Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

INTRUSION DETECTION BASED ON FEDERATED LEARNING – A REVIEW

[1]Abu Ubaida,[2]Khurram Zeeshan Haider*, [3]Temur-ul-Hassan,
[4]Muhammad Azam Rasheed

[1]*Centre of Data Science, Government College University, Faisalabad, Pakistan*
[2]*Department of Software Engineering, Government College University, Faisalabad, Pakistan*
[3]*Department of Computer Science, University of Lahore, Lahore, Pakistan*
[4]*Department of Computer Science, Government College University, Faisalabad, Pakistan*
[1]abuubaida.202202778@gcuf.edu.pk, [2]khurram.zeeshan@gcuf.edu.pk, [3]temur.hassan@cs.uol.edu.pk,
[4]AzamRasheedStudy@gmail.com

Keywords
IoT security, federated learning, intrusion detection systems, privacy-preserving learning.

Article History
Received on 17 March, 2026
Accepted on 10 April, 2026
Published on 11 April, 2026

Corresponding Author:
Khurram Zeeshan Haider*

Abstract
The lack of access to raw data during model training is addressed by privacy-preserving methods, but the construction of intrusion detection systems remains essential for federated learning. The recent increase in FL-based intrusion detection research between 2019 and 2025 is reviewed, covering study metadata, data types, FL architectural designs, communication architectures, model design, and performance results. We include 90 central studies in five tables, showcasing their areas of application, data and preprocessing, FL topology, client diversity and aggregation strategies, model design with privacy in mind, and performance and robustness outcomes. Our findings show that IoT and IIoT applications, horizontal FL, and FedAvg are common; non-IID data and class imbalance are frequent; and public benchmarks like NSL-KDD and CICIDS2017 are widely used. Nevertheless, standardized FL-IDS benchmarks, energy and latency reporting as well as strong aggregation techniques are not well studied. We single out such promising directions as hierarchical and personalized FL, federated data augmentation, privacy- and robustness-oriented aggregation, and cross-dataset benchmarks. This review aims to assist the researchers and practitioners to swiftly realize the present state of the field, the most important gaps, and concentrate on research that can hasten the implementation of dependable FL-based intrusion detection.

1. Introduction

The ever-growing list of connected devices, such as Internet-of-Things (IoT) sensors, industrial control systems (IIoT) and connected cars and medical devices, has broadened the attack surface and the need of automated intrusion detection. Traditional centralized intrusion detection systems (IDS) involve aggregating sensitive telemetry and packet traces somewhere to prepare and make an inference, which may be privacy-sensitive and unfeasible in bandwidth- or policy-constricted environments. Federated learning (FL) reduces these limitations by enabling multiple clients to collectively learn a global model without the need to transfer local data to the cloud. FL provides an avenue to better detection performance in intrusion detection by cooperating without jeopardizing privacy or data governance.

A recent surge in research in this field began in 2019 after the earliest FL applications to IDS were developed in the late 2010s, which has almost doubled since 2019. FL has been implemented to numerous fields, such as IoT, IIoT, Internet of Vehicles, UAVs, smart grids, and medical IoMT networks. This has resulted in a broad spectrum of research, surveys and experiments, as well as data contributions and security analyses. Although most experiments have shown to be highly accurate on benchmark datasets, non-IID and imbalanced client data, communication and latency problems are part of the challenges with real-world deployment.

on the edge, susceptibility to poisoning and gradient-leakage attacks, and unrealistic federated IDS benchmarks and reproducible evaluation protocols.

1.1 Scope and objectives of this review

This literature review is founded on the real-life and empirical experience of implementing federated learning to intrusion detection. We plan to conduct a systematic review and comparison of 90 selected FL-IDS studies published by 20192025 in five domains, namely: study metadata, datasets, model designs, and effectiveness (see Tables 1 to 5). We find general trends, methodological gaps, and performance and deployment issues and gaps. Some promising directions include personalized and hierarchical FL, federated data augmentation, improved aggregation methods, and standard benchmarks. We also suggest research priorities to make FL- IDS more robust, efficient, and reproducible.

1.2 Contributions

The systematic comparative analysis of 90 FL-IDS publications and cataloged into five review tables which contain metadata, data sets, communication/architecture, model selection and performance indicators.

