |
| Hajj et al. (2023) | IoT general | CNN | CrossLayer FL | Sec. aggr. (C) | Server sim. | TON-IoT |
| Sáez-de Cámara et al. (2023) | Hetero. IoT | Autoencoder | Clustered FL | Struct. FL (S) | Server sim. | CICIDS2017 |
| Jin et al. (2024) | IIoT | CNN | FedAvg+BC | Blockchain (S) | Server sim. | TON-IoT |
| Bhavsar et al. (2024) | Transport IoT | CNN | FedAvg | Struct. FL (S) | Server sim. | CICIDS2017 |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| Soomro et al. (2024) | IIoT CPS | CNN-LSTM | FedAvg | Struct. FL (S) | Server sim. | CIC-IDS2017 |
| Verma et al. (2024) | IoT general | GRU+AE | FedAvg | Struct. FL (S) | Server sim. | NSL-KDD |
| Agrawal et al. (2024) | IoT general | MLP | FedAvg | Struct. FL (S) | Server sim. | CICIDS2017 |
| Koroniotis et al. (2024) | Hetero. IoT | CNN | FedAvg+AdaBoost | Struct. FL (S) | Server sim. | BoT-IoT |
| Ahmad et al. (2025) | IoT general | CNN-LSTM | FedAvg | Struct. FL (S) | Server sim. | TON-IoT |
| Anjum et al. (2025) | IoT general | GNN | FedAvg | Struct. FL (S) | Server sim. | CICIoT2023 |
| Bukhari et al. (2024) | IIoT edge | CNN-LSTM | FedAvg+BC | Blockchain (S) | Server sim. | CICIDS2017 |
| Chaurasia et al. (2024) | IIoT | ResNet | FedAvg | Struct. FL (S) | Server sim. | N-BaIoT |
| Mothukuri et al. (2022) | IoT general | CNN | FedAvg | Struct. FL (S) | Server sim. | MQTT-IoT |
| Bouzeraib et al. (2025) | IoT general | GAN+DNN | FedAvg | Struct. FL (S) | Server sim. | CICIDS2017 |
| Abd Elaziz et al. (2025) | IoT general | TabTransformer | FedAvg | Struct. FL (S) | Server sim. | N-BaIoT |
| Almansour et al. (2025) | IoV | CNN | FedProx (PFL) | Struct. FL (S) | Server sim. | IoV-IDS |
| Peng et al. (2025) | Hetero. IoT | LSTM+KD | FedAvg+KD | Struct. FL (S) | Server sim. | N-BaIoT |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| Al Mazroa (2025) | IIoT | CNN-LSTM | FedAvg | Struct. FL (S) | Physical (RPi) | CICIDS2017 |
| Alsaleh et al. (2025) | Hetero. IoT | BiLSTM | Semi-decentral. | Struct. FL (S) | Server sim. | UNSW-NB15 |
| Beshah et al. (2025) | IoT DDoS | CNN-LSTM | FedDWC | Struct. FL (S) | Server sim. | CICIoT2023 |
| Praveen et al. (2025) | 6G IoT CPS | Dual-attn LSTM | RL-EAFRA | DP (F) | Physical (RPi) | CSE-CIC-IDS2018 |
| Sharaf and Nooh (2025) | IoMT | CNN-BiLSTM | FedAvg | Struct. FL (S) | Server sim. | Custom IoMT |
| Devi et al. (2025) | WSN/Smart city | CNN-LSTM | W-FedAvg | Struct. FL (S) | Server sim. | TON-IoT |
| Alabdulatif (2025) | Cognitive IIoT | Self-attn LSTM | FedCognis | Quantum-sec.(C) | Server sim. | WUSTL-IIoTCC |
| Farooq et al. (2025) | Smart city | MLP | FedAvg+SHAP | Struct. FL (S) | Server sim. | NSL-KDD |
| Khan and Svetinovic (2026) | IoT general | DNN | FedAvg | DP-LDP (F) | Server sim. | MNIST/CIFAR ^* |
| Danquah et al. (2025) | IoT edge | MLP | FedAvg | DP (F) | Server sim. | N-BaIoT |
| Alqazzaz (2025b) | IIoT | TCN | FedAvg+Paillier | HE-Paillier (F) | Server sim. | X-IIoTID |
| Khraisat et al. (2025b) | WSN | Random Forest | RF-FedAvg | Struct. FL (S) | Server sim. | WSN-DS |
| Al Tfaily et al. (2025) | IoT general | GNN (GATSage) | FedGATSage | Struct. FL (S) | Server sim. | NF-ToN-IoT |
| Ragab et al. (2025) | Smart city | Stacked AE | FedAvg | Struct. FL (S) | Server sim. | Custom (unnamed) |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| Hossain et al. (2025) | IoT botnet | RF+SHAP-KD | SHAP-KD FedAvg | Struct. FL (S) | Server sim. | N-BaIoT |
| Alqazzaz (2025a) | Smart city | CNN | FedAvg+HE+ DP | HE+DP (F) | Server sim. | CICIDS2017 |
| Ranpara et al. (2025) | SDN-IoT | GRU-SDN | H+V FedAvg | Struct. FL (S) | Server sim. | CICIDS2017 |
| Sanjalawe et al. (2025) | IoT general | CNN-GRU | AGAT-FL | Struct. FL (S) | Server sim. | N-BaIoT |
| Ma et al. (2025) | IoT botnet | ViT+KD | FedAvg/Scaffold | Struct. FL (S) | Physical (Jetson) | N-BaIoT |
| Babar et al. (2026) | Healthcare 6G | CNN-BiLSTM | TAWB-SFL | Blockchain (S) | Server sim. | TON-IoT |
| Nakayiza et al. (2026) | IoT general | GNN | APFed | HE+Blockchain(F) | Server sim. | CICIoT2023 |
| Mhawish et al. (2026) | IIoT | CNN | FedAvg | Struct. FL (S) | Server sim. | Edge-IIoTset |
| Issa et al. (2026) | IoT MTDC | LSTM | MTDC-FL | Struct. FL (S) | Server sim. | CICIoT2023 |
| Ullah et al. (2026) | IoT general | Hybrid adv. | Spectre-Fed | DP (F) | Server sim. | TON-IoT |
| Joseph et al. (2026) | IIoT | DNN | FedAvg | DP (F) | Server sim. | TON-IoT |
| Sorour et al. (2025) | IoT general | LSTM-JSO | FedAvg | Struct. FL (S) | Server sim. | TON-IoT |
| AlHayan and Al-Muhtadi (2026) | IoT general | LSTM+GAN+ LLM | FedAvg | Struct. FL (S) | Server sim. | UNSW-NB15 |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| Islam et al. (2025) | Fog IoT | CNN | PP-HFFL | DP (F) | Server sim. | NSL-KDD |
| Bilal et al. (2026) | IoT general | LSTM+Transformer | FedAvg/FedProx | Struct. FL (S) | Server sim. | Edge-IIoTset |
| García-Sáez et al. (2026) | Hetero. IoT | CNN-LSTM | Hybrid cluster FL | Struct. FL (S) | Server sim. | UNSW-NB15 |
| Puviarasu and Sudha (2026) | IoT general | CNN | FedAvg | HE+DP (F) | Server sim. | Custom IoT |
| Iqbal et al. (2026) | IoT edge | HANN-FL | SPADIS | Struct. FL (S) | Server sim. | Custom (unnamed) |
| Swarnalatha et al. (2026) | Hetero. IoT | BiLSTM | FedAvg | Struct. FL (S) | Server sim. | TON-IoT |
| Nishad et al. (2026) | IIoT edge | CNN | PoT-FedAvg | DP+Blockchain(F) | Server sim. | TON-IoT |
| Khraisat et al. (2025a) | IoT general | MLP | FedAvg/FedAvgM | Struct. FL (S) | Server sim. | N-BaIoT |
| Alharthi et al. (2025) | IIoT | CNN | Block-HFL | Blockchain (S) | Server sim. | Edge-IIoTset |
| Albanbay et al. (2025) | IoT general | CNN-BiLSTM | FedAvg | Struct. FL (S) | Physical (RPi) | CICIoT2023 |
| **DL-Blockchain extraction category (43 studies; Babar et al. shared with FL-IoT)** | | | | | | |
| Babar et al. | Healthcar | CNN-BiLSTM | TAWB-SFL | Blockchain (S) | Server | TON-IoT |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| (2026) | e 6G | | | | sim. | |
| Ibrahim et al. (2026a) | IIoT | BiLSTM | FedAvg+BC | DP+Blockchain(F) | Server sim. | N-BaIoT |
| Ibrahim et al. (2026b) | IIoT | CNN | PureChain FL | Blockchain (S) | Server sim. | CICIDS2017 |
| Abdelhady et al. (2026) | LoRaWAN | GAT | FedAvg | Blockchain (S) | Server sim. | Custom LoRa |
| Sengan et al. (2026) | Healthcare IoT | CNN-LSTM | Blockchain | Blockchain (S) | Server sim. | NSL-KDD |
| Lilhore et al. (2026) | Edge IoT | CNN-LSTM | FedAvg+BC | Blockchain+FL(S) | Server sim. | CICIDS2017 |
| Parashar et al. (2026) | Healthcare IoT | CNN | Blockchain | Blockchain (S) | Server sim. | Custom health |
| Ahakonye et al. (2025) | IIoT | LSTM | PureChain FL | Blockchain+FL(S) | Server sim. | N-BaIoT |
| Srinivasan and Senthilkumar (2025) | IIoT | CNN | Hybridised | Blockchain (S) | Server sim. | NSL-KDD |
| Luo et al. (2025) | IIoT | CNN | BC-sharding FL | Blockchain+FL(S) | Server sim. | CICIDS2017 |
| Nguyen et al. (2025) | IoT general | CNN | BC-FL | Blockchain+FL(S) | Server sim. | N-BaIoT |
| Manzano et al. (2025) | IoT general | DNN | FedAvg+diffusion | Blockchain (S) | Server sim. | CICIDS2017 |
| Villegas-Ch et al. (2025) | IoT general | CNN | Hybrid AI+BC | Blockchain (S) | Server sim. | NSL-KDD |
| Mukisa et al. (2025) | Edge IoT | CNN-LSTM | ATM-FL+BC | Blockchain+FL(S) | Server sim. | TON-IoT |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| Liu et al. (2021) | Vehicular IoT | GNN | BC+FL | Blockchain (S) | Server sim. | VeReMi |
| Dineshbabu and Vigenesh (2025) | IIoT | CNN | SecureFLACF | Blockchain (S) | Server sim. | CICIDS2017 |
| Sathyabama and Katiravan (2025) | IoT general | DNN | BC-DNN | Blockchain (S) | Server sim. | NSL-KDD |
| Alkhonaini et al. (2025) | IoT general | CNN | Sandpiper+BC | Blockchain (S) | Server sim. | CICIDS2017 |
| Ullah et al. (2025) | Large-scale IoT | LSTM | MBID-PINN | Blockchain (S) | Server sim. | BoT-IoT |
| Odeh and Abu Taleb (2025) | IoT access ctrl | CNN | BC-FL | Blockchain+FL(S) | Server sim. | CICIDS2017 |
| Alamro et al. (2025) | Consumer IoT | CNN | Attn+BC | Blockchain (S) | Server sim. | NSL-KDD |
| Alabdan et al. (2025) | Consumer IoT | CNN | IT2F-DL+BC | Blockchain (S) | Server sim. | NSL-KDD |
| Kolsur and Hosmani (2025) | IoT general | CNN | BC-DL | Blockchain (S) | Server sim. | NSL-KDD |
| Alatawi (2025) | IoT general | CNN | Attn+BC | Blockchain (S) | Server sim. | BoT-IoT |
| Mahendran et al. (2025) | IoT general | LSTM | BC-LSTM | Blockchain (S) | Server sim. | NSL-KDD |
| Gebresilassie et al. (2025) | IIoT | CNN | BC-CNN | Blockchain (S) | Server sim. | BoT-IoT |
| Ngo et al. | IoT | CNN | BC-DL | Blockchain (S) | Server | NSL-KDD |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| (2024) | general | | | | sim. | |
| Kokila and Reddy (2024) | IoT general | CNN | BC+DL | Blockchain (S) | Server sim. | CICIDS2017 |
| Alkhammash (2024) | IoT general | CNN | BC-IDS | Blockchain (S) | Server sim. | NSL-KDD |
| Alruwaili et al. (2024) | IoT general | CNN | BC+ML | Blockchain (S) | Server sim. | NSL-KDD |
| Lekssays et al. (2021) | IoT botnet | GNN (PeerHunter) | BC+PeerHunter | BC+Privacy (F) | Server sim. | Custom P2P |
| Farooq et al. (2022) | Smart home | DNN | Private BC | Blockchain (S) | Server sim. | NSL-KDD |
| Liu et al. (2022) | Smart transport | (RTS-DELM) AE+MLP | Hyperledger Fab. | Blockchain (S) | Server sim. | CICDDoS2019 |
| Ahmed et al. (2022) | IoT general | RBM | Private BC | Blockchain (S) | Server sim. | BoT-IoT |
| Mansour (2022) | IIoT | CNN | BC-cluster | Blockchain (S) | Server sim. | UNSW-NB15 |
| Khonde and Ulagamuthalvi (2022) | IoT general | CNN | Hyperledger+Saw. | Blockchain (S) | Server sim. | CICIDS2017 |
| Selvarajan et al. (2023) | IIoT | CNN | Lightweight BC | Blockchain (S) | Server sim. | NSL-KDD |
| Arazzi et al. (2023) | IoT general | CNN | FedAvg+HE | HE+Blockchain(F) | Server sim. | N-BaIoT |
| Vargas et al. (2021) | IIoT | DNN | BC+ML | Blockchain (S) | Server sim. | CICIDS2017 |
| Rathee et al. (2022) | IIoT | DNN | BC+Viterbi | Blockchain (S) | Server sim. | NSL-KDD |