1. An overall evaluation of the existing approaches and limitations, particularly those concerning non-IID data, privacy and security effects, communication and energy reporting, and reproducibility as well as explicit guidelines to conduct such research in the future.
2. A roadmap with recommendations to researchers and practitioners on the necessity to improve the benchmarks, practical deployment trials and better privacy, efficiency, and resource usage.

1.3 Sequence of the paper

The literature is arranged into the following way: Section 2 deals with our criteria regarding including and collection of literature. The comparative tables

and principal findings are contained in section 3. Section 4 explains the key challenges and provides design suggestions of FL-IDS. Future research opportunities and gaps are described in section 5. The concluding comments and reproducible FL-IDS evaluator checklist are in section 6.

2. Literature review

2.1 Literature search strategy

We utilized our goal to develop a selective and re-usable set of papers on federated learning (FL) to intrusion detection systems (IDS) on previous literature to the most current findings (2019-2025). The 90 studies included in this review were selected to represent a range of conferences, journals, and high-quality preprints, covering diverse fields such as IoT, IIoT, IoV, UAVs, smart grids, IoMT, and 5G/6G. The set includes papers from major venues like IEEE, ACM, Elsevier, and arXiv, as well as surveys, empirical studies, datasets, and security analyses.

2.2 Inclusion and exclusion criteria

Included:

Papers: proposing, evaluating, surveying or extending FL methods to intrusion detection task or network security task(s) with an anomaly task.

- Papers about FL design decisions (aggregation, personalization, hierarchical FL), model designs (CNN, LSTM, GAN, Transformer, hybrid), defense strategies (DP, secure aggregation, block chain) and/or IDS-related issues (datasets, label scarcity, non-IID data).
- English publications 2019-2025 (which include 90 references).

Excluded:

- Articles that do not deal directly with intrusion detection (pure FL algorithm articles with no IDS implementation), or articles outside the given time period, without giving a background.
- Poor-quality and workshop abstracts that lack adequate methodological information.

2.3 Screening & data extraction

We extracted and organized the following methodological areas from each included paper, as shown in Tables 1 to 5:

- Study metadata: authors, date, field of application, the type of IDS, and publication place.
- Dataset features: name(s) of the dataset, type of data, pre-processing, and comment on class balances.
- Pan-functional: FL architecture, communication: FL topology, reported number of clients, communication round number, mode of aggregation, special communication/security.
- When referring to a model architecture, it is model family (DNN/CNN
  - /LSTM/GAN/Transformer), hybridization, lightweight adaptations, optimizer/loss.
- Performance and evaluation: accuracy/F1/precision/recall of reported values, robustness experiments (poisoning/gradient leakage) and practical where feasible: latency, communication, energy.
- Other sections: trends/challenges and suggestions on future directions (summarized by the reviewers based on the corpus). We aggregated (interpolated) representative references in each instance of observation/aspect as such that a reader can follow where an observation is being substantiated in the set of 90 papers.

2.4 Synthesis approach

We organized the extracted information into five comparison tables (Tables 1–5). Each table includes a summary, grouped references, entries on trends and challenges, and future directions to highlight key

methodological points. In our qualitative analysis, we identified common themes such as popular datasets, FL approaches, and model types, as well as shortcomings like non-IID data, lack of real deployments, and missing communication or energy reporting.

Limitations: Because studies report information differently, not every field is filled out in each study (for example, the number of clients or communication rounds is sometimes missing or only simulated). We used the values provided by the authors when available, and otherwise followed common practices.