| Study | Domain | Architecture | Aggregation | Privacy (Rig.) | Edge Eval. | Dataset |
|---|---|---|---|---|---|---|
| Ashraf et al. (2022) | Healthcare IoT | CNN | FIDChain FL | Blockchain+FL(S) | Server sim. | IoT-Healthcare |
| Salim et al. (2022) | IIoT | CNN | Digital twin+BC | Blockchain (S) | Server sim. | N-BaIoT |
| Kumar et al. (2021) | Smart contract IoT | RF+XGBoost | IPFS+Ethereum | Blockchain (S) | Server sim. | BoT-IoT |

### 3.1 AI Architecture and Detection Performance (RQ1)

McMahan et al. (2017) is the most widely used aggregation algorithm across the combined corpus, but the literature has produced a substantial diversity of variants: FedProx, FedDWC, FedAGRU, APFed, attention-weighted FL, TAWB-SFL, and reinforcement learning-based aggregation schemes each appears in at least one included study. This diversity shows that the field has moved well beyond the basic FedAvg formulation. Each variant targets a specific weakness: non-IID data heterogeneity, communication overhead, adversarial robustness, or client trust management.

Twelve architecture families are confirmed across the FL-IoT extraction category: CNN, LSTM, BiLSTM, GRU, ResNet, graph neural networks (GNNs), TabTransformer, autoencoder, GAN-augmented, hybrid CNN-LSTM, dual-attention, and LLM-integrated models. CNN-LSTM hybrids and BiLSTM variants are the most frequent; both combine spatial feature extraction with temporal classification. GNN-based approaches represent the most architecturally distinct sub-family: Chen et al. (2020) proposed FedAGRU, an attention-weighted aggregation scheme over GRU-SVM local models, while Al Tfaily et al. (2025) introduced FedGATSage, partitioning Graph Attention Networks to clients and applying GraphSAGE at the server over a community overlay graph. LLM integration appears in AlHayan and Al-Muhtadi (2026), who combine DistilBERT and GPT-2-medium with LSTM and GAN components for real-time behavioural detection; this is the most architecturally complex model in the corpus. Full architecture and aggregation frequency data are reported in Table 2.

Detection performance on controlled benchmark datasets is uniformly high. Across the FL-IoT category, accuracy and weighted F1-scores in the range 93–99% are reported on TON-IoT, CICIoT2023, N-BaIoT, and similar IoT traffic benchmarks under IID and non-IID partitioning. However, this performance ceiling is an artefact of benchmark conditions. Figure 2 shows that 2025–2026 papers dominate the corpus, and the most precisely quantified controlled-versus-realistic gap in the corpus is 36.5 percentage points: Ranpara et al. (2025) report 96% detection accuracy on a balanced controlled dataset against 59.50% on a real-world imbalanced dataset using the same model; ROC AUC falls below 0.67 for all named attack classes on the real-world data. Only two papers in the combined corpus report FL exceeding a centralised baseline (Mhawish et al., 2026; Ullah et al., 2026); Ma et al. (2025) provide the most precisely stated FL-versus-centralised trade-off, at −1.40 percentage points on N-BaIoT.

Two emergent sub-themes appear across multiple papers but have not yet constituted a methodological standard. Interpretability is present in six FL-IoT papers (via SHAP feature importance (Hossain et al., 2025; Farooq et al.,

2025), GAT-based attention weights (Sanjalawe et al., 2025), or federated feature selection) and absent from the entire DL-Blockchain category. Open-set and zero-day detection, addressed by Verma et al. (2024), targets attack classes unseen at training time; no DL-Blockchain paper addresses this threat scenario.

### 3.2 Privacy-Preserving Mechanisms (RQ2)

Structural FL is the most prevalent privacy approach in the FL-IoT category. Under this approach, the federated training paradigm is treated as a sufficient privacy guarantee on the grounds that raw data are not shared. Across 41 of the 61 FL-IoT studies, privacy is asserted at the level of the training architecture without differential privacy bounds, cryptographic secure aggregation, or any mechanism that constrains information leakage from gradient updates (see Table 2, Privacy column). The operational consequence is that gradient inversion and membership inference attacks (Ruzafa-Alcázar et al., 2023) remain unaddressed threat vectors in the majority of the corpus. Representative examples illustrate the range of architectures operating under this assumption. Soomro et al. (2024) deploy a CNN-LSTM model across industrial CPS clients under FedAvg on CIC-IDS2017, achieving 99.1% accuracy with no privacy mechanism beyond the federated training paradigm itself. Koroniotis et al. (2024) combine FedAvg with AdaBoost on BoT-IoT across heterogeneous IoT clients; the absence of gradient protection is not flagged as a limitation despite the industrial deployment context. Anjum et al. (2025) extend this pattern to GNN architectures on CICIoT2023, reporting 98.7% F1 with no formal privacy bound; the contribution is architectural novelty rather than privacy rigour. Across these and the remaining structural FL papers, the common thread is that privacy is a design assumption rather than an evaluated property.

Formal privacy guarantees appear in eleven FL-IoT papers. Differential privacy is the most common formal mechanism: Ruzafa-Alcázar et al. (2023) and Danquah et al. (2025) apply standard ( \epsilon, \delta )-DP with fixed budgets; Praveen et al. (2025) introduce an adaptive decaying \epsilon schedule; Islam et al. (2025) apply DP-SGD via the Opacus library with formal RDP composition; and Ullah et al. (2026) implement adaptive Gaussian gradient noise with exponential decay, although no formal ( \epsilon, \delta ) bound is stated. Homomorphic encryption appears in two papers: Alqazzaz (2025b) applies Paillier partially homomorphic encryption to gradient aggregation, and Nakayiza et al. (2026) use CKKS fully homomorphic encryption with dynamic precision scaling; CKKS encryption and decryption are three orders of magnitude faster than Paillier on equivalent inputs. Two further papers combine mechanisms: Alqazzaz (2025a) pairs optimised HE with adaptive DP, and Nishad et al. (2026) apply Gaussian DP with Moments Accountant alongside a blockchain proof-of-trust consensus layer.

In the DL-Blockchain category, blockchain-as-auditability functions as the primary privacy mechanism across all 43 papers. Proof-of-Authority (PoA) is the most common consensus protocol; its low latency relative to Proof-of-Work makes it the preferred choice in healthcare and IIoT deployments (Salim et al., 2022; Babar et al., 2026). However, 19 of the 43 DL-Blockchain papers describe blockchain architecturally without reporting throughput, latency, or consensus overhead (see Table 2). Representative examples illustrate the pattern. Sengan et al. (2026) integrate Ethereum into a healthcare IoT IDS pipeline with a CNN-LSTM classifier on NSL-KDD; the paper reports 99.2% accuracy but provides no blockchain throughput or transaction confirmation time. Kolsur and Hosmani (2025) implement a permissioned blockchain for audit trail logging without any performance benchmarking. Odeh and Abu Taleb (2025) combine blockchain access control with FL-based intrusion detection but measure only detection accuracy, not the overhead of the blockchain coordination layer. Among the papers that do quantify blockchain overhead, Ashraf et al. (2022) report approximately 3% computational overhead per training epoch for blockchain weight validation in a healthcare IoT FL setting; this is one of the few concrete overhead figures in the category. Lekssays et al. (2021) quantify a more substantial cost: privacy-preserving anonymisation adds a 2.5 \times

processing overhead relative to blockchain-only operation across 38 million network flows.

Explainability of detection decisions is absent from all 43 DL-Blockchain papers. The audit trail that blockchain logging is intended to provide records what was decided and when, but not why. In regulated deployment contexts where decision transparency is a compliance requirement, this absence is a structural gap that blockchain auditability alone does not address.

### 3.3 Edge Deployability (RQ3)

Server simulation is the dominant evaluation mode across the combined corpus. As shown in Figure 5, 54 of 61 FL-IoT studies and all 43 DL-Blockchain studies evaluate solely on desktop or cloud hardware; no DL-Blockchain paper reports inference latency, model size, or energy consumption on any IoT-class device.

Physical hardware evaluation appears in five FL-IoT studies. Chen et al. (2020) deploy on Raspberry Pi; their testbed is the earliest physical FL-IDS evaluation in the corpus. Huong et al. (2022) evaluate on Raspberry Pi with HAI and SWaT industrial control datasets. Bhavsar et al. (2024) operate a two-tier physical testbed of Raspberry Pi 4 client nodes and a Jetson Xavier server, the most complete multi-node physical FL deployment in the corpus. Al Mazroa (2025) and Albanbay et al. (2025) each deploy on Raspberry Pi for IIoT and general IoT threat detection scenarios respectively. On the inference side, Ma et al. (2025) report knowledge distillation from a Vision Transformer teacher to a compressed student model targeted at the Jetson Nano; this is the only paper in the corpus to state hardware-level inference metrics for an IoT-class edge device. Praveen et al. (2025) conduct a 6G CPS evaluation on Raspberry Pi with an adaptive RL-based aggregation scheme under real-world class imbalance.

Communication overhead is almost entirely absent from reporting. Issa et al. (2026) state a model transmission size of 35 KB for a two-layer DNN, the only explicit model size in the corpus. Alqazzaz (2025a) report a 40% reduction in transmission volume and a 43% reduction in latency through gradient sparsification combined with optimised homomorphic encryption; no other FL-IoT paper reports comparable communication metrics.

The sharpest quantification of deployment risk is provided by Ranpara et al. (2025), whose results are discussed in Section 3.1: a 36.5 percentage-point gap between controlled and real-world accuracy on the same model. ROC AUC falls below 0.67 for all named attack classes on real-world imbalanced data. No DL-Blockchain paper reports a controlled-versus-realistic comparison of any kind.

### 3.4 Domain Coverage and Threat Taxonomy (RQ4)

IoT general and IIoT account for 44 of the 99 included studies, as shown in Figure 3. Healthcare IoT, vehicular IoT, and smart city environments each appear in fewer than seven studies despite representing high-value attack surfaces. Specialised domains (LoRaWAN, smart transport, and 6G-enabled IoT) appear in a single study each (Abdelhady et al., 2026; Liu et al., 2022; Praveen et al., 2025).

DDoS and its sub-variants are the dominant threat class across the combined corpus. Among FL-IoT papers, Agrawal et al. (2024) provide the most granular DDoS taxonomy, disaggregating seven sub-types (UDP, TCP, ICMP, HTTP, HTTPS, DNS, and SSDP flooding) on CICIoT2023 using a hierarchical three-tier FL architecture. Beshah et al. (2025) use DDoS as the sole threat class across 1,000 simulated clients and achieve 98.47% weighted F1 with FedDWC aggregation on CICIoT2023; the limitation is that single-threat evaluation precludes assessment of multi-class detection capability. Botnet detection is the second most frequent threat class, with N-BaIoT serving as the primary benchmark across nine FL-IoT studies. The dataset captures traffic from nine real IoT devices infected with Mirai and BASHLITE botnets, making it one of the few genuinely IoT-native benchmarks in the corpus. Abd Elaziz et al. (2025) apply a TabTransformer architecture under FedAvg across heterogeneous client types, reporting 99.4% accuracy; the non-IID evaluation across seven device families is methodologically stronger than most papers using this dataset. Nakayiza et al. (2026) use N-

BaIoT in the only paper combining FL with CKKS homomorphic encryption, evaluating APFed aggregation with privacy overhead quantified. The remaining N-BaIoT users evaluate under IID or unreported partitioning (Peng et al., 2025; Danquah et al., 2025; Hossain et al., 2025; Sanjalawe et al., 2025; Ma et al., 2025; Nguyen et al., 2025; Ahakonye et al., 2025).

False data injection attacks on smart grid infrastructure appear in one FL-IoT study. Tran et al. (2023) deploy a cross-silo FL framework across four transmission grid companies; DCR-based double-layer encryption and Shamir secret sharing protect gradient exchange. A simulation-based security proof establishes computational indistinguishability against an honest-but-curious aggregator colluding with up to \tau - 1 clients; SIMD parallelisation reduces the privacy overhead to 2.38% of total training time. The primary limitation is that evaluation uses the synthetic SimBench power grid dataset; no real utility network traffic is used.

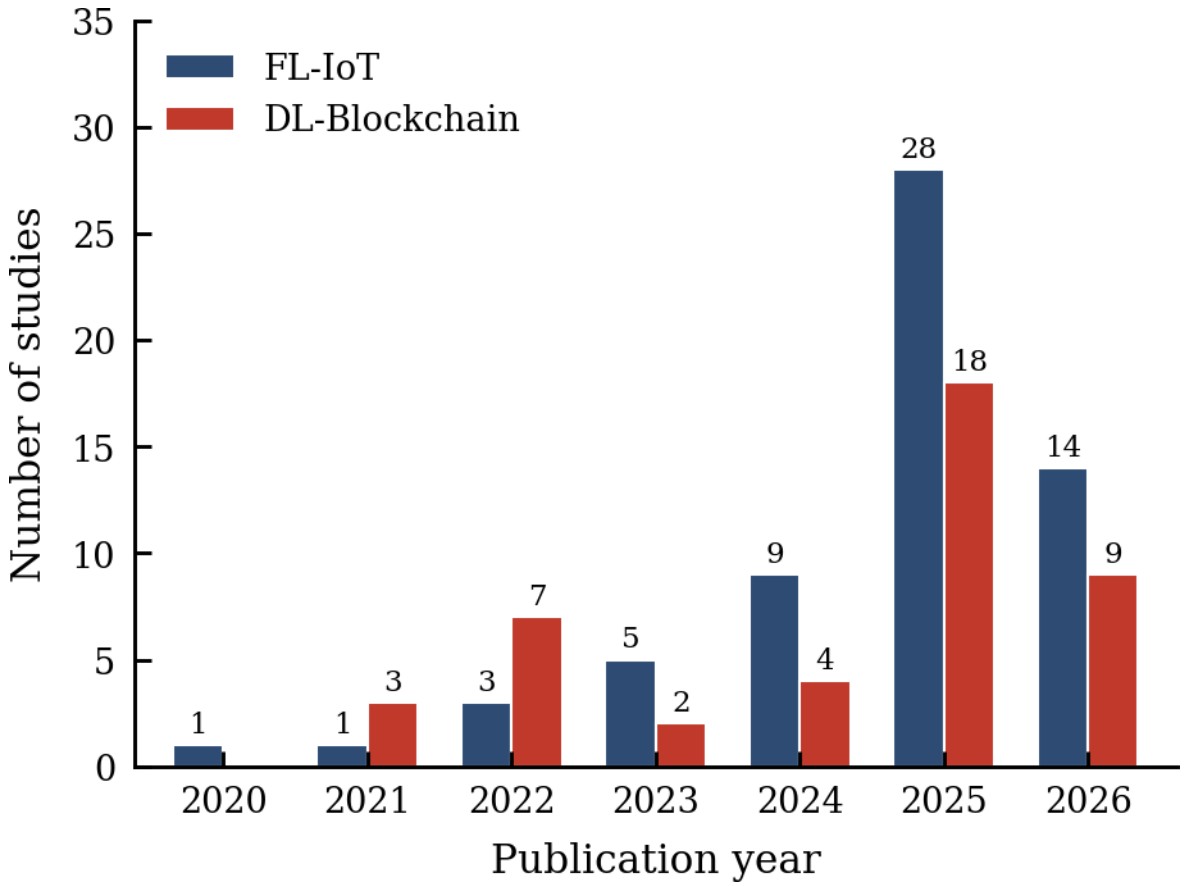
The most complete threat diversity in the FL-IoT category comes from Sáez-de Cámara et al. (2023), who construct the Gotham testbed, a GNS3-based emulated IoT network of 78 devices across 30 switches and 10 routers. Full Mirai malware lifecycle (scanning, brute force, command-and-control, eight DoS variants) and Merlin C&C with hping3 DDoS are executed against the testbed. A clustered FL framework with an unsupervised autoencoder (trained on benign traffic only; attacks are detected via reconstruction error) is evaluated against the published Kitsune non-FL IDS baseline using Matthews Correlation Coefficient as the primary metric; this is the only paper in the FL-IoT category to benchmark against a state-of-the-art non-FL IDS. The limitation is that the threat scenarios are confined to network-layer volumetric attacks; application-layer and protocol-specific attacks are not covered.