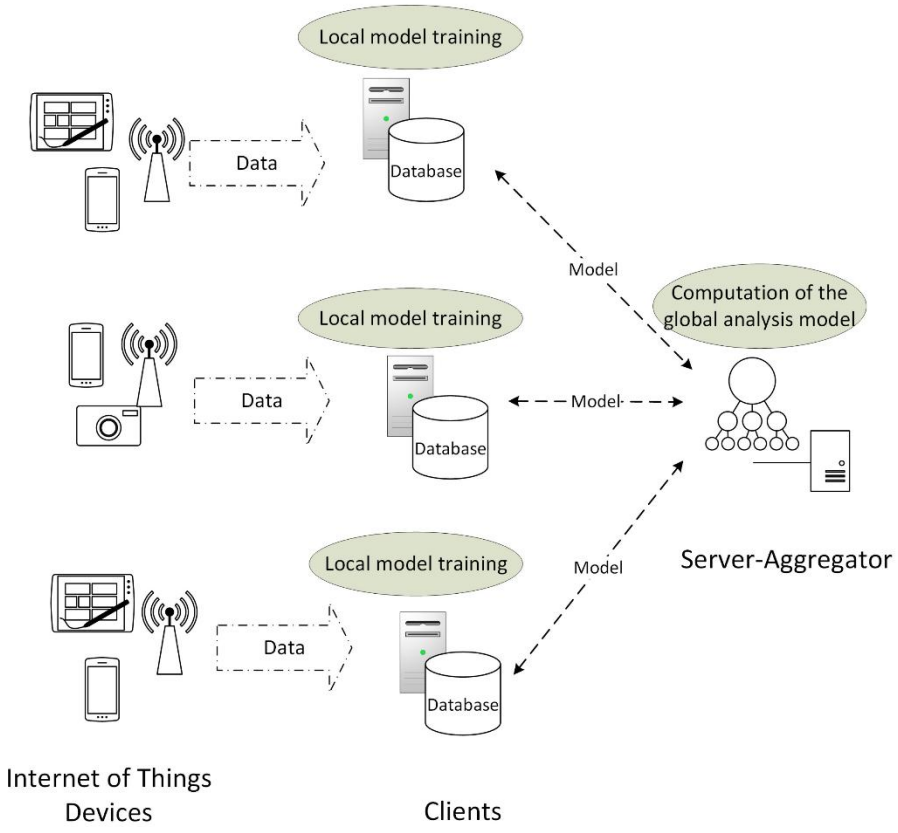

Figure 1: Generic architecture Federated learning-based intrusion detection system with a generic architecture.

Figure 1 demonstrates that distributed IoT clients train models locally using their data and transmit model updates only to a central server, which assembles a global model without transmitting raw data. As illustrated in figure 2, various sensor combinations with local self-supervised learning and model updates sent to a cloud server are used to create a global model. This new universal model is then conveyed to clients to enhance the categorization of attacks and normal traffic.

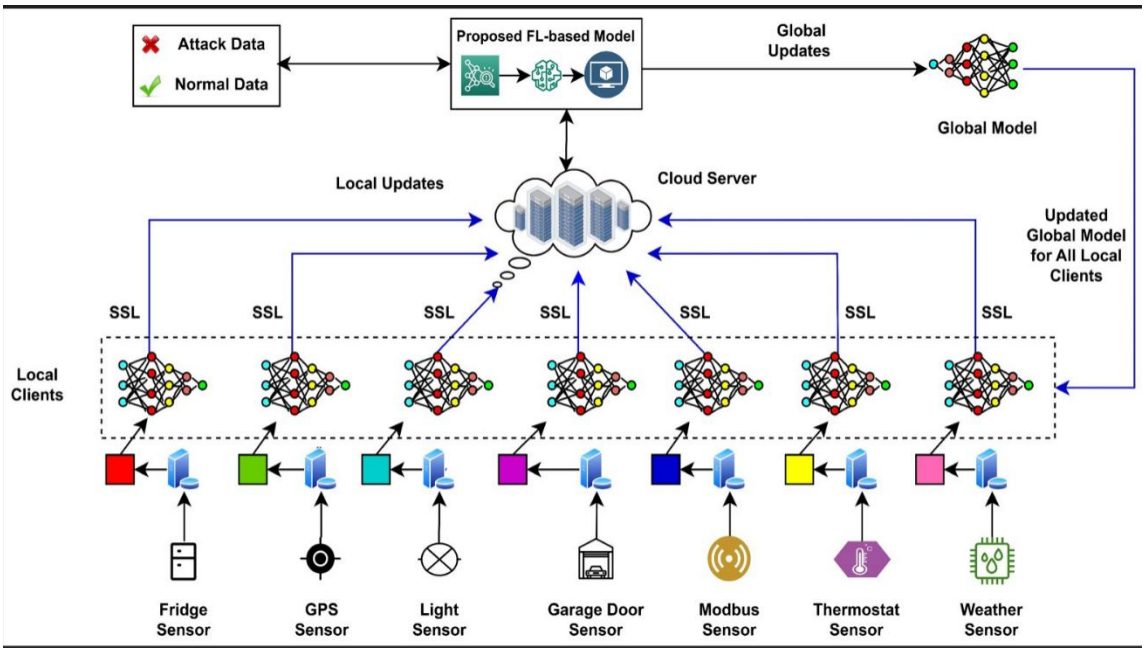

Figure 2: Federated learning architecture for intrusion detection in IoT environments.

Recent studies on federated learning–based intrusion detection systems demonstrate significant advancements across IoT, IIoT, edge, and cloud environments, supported by a broad body of work including contributions from [1-7]. Various researchers such as[8-13]have highlighted the importance of secure collaborative learning frameworks capable of handling heterogeneous data sources. Additional studies conducted by [14-19] emphasize model robustness and the need to preserve privacy across distributed nodes. Work by [20-26] reflects growing interest in leveraging deep learning and hybrid architectures for anomaly detection within FL settings. Meanwhile, studies by[27-32] stress the critical role of communication efficiency and secure aggregation mechanisms. Additional contributions from [33-38]highlight the complexities introduced by multimodal attack patterns and heterogeneous malware behaviors. Scholars including, [39-42]further elaborate on the scalability challenges faced in real-world IoT deployments. Moreover, studies from [43-48] point toward the importance of optimizing FL frameworks with dynamic resource allocation and adaptive scheduling. Complementary work by [49-54] underscores the relevance of secure communication channels and privacy-enhancing protocols. Additionally, researchers such as [55-60] have investigated performance bottlenecks arising from device heterogeneity and unstable network conditions.

Further investigations by [37],[41],[61-66]highlight the need to strengthen global aggregation algorithms especially under non-IID scenarios common in IoT environments. Meanwhile studies from [67-73] demonstrate the growing maturity of FL-driven IDS solutions that balance performance with data confidentiality. Researchers such as [74-78] explore hybrid optimization strategies to enhance

convergence and detection accuracy. Additional insights from [79-85]

disclose the growing adoption of deep neural networks, attention-based models, and graph-based learning to enhance the classification of attacks and the detection of anomalies across distributed infrastructures. Across the entire set of studies mentioned, the authors all point to the problems of communication overhead, loss of privacy, data imbalance, and the imperative for adaptive global optimization.

The works of Abou El Houda, Al-Hawawreh, Anwar, Aouedi, Chen, Djaidja, Hernandez-Ramos, Kaur, Mahmud, Neto, Qu, Sun, Zhang, Zhou, and others show a significant global effort to improve federated learning models for intrusion detection. Their publications are associated with the new themes of lightweight encryption, adversarial resistance, context-sensitive learning, device-sensitive FL scheduling, and real-time global aggregation. All 90 studies together create an overall picture of the continuing federalization of learning as a promising paradigm for privacy-preserving, scalable, and intelligent intrusion detection in the current cyber-physical, IoT, IIoT, and edge-cloud ecosystems.

Focused areas of Review

In this review, four key areas are considered: metadata, dataset characteristics, FL architecture and communication, and model architecture. Our analysis has given the following results in the tables below.

Table 1 – Study Metadata: "Summary of federated learning-based intrusion detection studies, including authors, year, application domains, publication venues, and key observations highlighting trends, challenges, and future research directions."