Protocol-specific threat coverage is sparse. CAN bus intrusion detection appears in Nakayiza et al. (2026) (vehicular IoT). MQTT-specific traffic is used as the evaluation dataset in two early FL-IoT papers (Mothukuri et al., 2022; Attota et al., 2021). P2P botnet detection via graph community analysis rather than a classifier appears in Lekssays et al. (2021), the only paper in either category not to use a DL model for detection. Smart contract attack surfaces and supply-chain threats are absent from the corpus entirely.

The dataset landscape shows pronounced concentration on legacy benchmarks. NSL-KDD (2009) appears in 19 of the 43 DL-Blockchain studies and ten FL-IoT papers (see Table 2, Dataset column). The dataset was designed for conventional TCP/IP network intrusion scenarios and predates the IoT by a decade; its attack taxonomy includes no IoT-specific threat vectors. Sathyabama and Katiravan (2025) apply a blockchain-integrated DNN on NSL-KDD and report 99.7% accuracy; the absence of IoT-native evaluation is not flagged as a limitation. AlHayan and Al-Muhtadi (2026), despite building the most architecturally complex model in the FL-IoT corpus (LSTM+GAN+LLM), evaluate it on NSL-KDD, which obscures whether the added complexity transfers to real IoT traffic. García-Sáez et al. (2026) use NSL-KDD for a heterogeneous FL evaluation across 100 clients; the non-IID setup is methodologically rigorous but the dataset choice undermines the IoT deployment claim. In the FL-IoT category, CICIDS2017 and N-BaIoT are the primary benchmarks across 23 and nine studies respectively; both are IoT-relevant but pre-date the current generation of edge FL architectures by several years.

## 4. Discussion

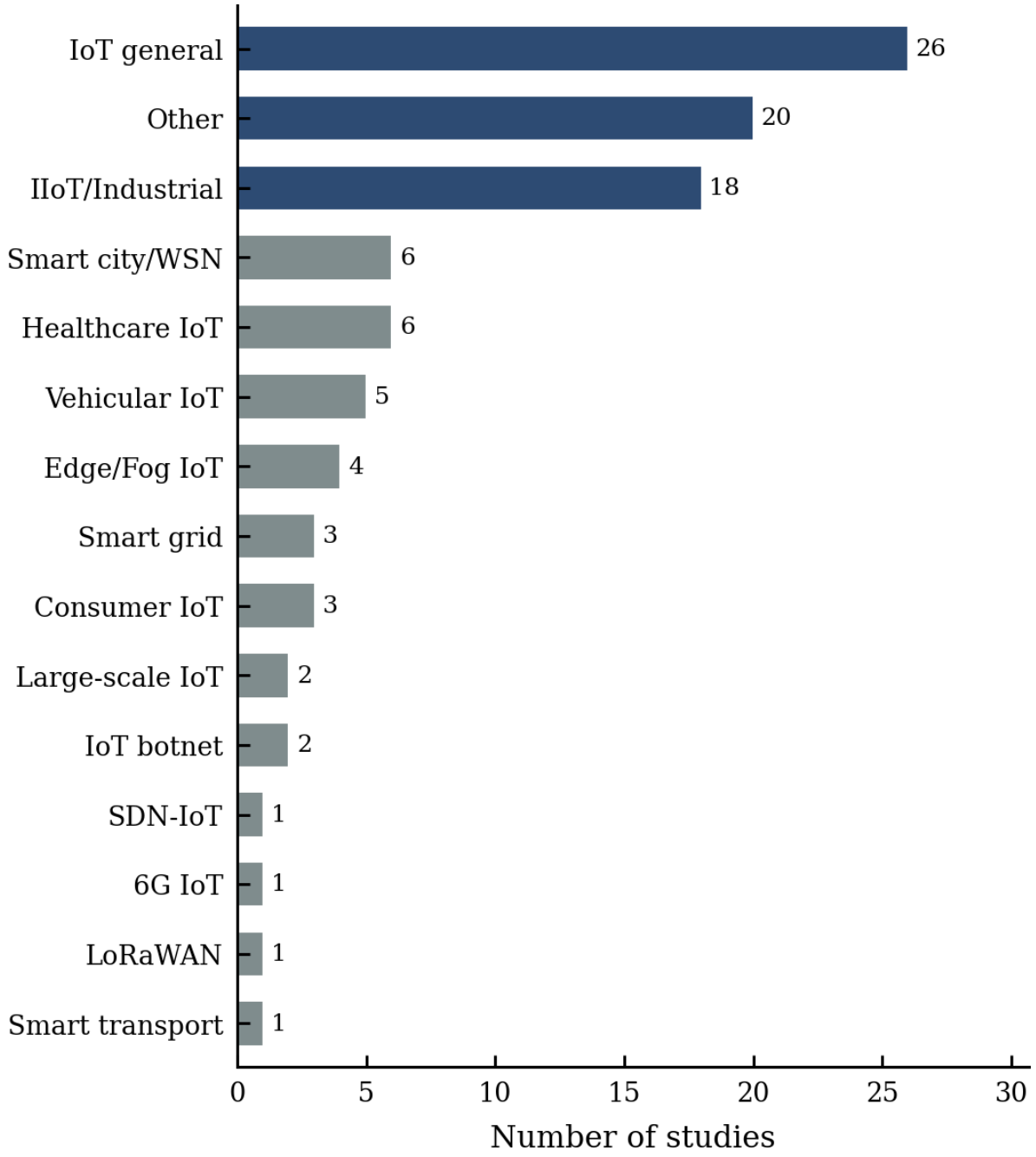
The findings in Section 3 point to three clusters of unresolved methodological gaps that collectively constrain the translation of FL-IDS and blockchain-IDS research into operational IoT deployment. Each cluster is characterised using the research gap taxonomy of Miles (2017).




*(Figure 2: Annual publication count across both extraction categories, 2020–2026. The corpus is heavily skewed towards 2025–2026, reflecting accelerating activity in both sub-fields.)*

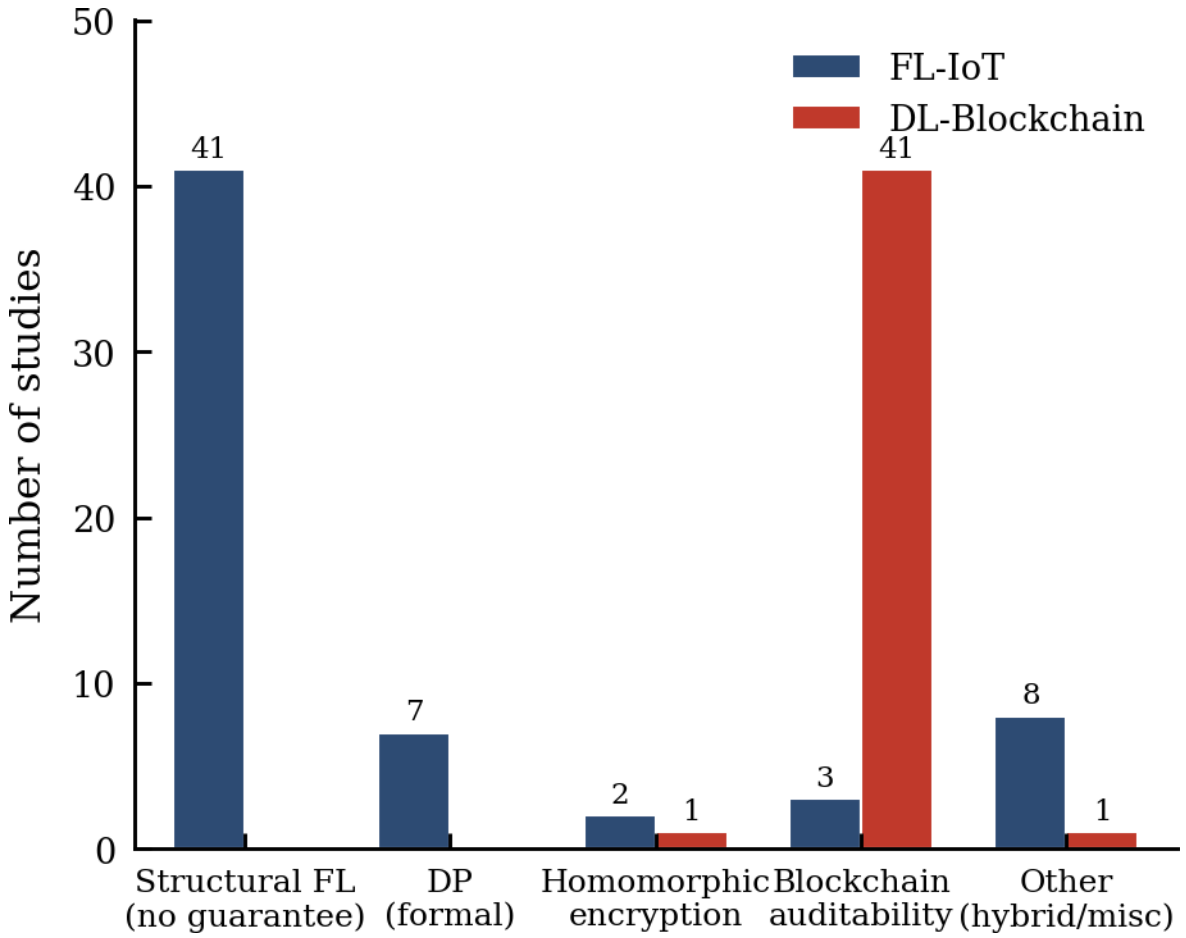
### 4.1 Gap Cluster A: The Deployment Realism Gap

This cluster constitutes an empirical gap (Miles, 2017): research findings and performance claims have not been tested under the conditions that would be required to validate them in practice. Across 88% of the combined corpus, detection performance is reported exclusively from server simulation on desktop or cloud hardware. The five FL-IoT studies that deploy on physical hardware (Raspberry Pi and Jetson-class devices) achieve this at the cost of substantial engineering effort per study, and no DL-Blockchain paper deploys on any IoT-class device. The consequences of this gap are visible in the corpus's sharpest datapoint: a 36.5 percentage-point accuracy degradation when the same FL-IDS model is evaluated on real-world imbalanced data versus a controlled balanced dataset (Ranpara et al., 2025). This gap is not closed by claims of edge deployment intent; server simulation cannot expose the inference latency, memory footprint, energy draw, or class-imbalance sensitivity that govern whether a model is deployable on constrained hardware.