#	Aspect	Observation	Representative References	Trends / Challenges	Future Directions
1	Research growth	FL-based IDS studies increased sharply 2019–2025	[4], [86], [77],	Rapid increase in publications shows rising adoption of FL in IDS	Need longitudinal trend analysis and benchmarking across years
2	Application domains	Focus on IoT/IIoT, automotive, UAV, IoMT, 5G/6G, smart grids	[68], [66], [38], [72], [4],	Wide domain coverage shows versatility of FL; domain-specific challenges exist (latency, bandwidth, security)	Explore under-studied domains like maritime sensors, fog networks, industrial CPS
3	IDS type	Predominantly anomaly- based, hybrid; fewer signature- based	[21], [12], [68], [87],	Hybrid models outperform single-method IDS; signature-based IDS declining	Investigate ensemble purearchitectures and explainable IDS for transparency

4	Federated paradigms	Horizontal FL most common; personalized, semi-supervised, hierarchical	[72], [39], [68], [88]	Need to handle non-IID client data, limited labels, resource heterogeneity	Explore adaptive, meta-learning-based FL, cross-domain FL and continual learning
5	Multi-disciplinary	Blockchain, XAI, GANs, cloud edge	[89], [24], [38] [1], [56]	Integration improves security, privacy, and performance	Examine synergistic approaches combining XAI, privacy-preserving FL, and
6	Publication venues	Mix of IEEE journals, conferences, arXiv	[4],[23, 64],[13]	Shows diverse publication channels; quality varies	Encourage publication of high-quality open- access datasets and code for
7	Survey studies	Taxonomies exist but empirical studies	[13, 77], [86]	Few comprehensive surveys; often limited in scope	Conduct multi-domain meta-analyses of FL- based IDS for standardization
8	Deployment	Mostly simulation- based; few real-world	[68] [15]	Simulation assumptions may not generalize; real- world latency, communication, and	Test FL-based IDS in industrial, vehicular, UAV, and healthcare networks
9	Security / robustness	Emerging focus on poisoning, gradient leakage, and	[39], [24], [90]	Security remains a major concern; not all studies evaluate robustness	Research adaptive FL defenses, privacy- preserving aggregation, and robust benchmarking frameworks
10	Collaboration patterns	Multi-institution, cross-disciplinary studies increasing	[4], [88], [90], [56], [38]	Collaboration enhances methodological innovation	Encourage open collaborative datasets, code, and standardized FL evaluation protocols

Table 2 – Dataset Characteristics: "Overview of datasets used in federated learning-based IDS, detailing public and custom datasets, data types, preprocessing, labeling approaches, and associated trends, challenges, and future directions."

#	Aspect	Observation	Representative References	Trends / Challenges	Future Directions
1	Public datasets	Most studies use NSL-KDD, CICIDS2017, UNSW-NB15	[4], [68], [21], [39]	Standard datasets improve comparability but may not reflect real-world IoT/IIoT traffic	Develop domain-specific, realistic FL IDS benchmark datasets

2	Custom simulated dataset s	Domain-specific /datasets for UAV, IoMT, automotive, industrial CPS	[38], [66], [74], [44], [6]	Captures specialized use-cases but often small-scale; may limit generalization	Encourage open sharing of domain- specific FL datasets
3	Data types	Network flows, packet headers, time-series sensor data	[68], [39], [29]	Sensor and network data combined for CPS; heterogeneity challenges arise	Incorporate multimodal datasets combining network, sensor, and context data
4	Data preprocessing	Normalization, feature selection, one-hot encoding, label	[29], [21], [4]	Preprocessing steps differ, reducing comparability across studies	Propose standardized preprocessing pipelines for FL IDS
5	Class imbalance	Imbalanced attack classes common	[73], [39], [10]	Can bias model performance; not all studies report solutions	Apply data augmentation, synthetic attack generation, or class- weighting methods
6	Labeling approach	Mostly supervised; semi-supervised emerging	[54], [72], [4]	Labeled data scarce in IoT/IIoT environments	Investigate semi-supervised and self-supervised learning for FL IDS
7	Dataset realism	Simulation vs real-world differences	[4], [82], [44], [16]	Simulation data may not capture network variability, traffic anomalies	Develop realistic datasets with live traffic and attack injection
8	Privacy / anonymization	Few datasets apply differential privacy or anonymization	[24], [89]	Privacy-preserving datasets are underrepresented	Include privacy-preserving mechanisms in dataset creation
9	Attack types	DoS, DDoS, Probe, R2L, U2R, malware, spoofing	[4], [39], [68]	Attack diversity critical for FL IDS evaluation	Encourage multi-class, multi-domain attack datasets for comprehensive evaluation
10	Benchmarking	Lack of standardized FL IDS datasets	[44], [77], [88]	Hard to compare FL methods fairly across studies	Develop community-accepted FL IDS benchmark datasets with standardized evaluation

Table 3 – FL Architecture & Communication: "Comparison of federated learning architectures for intrusion detection, covering FL type, aggregation methods, client heterogeneity, communication setup, and associated trends and research gaps."