*(Figure 3: Distribution of IoT application domains across the combined corpus (n = 99). General IoT and IIoT account for the majority of studies; specialised domains such as LoRaWAN, smart transport, and 6G IoT appear in only one study each.)*

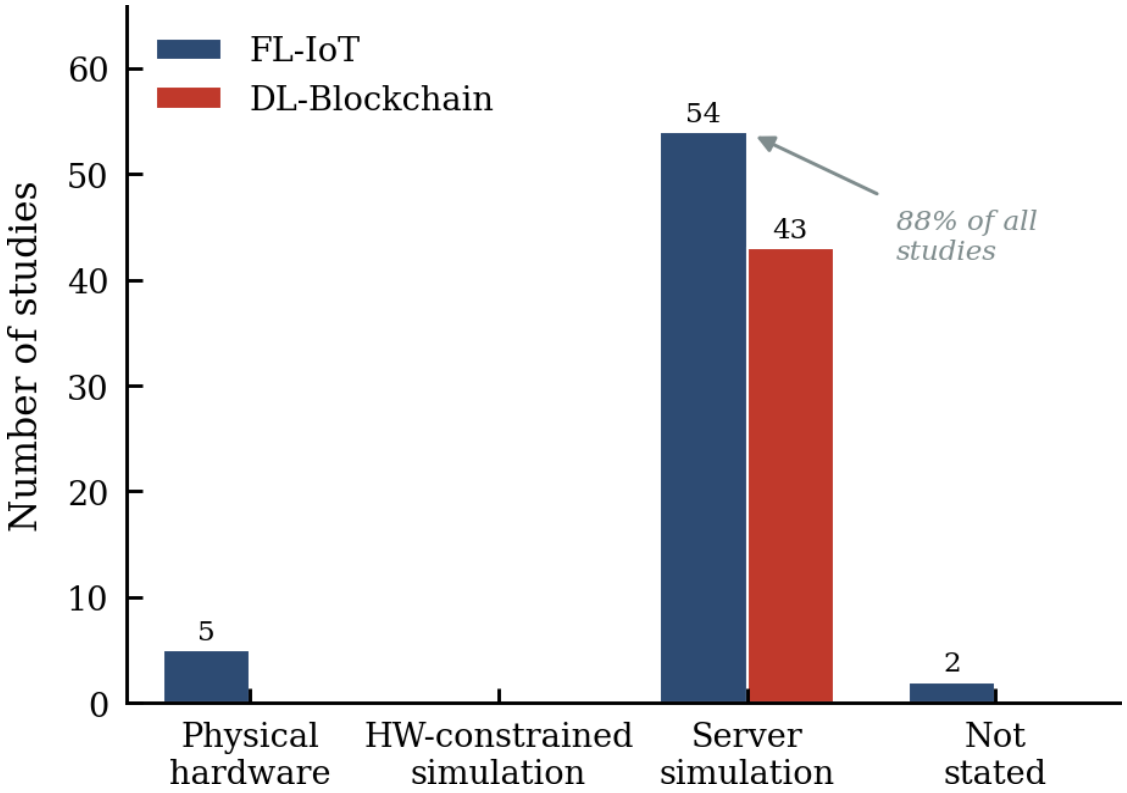
Future primary research should adopt hardware-realistic evaluation as a baseline requirement rather than an optional supplement. Concretely, this means reporting inference latency and memory consumption on MCU-class or single-board-computer hardware alongside accuracy, and reporting performance on real-world imbalanced data as the primary metric rather than as a secondary stress test. The knowledge distillation pipeline of Ma et al. (2025) and the physical Raspberry Pi testbed of Bhavsar et al. (2024) are methodological templates that the field has yet to adopt at scale.




*(Figure 4: Privacy mechanism classification across both extraction categories. Structural FL dominates the FL-IoT category; blockchain auditability dominates the DL-Blockchain category. Formal guarantees (DP and HE) appear in only nine FL-IoT studies.)*

### 4.2 Gap Cluster B: The Privacy Rigour Gap

This cluster combines a practical-knowledge gap and an evidence gap (Miles, 2017). The practical-knowledge dimension is the divergence between the field's stated privacy objective (protecting IoT data from inference attacks on gradient updates) and its predominant practice (structural FL, which provides no formal guarantee against gradient inversion or membership inference). Ruzafa-Alcázar et al. (2023) are among the first in the FL-IoT category to name gradient inversion and membership inference explicitly as threat vectors. The majority of structurally-private papers do not acknowledge these threats at all (see Table 2, Privacy column). Soomro et al. (2024) deploy CNN-LSTM across IIoT CPS clients under FedAvg, reporting 99.1% accuracy; gradient attack vulnerability is neither evaluated nor mentioned. Koroniotis et al. (2024) combine FedAvg with ensemble boosting across heterogeneous IoT environments; the paper discusses adversarial robustness at the model level but not gradient-level inference risk. Jithish et al. (2023) implement smart grid FL-IDS with no privacy mechanism and no acknowledgement of gradient interception as a threat in a cross-organisational training context—precisely the scenario in which gradient leakage risk is highest.




*(Figure 5: Distribution of edge evaluation types across included studies. Server simulation accounts for 88% of all studies; physical hardware evaluation appears in only five FL-IoT papers and no DL-Blockchain paper.)*

The evidence gap arises in the formal privacy sub-literature. Differential privacy implementations produce conflicting evidence on the accuracy-privacy trade-off: Ullah et al. (2026) report near-zero accuracy cost from adaptive Gaussian gradient noise, whilst standard fixed-budget DP approaches reported in the same paper incur a 5.77 percentage-point accuracy drop. These results conflict and cannot be reconciled without standardised privacy budget reporting. No two papers in the FL-IoT category report DP under the same \epsilon value, making cross-study comparison impossible.

In the DL-Blockchain category, the privacy rigour gap takes a different form. Blockchain provides tamper-proof logging of what was detected and when, but no paper in the category addresses explainability of why a detection decision was made (see Table 2). For regulated deployment contexts (healthcare IoT, critical infrastructure), audit trail completeness requires both what and why. The operational implication is direct: Sengan et al. (2026) deploy blockchain-integrated CNN-LSTM for healthcare IoT monitoring, where regulatory accountability requires explainable decisions; the paper records blockchain transactions but provides no mechanism to interrogate individual detection decisions. Kokila and Reddy (2024) and Ngo et al. (2024) follow the same pattern in general IoT contexts, logging model update hashes on-chain without any feature attribution or decision explanation. The FL-IoT sub-literature is more advanced in this respect; SHAP-based interpretability is present in six papers (Hossain et al., 2025; Farooq et al., 2025; Sanjalawe et al., 2025; Agrawal et al., 2024; Ma et al., 2025; Joseph et al., 2026), but these are exceptions rather than a standard evaluation component.

### 4.3 Gap Cluster C: The Evaluation Reproducibility Gap

This cluster constitutes a methodological gap (Miles, 2017): the absence of a shared evaluation

protocol makes findings from different studies cumulative in appearance but not in practice. Three specific reproducibility failures recur across the corpus.

First, FL configuration is incompletely reported in a substantial proportion of studies. The number of clients, communication rounds, local epochs, and non-IID partitioning scheme are all necessary to reproduce an FL-IDS result; yet papers that omit one or more of these parameters are not exceptional in the corpus. Bouzeraib et al. (2025) report GAN+DNN detection on CICIDS2017 without stating client count or round count. Devi et al. (2025) implement W-FedAvg for smart city intrusion detection with no partitioning scheme described. Ragab et al. (2025) report results on an unnamed custom dataset with no FL configuration detail; the result is neither reproducible nor comparable. Without complete configuration reporting, a result such as 99% accuracy on CICIoT2023 under FedAvg cannot be reproduced, compared, or falsified.

Second, the dataset landscape is anchored on benchmarks that pre-date the evaluation targets. As discussed in Section 3.4, NSL-KDD (2009) appears in 29 of the 104 included studies across both categories. The IoT attack taxonomy that NSL-KDD encodes does not address the threat landscape that current IDS systems are expected to address. High accuracy on NSL-KDD is therefore not evidence of fitness for IoT deployment; it is evidence of fitness for a network threat taxonomy that is over fifteen years old.

Third, dataset identity is omitted in a growing number of recent papers. Where a paper reports accuracy without naming the dataset, the result is unverifiable (Ragab et al., 2025; Iqbal et al., 2026; Puviarasu and Sudha, 2026). This pattern is observed across multiple 2025–2026 papers in the FL-IoT category; the field's publication pressure appears to be outpacing its methodological discipline.

### 4.4 Limitations

First, the evidence base rests on a pre-extraction corpus architecture in which both thematic categories were originally assembled for distinct research purposes. Although eligibility criteria were harmonised and cross-category duplicates removed, the source corpora may systematically over-represent the sub-problems their respective search strategies were designed to capture, and under-represent research at the intersection of FL, blockchain, and hardware-realistic edge deployment. Second, quality assessment uses a corpus-specific three-tier rubric (Strong, Adequate, Weak) rather than a validated appraisal instrument such as CASP. The rubric was applied consistently, but the ratings are not directly comparable with quality scores from other systematic reviews. Third, the corpus is temporally skewed: 42 of the 99 included studies were published in 2025 or 2026. Findings characterising the 2024–2026 literature cover an active and rapidly-changing sub-field; claims about the state of the field in earlier periods are supported by fewer studies per year.

## 5. Conclusion

A scoping review of 99 empirical studies of AI-driven IoT intrusion detection (2020–2026) identified three gap clusters that constrain translation of FL-IDS and blockchain-IDS research into operational deployment.

The deployment realism gap (empirical gap) is the most operationally consequential. Server simulation dominates 88% of the combined corpus; physical hardware evaluation has been conducted in five FL-IoT studies, and no DL-Blockchain paper has evaluated inference on any IoT-class device. The quantified penalty for this gap reaches 36.5 percentage points when a deployed model encounters real-world class imbalance.

The privacy rigour gap (practical-knowledge and evidence gap) separates the field's stated objective from its practice. Forty-one of 61 FL-IoT studies assert privacy through the federated training paradigm alone, without formal differential privacy, homomorphic encryption, or secure aggregation. In the DL-Blockchain category, blockchain audit trail logging records detection outcomes but no paper addresses why those outcomes were produced; explainability is absent from the entire category.

The evaluation reproducibility gap (methodological gap) prevents findings from

accumulating into comparable knowledge. Incomplete FL configuration reporting, a persistent dependence on NSL-KDD despite its 2009 origins, and unnamed datasets in a growing number of recent papers collectively make cross-study comparison unreliable.

Closing these three gaps requires three corresponding commitments from the primary research community: hardware-realistic evaluation as a baseline standard rather than an optional supplement; formal privacy guarantees with standardised budget reporting rather than architectural claims; and complete FL configuration and dataset identity disclosure as a condition of publishable results. Until these are in place, the performance figures reported in this literature cannot be taken as evidence of IoT deployment readiness.

## Declaration of Competing Interest

The author declares no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data Availability

The full extraction records for both thematic extraction categories are available from the corresponding author on reasonable request.

## References


- Abd Elaziz, M., Fares, I.A., Dahou, A., Shrahili, M., 2025. Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimisation. Frontiers in Big Data 8, 1526480. doi:10.3389/fdata.2025.1526480.
- Abdelhady, G., Ghandoura, A., Motwakel, A., Alajmi, A., 2026. Hybrid machine learning anomaly detection and lightweight zero trust authentication for LoRaWAN networks. IEEE Access 14, 18387–18407. doi:10.1109/ACCESS.2026.3660731.
- Agrawal, S., Sarkar, S., Srivastava, G., Ghosh, U., 2024. Federated learning for decentralized DDoS attack detection in IoT networks. IEEE Access 12, 39810–39825. doi:10.1109/ACCESS.2024.3378727.
- Ahakonye, L.A.C., Nwakanma, C.I., Lee, J.M., Kim, D.S., 2025. PureChain-enhanced federated learning for dynamic fault tolerance and attack detection in distributed systems. High-Confidence Computing 6, 100354. doi:10.1016/j.hcc.2025.100354.
- Ahmad, I., Shaikh, A., Ahmad, J., Alqahtani, S., Alsubai, S., Binbusayyis, A., 2025. FFL-IDS: a fog-enabled federated learning-based intrusion detection system to counter jamming and spoofing attacks in IoT. Sensors 25, 10. doi:10.3390/s25010010.
- Ahmed, M.A., Althubiti, S.A., Nageswara Rao, D., Lydia, E.L., Cho, W., Joshi, G.P., Kim, S.W., 2022. Blockchain assisted intrusion detection system using differential flower pollination model. Computers, Materials and Continua doi:10.32604/crnc.2022.
- Al Mazroa, A., 2025. FORT-IDS: a federated, optimized, robust and trustworthy intrusion detection system for IIoT security. Scientific Reports 15. doi:10.1038/s41598-025-31025-x.
- Al Tfaily, F., Ghalmane, Z., Brahmia, M.e.A., Hazimeh, H., Jaber, A., Zghal, M., 2025. Graph-based federated learning approach for intrusion detection in IoT networks. Scientific Reports 15, 41264. doi:10.1038/s41598-025-25175-1.
- Alabdan, R., Alabduallah, B., Alruwais, N., Arasi, M.A., Asklany, S.A., Alghushairy, O., Alallah, F.S., Alshareef, A., 2025. Blockchain-assisted improved interval type-2 fuzzy deep learning-based attack detection on internet of things driven consumer electronics. Alexandria Engineering Journal 110, 153–. doi:10.1016/j.aej.2024.09.117.

- Alabdulatif, A., 2025. FedCognis: an adaptive federated learning framework for secure anomaly detection in industrial IoT-enabled cognitive cities. Computers, Materials & Continua doi:10.32604/crnc.2025.066898.
- Alamro, H., Maray, M., Aljabri, J., Alahmari, S., Abdullah, M., Alqurni, J.S., Alotaibi, F.A., Mohamed, A.A., 2025. Mathematical modelling-based blockchain with attention deep learning model for cybersecurity in IoT-consumer electronics. Alexandria Engineering Journal 113, 366–. doi:10.1016/j.aej.2024.11.016.
- Alatawi, M.N., 2025. EdgeGuard-IoT: 6G-enabled edge intelligence for secure federated learning and adaptive anomaly detection in Industry 5.0. Computers, Materials and Continua.
- Albanbay, N., Tursynbek, Y., Graffi, K., Uskenbayeva, R., Kalpeyeva, Z., Abilkaiyr, Z., Ayapov, Y., 2025. Federated learning-based intrusion detection in IoT networks: Performance evaluation and data scaling study. Journal of Sensor and Actuator Networks 14, 78. doi:10.3390/jsan14040078.
- Alharthi, H.S., Alshehri, S., Kalkatawi, M., 2025. Blockchain-enabled hierarchical federated learning framework for anomaly detection in IoT systems. Applied Sciences 15, 13037. doi:10.3390/app152413037.
- AlHayan, A., Al-Muhtadi, J., 2026. Federated learning-powered real-time behavioral intrusion detection leveraging LSTM, attention, GANs, and large language models. Scientific Reports doi:10.1038/s41598-026-40763-5.
- Alkhammash, M., 2024. A metaheuristic approach to detecting and mitigating DDoS attacks in blockchain-integrated deep learning models for IoT applications. IEEE Access 13, 193184–. doi:10.1109/ACCESS.2024.3519132.
- Alkhonaini, M.A., Alohali, M.A., Aljebreen, M., Eltahir, M.M., Alanazi, M.H., Yafoz, A., Alsini, R., Khadidos, A.O., 2025. Sandpiper optimization with hybrid deep learning model for blockchain-assisted intrusion detection in IoT environment. Alexandria Engineering Journal 112, 49–61. doi:10.1016/j.aej.2024.10.032.
- Almansour, S., Yadav, K., Alkwai, L.M., Alghamdi, N.S., Viriyasitavat, W., Dhiman, G., 2025. Adaptive personalized federated learning with lightweight depthwise convolutional bottleneck network for novel intrusion detection system in internet of vehicles. Scientific Reports 15. doi:10.1038/s41598-025-17699-3.
- Alqazzaz, A., 2025a. Federated learning with homomorphic encryption: a privacy-preserving solution for smart cities. International Journal of Computational Intelligence Systems 18, 304. doi:10.1007/s44196-025-00829-0.
- Alqazzaz, A., 2025b. SecuFL-IoT: an adaptive privacy-preserving federated learning framework for anomaly detection in smart industrial networks. Scientific Reports 15. doi:10.1038/s41598-025-11883-1.
- Alruwaili, F.F., Alohali, M.A., Aljaffan, N., Alhashmi, A.A., Mahmud, A., Assiri, M., 2024. A decentralized approach to smart home security: blockchain with red-tailed hawk-enabled deep learning. IEEE Access 12, 14146–. doi:10.1109/ACCESS.2024.3352502.
- Alsaleh, S., Menai, M.E.B., Al-Ahmadi, S., 2025. A heterogeneity-aware semi-decentralized model for a lightweight intrusion detection system for IoT networks based on federated learning and BiLSTM. Sensors 25, 1039. doi:10.3390/s25041039.
- Anjum, M., Dutta, A.K., Elrashidi, A., Shahab, S., Aldrees, A., Shaikh, Z.A., Aljohani, A., 2025. GraphFedAI framework for DDoS attack detection in IoT systems using federated learning and graph neural networks. Scientific Reports

15, 9447. doi:10.1038/s41598-025-10826-0.

- Arazzi, M., Nicolazzo, S., Nocera, A., 2023. A fully privacy-preserving solution for anomaly detection in IoT using federated learning and homomorphic encryption. Information Systems Frontiers.
- Arksey, H., O'Malley, L., 2005. Scoping studies: towards a methodological framework. International Journal of Social Research Methodology 8, 19–32. doi:10.1080/1364557032000119616.
- Ashraf, E., Areed, N.F.F., Salem, H., Abdelhay, E.H., Farouk, A., 2022. FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications. Healthcare 10, 1110. doi:10.3390/healthcare10061110.
- Attota, D.C., Mothukuri, V., Parizi, R.M., Pouriyeh, S., 2021. An ensemble multi-view federated learning intrusion detection for IoT. IEEE Access 9, 117734–117745. doi:10.1109/ACCESS.2021.3107337.
- Babar, M., Khan, Z., Kaleem, S., Qureshi, B., Boulila, W., 2026. TAWB-SFL: trust-aware blockchain-orchestrated split federated learning for intrusion detection in 6G healthcare IoT. IEEE Open Journal of Communications Society doi:10.1109/OJCOMS.2026.3667693.
- Beshah, Y.K., Abebe, S.L., Melaku, H.M., 2025. Dynamic weight clustered federated learning for IoT DDoS attack detection. Scientific Reports 15. doi:10.1038/s41598-025-13204-y.
- Bhavsar, M.H., Bekele, Y.B., Roy, K., Kelly, J.C., Limbrick, D., 2024. FL-IDS: federated learning-based intrusion detection system using edge devices for transportation IoT. IEEE Access 12, 52215–52230. doi:10.1109/ACCESS.2024.3386631.
- Bilal, M.A., Islam, I.U., Idrees, S., Qasim, M., Khan, M.J., Khan, J., 2026. Dataset-centric evaluation of federated intrusion detection models in IoT networks. Scientific Reports doi:10.1038/s41598-025-32567-w.
- Bouzeraib, W., Ghenai, A., Zeghib, N., 2025. Enhancing IoT intrusion detection systems through horizontal federated learning and optimized WGAN-GP. IEEE Access 13, 45059–45075. doi:10.1109/ACCESS.2025.3547255.
- Bukhari, S.M.S., Zafar, M.H., Abou Houran, M., Qadir, Z., Moosavi, S.K.R., Sanfilippo, F., 2024. Enhancing cybersecurity in edge IIoT networks: an asynchronous federated learning approach with a deep hybrid detection model. Internet of Things 27, 101252. doi:10.1016/j.iot.2024.101252.
- Sáez-de Cámara, X., Flores, J.L., Arellano, C., Urbieta, A., Zurutuza, U., 2023. Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks. Computers & Security 131, 103299. doi:10.1016/j.cose.2023.103299.
- Chaurasia, N., Ram, M., Verma, P., Mehta, N., Bharot, N., 2024. A federated learning approach to network intrusion detection using residual networks in industrial IoT networks. The Journal of Supercomputing 80, 18325–18346. doi:10.1007/s11227-024-06153-2.
- Chen, Z., Lv, N., Liu, P., Fang, Y., Chen, K., Pan, W., 2020. Intrusion detection for wireless edge networks based on federated learning. IEEE Access 8, 217463–217472. doi:10.1109/ACCESS.2020.3041793.
- Danquah, L.K.G., Appiah, S.Y., Mantey, V.A., Danlard, I., Akowuah, E.K., 2025. Computationally efficient deep federated learning with optimized feature selection for IoT botnet attack detection. Intelligent Systems with Applications 25, 200462. doi:10.1016/j.iswa.2024.200462.
- Devi, M., Nandal, P., Sehrawat, H., 2025. Federated learning-enabled lightweight