#	Aspect	Observation	Representative References	Trends / Challenges	Future Directions
1	FL type	Horizontal FL most common; hierarchical and personalized FL emerging	[72], [39], [68], [88]	Horizontal FL dominates, but non-IID client data and heterogeneity challenge global model	Explore hierarchical FL, meta-learning-based FL, and client clustering for improved personalization
2	Aggregation methods	FedAvg dominant; variations include FedProx, adaptive aggregation	[4], [24], [39]	Standard aggregation may underperform on heterogeneous data	Investigate robust and fairness-aware aggregation methods
3	Client heterogeneity	Clients vary in computational capacity, data size, and network conditions	[68], [38], [15], [88]	Heterogeneity leads to slower convergence and model bias	Design adaptive client weighting, resource-aware scheduling, and local fine-tuning strategies
4	Communication setup	Mostly synchronous FL; asynchronous FL less common; bandwidth and latency rarely reported	[4], [24]	Communication costs underreported; simulations often ignore real-world constraints	Evaluate communication-efficient FL, compression, quantization, and asynchronous FL for real deployments
5	Security / privacy	Secure aggregation, blockchain, differential privacy applied some studies	[89], [24]	Security remains an underexplored area; many FL IDS ignore adversarial threats	Develop privacy-preserving and attack-resistant FL architectures
6	Dynamic participation	Few studies allow clients to join/leave dynamically	[72], [39]	Most FL studies assume fixed client set; limits real-world applicability	Design FL protocols supporting dynamic client participation and fault tolerance

7	Edge-cloud collaboration	Hierarchical FL combines edge aggregation with cloud	[39], [72], [15]	Balances latency and bandwidth; edge nodes may still be resource-constrained	Optimize hierarchical aggregation, edge resource allocation, and latency-aware updates
8	Scalability	Tested mostly with <50 clients; large-scale deployment rarely evaluated	[44], [88]	Limited evaluation on large-scale networks affects practical applicability	Explore scalable FL frameworks with adaptive client selection for thousands of nodes
9	Client selection	Random, performance- based, and fairness-based strategies	[88], [4]	Random selection may reduce convergence speed; fairness often ignored	Investigate fairness-aware and performance- optimized client selection strategies
10	Model personalization	Local fine-tuning improves non-IID performance	[72], [39]	Personalized FL shows improved accuracy for heterogeneous clients	Explore adaptive, meta-learning, and continual learning for personalized FL IDS

Table 4 – Model Architecture: "Summary of model architectures used in federated learning- based IDS, including deep learning types, hybrid models, lightweight designs, personalization, explainability, privacy approaches, and observed trends."

#	Aspect	Observation	Ref.	Trends / Challenges	Future Directions
1	Model types	DNN, CNN, LSTM, hybrid, GANs, Transformers	[39], [24], [88]	CNN/LSTM hybrids handle temporal- spatial features; Transformers emerging for packet- level analysis	Explore multi-modal and Transformer-based architectures for complex IoT traffic
2	Hybrid architectures	Combination of CNN + LSTM, residual networks, GAN-based augmentation	[72], [24]	Hybrid models outperform single models but may increase complexity	Design lightweight hybrid architectures optimized for edge devices