intrusion detection system for wireless sensor networks: a cybersecurity approach against DDoS attacks in smart city environments. Intelligent Systems with Applications 25, 200553. doi:10.1016/j.iswa.2025.200553.

- Dineshbabu, V., Vigenesh, M., 2025. SecureFLACF: secure federated learning access control framework with blockchain-infused intrusion detection system for IIoT. Journal of Mobile Multimedia 21, 939–966. doi:10.13052/jrnrn1550-4646.2155.
- Driss, M., Almomani, I., Huma, Z.e., Ahmad, J., 2022. A federated learning framework for cyberattack detection in vehicular sensor networks. Complex & Intelligent Systems 8, 3569–3579. doi:10.1007/s40747-022-00705-w.
- Farooq, M.S., Khan, S., Rehman, A., Abbas, S., Khan, M.A., Hwang, S.O., 2022. Blockchain-based smart home networks security empowered with fused machine learning. Sensors 22, 4522. doi:10.3390/s22124522.
- Farooq, M.S., Saleem, M., Khan, M., Khan, M.F., Siddiqui, S.Y., Aslam, M.S., Adnan, K.M., 2025. Interpretable federated learning model for cyber intrusion detection in smart cities with privacy-preserving feature selection. Computers, Materials & Continua doi:10.32604/crnc.2025.069641.
- García-Sáez, L.M., Ruiz-Villafranca, S., Roldán-Gómez, J., Carrillo-Mondéjar, J., Martínez, J.L., 2026. Hybrid clustering-guided federated learning for robust intrusion detection in highly heterogeneous IoT environments. Computer Networks 281, 112205. doi:10.1016/j.cornnet.2026.112205.
- Gebresilassie, S.K., Rafferty, J., Abu-Tair, M., Ali, A., Chen, L., Cui, Z., 2025. SHIELD: secure holistic IoT environment with ledger-based defense. Internet of Things 30, 101473. doi:10.1016/j.iot.2024.101473.
- Hajj, S., Azar, J., Bou Abdo, J., Demerjian, J., Guyeux, C., Makhoul, A., Ginhac, D., 2023. Cross-layer federated learning for lightweight IoT intrusion detection systems. Sensors 23, 7038. doi:10.3390/s23167038.
- Hossain, M.A., Saif, S., Islam, M.S., 2025. A novel federated learning approach for IoT botnet intrusion detection using SHAP-based knowledge distillation. Complex & Intelligent Systems 11. doi:10.1007/s40747-025-02001-9.
- Huong, T.T., Bac, T.P., Ha, K.N., Hoang, N.V., Hoang, N.X., Hung, N.T., Tran, K.P., 2022. Federated learning-based explainable anomaly detection for industrial control systems. IEEE Access 10, 53854–53873. doi:10.1109/ACCESS.2022.3173288.
- Ibrahim, H., Ahakonye, L.A.C., Lee, J.M., Kim, D.S., 2026a. PureChain closed loop intrusion detection and real-time recovery for industrial IoT. IEEE Internet of Things Journal.
- Ibrahim, H., Ahakonye, L.A.C., Lee, J.M., Kim, D.S., 2026b. A unified AI–PureChain framework for verifiable intrusion prevention in industrial IoT systems. IEEE Internet of Things Journal 13, 12906–12919. doi:10.1109/JIOT.2026.3652250.
- Iqbal, R., Ismail, S., Rathee, G., 2026. Hardware aware federated learning with sparse models for adaptive anomaly detection in IoT. Discover Artificial Intelligence doi:10.1007/s44163-026-01171-w.
- Islam, M.M., Abdullah, W.M., Saha, B.N., 2025. Privacy-preserving hierarchical fog federated learning (PP-HFFL) for IoT intrusion detection. Sensors 25, 7296. doi:10.3390/s25237296.
- Issa, M.A., Eldosouky, A., Matrawy, A., Ibnkahla, M., 2026. Multi-temporal device clustering for federated learning–Internet of Things intrusion detection

systems. IEEE Transactions on Machine Learning in Communications and Networking doi:10.1109/TMLCN.2026.3706262.

- Jin, X., Ma, C., Luo, S., Zeng, P., Wei, Y., 2024. Distributed IIoT anomaly detection scheme based on blockchain and federated learning. Journal of Communications and Networks 26, 252–262. doi:10.23919/JCN.2024.000016.
- Jithish, J., Alangot, B., Mahalingam, N., Yeo, K.S., 2023. Distributed anomaly detection in smart grids: a federated learning-based approach. IEEE Access 11, 7157–7179. doi:10.1109/ACCESS.2023.3237554.
- Joseph, L., Prabha, B., Sambath, M., 2026. TrustFed-RHIO: an optimization-driven differential privacy federated learning framework for secure and explainable IIoT attack detection. Scientific Reports doi:10.1038/s41598-026-45277-8.
- Khan, S., Svetinovic, D., 2026. Adaptive privacy-preserving federated learning for robust IoT systems: a defence against data poisoning attacks. IoT and Cyber-Physical Systems doi:10.1016/j.iotcps.2026.03.006.
- Khonde, S.R., Ulagamuthalvi, V., 2022. Hybrid intrusion detection system using blockchain framework. EURASIP Journal on Wireless Communications and Networking 2022, 97. doi:10.1186/s13638-022-02089-4.
- Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S., Jan, T., 2025a. Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy. Discover Internet of Things 5, 72. doi:10.1007/s43926-025-00169-7.
- Khraisat, A., Alazab, A., Vasan, D., Marshall, A., Alqhtani, S.M., 2025b. RF-FedAvg: federated learning-based random forest model for intrusion detection in wireless sensor networks. Cluster Computing 28. doi:10.1007/s10586-025-05591-8.
- Kokila, M., Reddy, K.S., 2024. BlockDLO: blockchain computing with deep learning orchestration for secure data communication in IoT environment. IEEE Access 12, 134521–. doi:10.1109/ACCESS.2024.3462735.
- Kolsur, S., Hosmani, S., 2025. Artificial intelligence-based healthcare cybersecurity system with blockchain: modified parallel convolutional neural network for attack detection. Medicine in Novel Technology and Devices 28, 100412. doi:10.1016/j.medntd.2025.100412.
- Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., Janicke, H., 2024. Edge-federated learning-based intelligent intrusion detection system for heterogeneous internet of things. IEEE Access 12, 83375–83393. doi:10.1109/ACCESS.2024.3410046.
- Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R., 2021. A distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT systems by leveraging fog computing. Transactions on Emerging Telecommunications Technologies 32, e4112. doi:10.1002/ett.4112.
- Lekssays, A., Landa, L., Carminati, B., Ferrari, E., 2021. PAutoBotCatcher: A blockchain-based privacy-preserving botnet detector for Internet of Things. Computer Networks 200, 108512. doi:10.1016/j.cornnet.2021.108512.
- Levac, D., Colquhoun, H., O'Brien, K.K., 2010. Scoping studies: advancing the methodology. Implementation Science 5, 69. doi:10.1186/1748-5908-5-69.
- Lilhore, U.K., Sharma, Y.K., Pradeep, S., Rubaiee, S., Alroobaea, R., Baqasah, A.M., Alsafyani, M., Tekeste, L.G., 2026. Blockchain-enabled federated learning framework with hybrid CNN-LSTM anomaly detection for secure edge

IoT networks. Journal of Cloud Computing.

- Liu, H., Zhang, S., Zhang, P., Zhou, X., Shao, X., Pu, G., Zhang, Y., 2021. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. IEEE Transactions on Vehicular Technology doi:10.1109/TVT.2021.3076780.
- Liu, T., Sabrina, F., Jang-Jaccard, J., Xu, W., Wei, Y., 2022. Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems. Sensors 22, 32. doi:10.3390/s22010032.
- Luo, S., Zeng, P., Ma, C., Wei, Y., 2025. Anomaly detection for industrial internet of things devices based on self-adaptive blockchain sharding and federated learning. Journal of Communications and Networks 27, 92–102. doi:10.23919/JCN.2025.000019.
- Ma, L., He, J., Lu, K., Wang, D., Yin, L., Li, Z., 2025. A contrastive learning and knowledge distillation-based framework for efficient federated intrusion detection in IoT. Systems Science & Control Engineering 13, 2518963. doi:10.1080/21642583.2025.2518963.
- Mahendran, R.K., Khan, A., Ullah, F., Ali, F., AlZubi, A.A., 2025. PRISM-IIoT: a holistic approach for privacy preservation in industrial IoT using advanced cryptography and blockchain-enabled auditability framework. Alexandria Engineering Journal 128, 816–. doi:10.1016/j.aej.2025.07.027.
- Mansour, R.F., 2022. Blockchain assisted clustering with intrusion detection system for industrial internet of things environment. Expert Systems with Applications 207, 117995. doi:10.1016/j.eswa.2022.117995.
- Manzano, R., Zaman, M., Upadhyay, D., Goel, N., Sampalli, S., 2025. Federated learning framework based on distributed storage and diffusion model for intrusion detection on IoT networks. IEEE Access 13, 79571–. doi:10.1109/ACCESS.2025.3565409.
- McMahan, B., Moore, E., Ramage, D., Hampson, S., y Arcas, B.A., 2017. Communication-efficient learning of deep networks from decentralized data, in: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), pp. 1273–1282.
- Mhawish, M.Y., Aljamal, M., Alsarhan, A., Khassawneh, B.S., Akhunzada, A., Al-Shamayleh, A.S., 2026. A novel adaptive generalization-guided federated learning for multimodal industrial IoT intrusion detection under statistical heterogeneity. IEEE Open Journal of Computer Society doi:10.1109/OJCS.2026.3703977.
- Miles, D.A., 2017. A taxonomy of research gaps: identifying and defining the seven research gaps, in: Doctoral Student Workshop: Finding Research Gaps—Research Methods and Strategies, Dallas, Texas. pp. 1–11.
- Mothukuri, V., Khare, P., Parizi, R.M., Pouriyeh, S., Dehghantanha, A., Srivastava, G., 2022. Federated-learning-based anomaly detection for IoT security attacks. IEEE Internet of Things Journal 9, 2545–2554. doi:10.1109/JIOT.2021.3077803.
- Mukisa, K.J., Ahakonye, L.A.C., Kim, D.S., Lee, J.M., 2025. Blockchain-augmented FL IDS for non-IID edge-IoT data using adaptive trimmed mean aggregation. IEEE Internet of Things Journal 12, 45150–45159. doi:10.1109/JIOT.2025.3598832.
- Nakayiza, H.L., Ahakonye, L.A.C., Kim, D.S., Lee, J.M., 2026. PureFL: trust-weighted federated learning with noise-resilient homomorphic encryption for blockchain-based IoV networks. IEEE Internet of Things Journal doi:10.1109/JIOT.2026.3691349.
- Ngo, D.M., Lightbody, D., Temko, A., Murphy, C.C., Popovici, E., 2024. A scalable security approach in IoT

networks: smart contracts and anomaly-based IDS for gateways using hardware accelerators. IEEE Access 12, 159519–. doi:10.1109/ACCESS.2024.3486605.

- Nguyen, V.D., Diro, A., Chilamkurti, N., Heyne, W., Phan, K.T., 2025. A novel blockchain-enabled federated learning scheme for IoT anomaly detection. IEEE Transactions on Machine Learning in Communications and Networking.
- Nishad, D.K., Singh, R., Khalid, S., 2026. A lightweight blockchain-enabled federated intrusion prevention framework for resource-constrained industrial IoT devices to detect and mitigate emerging cyberattacks. Journal of Cloud Computing doi:10.1186/s13677-026-00843-3.
- Odeh, A., Abu Taleb, A., 2025. Federated learning and blockchain framework for scalable and secure IoT access control. Computers, Materials and Continua.
- Parashar, J., Hung, B.T., Upreti, K., Kshirsagar, P.R., Mahajan, S., Kadry, S., 2026. An enhanced hybrid framework for IoT healthcare security using blockchain-driven multimedia data analysis and cybersecurity techniques. Array 30, 100759. doi:10.1016/j.array.2026.100759.
- Peng, H., Wu, C., Xiao, Y., 2025. FD-IDS: federated learning with knowledge distillation for intrusion detection in non-IID IoT environments. Sensors 25, 4309. doi:10.3390/s25144309.
- Praveen, S.P., Sharma, K., Parashar, D., Murthy, V.S.N., Sirisha, U., Dewi, D.A., 2025. Design of an iterative method for adaptive federated intrusion detection for energy-constrained edge-centric 6G IoT cyber-physical systems. Scientific Reports 15. doi:10.1038/s41598-025-25293-w.
- Puviarasu, A., Sudha, V., 2026. Enhanced IoT security: privacy-preserving federated learning model for accurate, real-time intrusion detection across devices. Ain Shams Engineering Journal 17, 103866. doi:10.1016/j.asej.2025.103866.
- Ragab, M., Ashary, E.B., Alghamdi, B.M., Aboalela, R., Alsaadi, N., Maghrabi, L.A., Allehaibi, K.H., 2025. Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. Scientific Reports 15. doi:10.1038/s41598-025-88843-2.
- Ranpara, R., Patel, S.K., Kumar, O.P., Al-Zahrani, F.A., 2025. Scalable architecture for autonomous malware detection and defense in software-defined networks using federated learning approaches. Scientific Reports 15. doi:10.1038/s41598-025-14512-z.
- Rathee, G., Kerrache, C.A., Ferrag, M.A., 2022. A blockchain-based intrusion detection system using Viterbi algorithm and indirect trust for IIoT systems. Journal of Sensor and Actuator Networks 11, 71. doi:10.3390/jsan11040071.
- Ruzafa-Alcázar, P., Fernández-Saura, P., Mármol-Campos, E., González-Vidal, A., Hernández-Ramos, J.L., Bernal-Bernabe, J., Skarmeta, A.F., 2023. Intrusion detection based on privacy-preserving federated learning for the industrial IoT. IEEE Transactions on Industrial Informatics 19, 1145–1154. doi:10.1109/TII.2021.3126728.
- Salim, M.M., Comivi, A.K., Nurbek, T., Park, H., Park, J.H., 2022. A blockchain-enabled secure digital twin framework for early botnet detection in IIoT environment. Sensors 22, 6133. doi:10.3390/s22166133.
- Sanjalawe, Y., Al-E'mari, S., Alqurashi, T., Alharbi, Z.H., Makhadmeh, S.N., Alsharaiah, M., 2025. Adaptive graph attention-based federated learning for IoT intrusion detection: mitigating poisoning attacks. PeerJ Computer Science 11, e3281. doi:10.7717/peerj-cs.3281.

- Sathyabama, A.R., Katiravan, J., 2025. Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security. Scientific Reports 15. doi:10.1038/s41598-025-04164-4.
- Selvarajan, S., Srivastava, G., Khadidos, A.O., Khadidos, A.O., Baza, M., Alshehri, A., Lin, J.C.W., 2023. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing: Advances, Systems and Applications 12, 38. doi:10.1186/s13677-023-00412-y.
- Sengan, S., Shieh, C.S., Horng, M.F., 2026. A hybrid blockchain based deep learning model for multivector attack detection in internet of things enabled healthcare systems. Scientific Reports 16, 10060. doi:10.1038/s41598-026-40765-3.
- Sharaf, S.A., Nooh, S., 2025. Identifying significant features in adversarial attack detection framework using federated learning empowered medical IoT network security. Scientific Reports 15. doi:10.1038/s41598-025-14913-0.
- Soomro, I.A., Khan, H.u.R., Hussain, S.J., Ashraf, Z., Alnfiai, M.M., Alotaibi, N.N., 2024. Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system. Journal of Communications and Networks 26, 632–649. doi:10.23919/JCN.2024.000054.
- Sorour, S.E., Aljaafari, M., Shaker, A.M., Amin, A.E., 2025. LSTM-JSO framework for privacy preserving adaptive intrusion detection in federated IoT networks. Scientific Reports doi:10.1038/s41598-025-95966-z.
- Srinivasan, M., Senthilkumar, N.C., 2025. Intrusion detection and prevention system (IDPS) model for IIoT environments using hybridized framework. IEEE Access 13, 26608–. doi:10.1109/ACCESS.2025.3538461.
- Swarnalatha, T., Aruna Rao, S., Suryodai, R., Narsimha Reddy, D., Vanathi, A., Sudheer Kumar, K., 2026. CyberFedEdgeAI framework for real time cyberattack detection in heterogeneous IoT systems using federated edge intelligence. Discover Computing doi:10.1007/s10791-026-10129-6.
- Tran, H.Y., Hu, J., Yin, X., Pota, H.R., 2023. An efficient privacy-enhancing cross-silo federated learning and applications for false data injection attack detection in smart grids. IEEE Transactions on Information Forensics and Security 18, 2538–2552. doi:10.1109/TIFS.2023.3267892.
- Tricco, A.C., Lillie, E., Zarin, W., O'Brien, K.K., Colquhoun, H., Levac, D., Moher, D., Peters, M.D., Horsley, T., Weeks, L., Hempel, S., Akl, E.A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M.G., Garritty, C., Lewin, S., Godfrey, C.M., Macdonald, M.T., Langlois, E.V., Soares-Weiser, K., Moriarty, J., Clifford, T., Tunçalp, O., Straus, S.E., 2018. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. Annals of Internal Medicine 169, 467–473. doi:10.7326/M18-0850.
- Ullah, S., Wu, J., Kamal, M.M., Alzaylaee, M.K., Alibakhshikenari, M., 2026. Spectre-Fed: evolving federated edge intelligence from FedEdge-ID to robust-private IoT intrusion detection via hybrid adversarial training. IEEE Open Journal of Communications Society doi:10.1109/OJCOMS.2026.3665325.
- Ullah, S., Wu, J., Kamal, M.M., Mohamed, H.G., Sheraz, M., Chuah, T.C., 2025. MBID: a scalable multi-tier blockchain architecture with physics-informed neural networks for intrusion detection in large-scale IoT networks. Computer Modeling in Engineering and Sciences.
- Vargas, H., Lozano-Garzon, C., Montoya, G.A., Donoso, Y., 2021.

Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach. Electronics 10, 2662. doi:10.3390/electronics10212662.

- Verma, P., Bharot, N., Breslin, J.G., O'Shea, D., Vidyarthi, A., Gupta, D., 2024. Zero-Day Guardian: a dual model enabled federated learning framework for handling zero-day attacks in 5G-enabled IIoT. IEEE Transactions on Consumer Electronics 70, 3856–3866. doi:10.1109/TCE.2023.3335385.
- Villegas-Ch, W., Govea, J., Gutierrez, R., Mera-Navarrete, A., 2025. Optimizing security in IoT ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection. IEEE Access 13, 16933–. doi:10.1109/ACCESS.2025.3532800.