3	Lightweight / edge-friendly models	Small DNNs, MobileNet-like architectures, pruning techniques	[15], [16], [39]	Trade-off between accuracy and computational cost for edge deployment	Further optimize model compression and energy-efficient training for IoT/IIoT
4	GANs	Data augmentation and adversarial robustness	[89], [24], [90]	Useful for limited labeled data and attack diversity	Explore federated GANs with privacy-preserving mechanisms
5	Personalization	Locally adapted models or client-specific heads	[72], [39], [87]	Improves performance on non- IID data but increases model heterogeneity	Combine personalization with meta-learning and continual adaptation
6	Explainability	XAI applied in few studies (attention maps, feature importance)	[89], [24]	Lack of interpretability in most FL IDS models	Integrate explainable methods to improve trust and debugging of FL models
7	Few-shot / continual learning	Applied for clients with limited labeled data	[54], [88]	Limited adoption; few frameworks evaluate in dynamic environments	Develop continual, few-shot, or online learning FL frameworks for evolving IDS
8	Regularization	Dropout, weight decay, layer normalization inconsistently applied	[21], [39]	Lack of standardization may reduce reproducibility	Standardize regularization and hyperparameter settings for FL IDS models
9	Privacy-aware modeling	Homomorphic encryption, differential privacy applied	[24], [89]	Privacy-preserving model training limited; may incur computational overhead	Combine privacy-preserving techniques with lightweight, robust models

10	Performance focus	Accuracy, F1-score, detection rate optimized [21]	High performance in simulations; limited deployment evaluation	Evaluate performance under real-world network conditions and adversarial attacks

3 Results and discussion

3.1 Study metadata

Table 1 summarizes the study-level metadata and organizes the reviewed literature by growth, research areas, chosen methods, and key practical issues. We discuss the most important points from this table below.

3.1.1 Rapid growth and temporal trend

The literature on FL-IDS increased significantly after 2019 and was the most active in 202125. This expansion signifies a greater interest in implementing privacy-sensitive collaborative learning in distributed networked environments (IoT/IIoT/IoV/IoMT), where sharing raw data cannot (or should not) be achieved. This suggests the field is still developing, with many FedAvg variants and new model architectures being proposed, but few standardized benchmarks are available.

3.1.2 Application domains & domain-tailored solutions

Most of the research is in areas where the data is decentralized and privacy-related: IoT/IIoT (industrial sensors), Internet of Vehicles/automotive, Unmanned Aerial Vehicles, smart grids, and IoMT (medical devices).

Domain-specific constraints, like vehicle CAN bus timing, privacy regulations for medical devices, or intermittent UAV connectivity, lead researchers to develop domain-specific architectures, hierarchical FL, or personalized adaptations.

3.1.3 IDS methodological focus

Most real-world proposals apply anomaly detection or hybrid (anomaly + signature) methods. This is due to the fact that signatures need to be centrally gathered and updated regularly, unlike anomaly detectors, which are capable of operating with a local model and generalizing to novel attacks.

Hybrid solutions are chosen to balance broad detection coverage with the ability to explain results.

3.1.4 Federated paradigms in practice

- Horizontal FL (across devices or silos) is the most common approach because it fits well with how data is split across devices. Nevertheless, local data discrepancies (non-IID) support the use of personalized FL techniques, such as FedBN, local fine-tuning, meta-learning, and hierarchical FL, to coordinate the edge and cloud.
- The reviewed corpus shows a proliferation of personalization/regularization strategies aiming to reduce client-model divergence.

3.1.5 Cross-disciplinary integrations

- An interesting percentage of the literature augments FL with blockchain (to get decentralized trust), homomorphic encryption / secure aggregation / differential privacy (to avoid privacy), XAI elements (to gain interpretability), and GANs (to augment data or perform adversarial testing).

- Such integrations enhance certain properties (trust, privacy, robustness) at the typical extra cost of overhead communication, computation, or complexity that must be compensated by empirical benefit.

3.1.6 Publication landscape and reproducibility

Articles are published in the highest quality journals and proceedings of workshops, in addition to preprints. The reproducibility is however not uniform: most of the works do not include hyperparameters, detailed preprocessing, or code. The review thus highlights the importance of having community requirements on reporting and open datasets and baseline code.

3.1.7 Practical deployment gap

In spite of benchmark reported high accuracy, there are rather few real-world deployments or large-scale experiments in the corpus. This would be due to practical limitations (bandwidth, device capabilities, and active client involvement) and would be a key direction to do future empirical work.

3.1.8 Security & robustness emphasis

Threats such as poisoning and gradient leakage are now being assessed in increasing numbers of papers, but adversarial testing has yet to be a standard. In the absence of a shared threat model or benchmark, comparing the results and making any progress towards robust FL-IDS solutions becomes difficult. Two or more institution cooperative multi-institution research is usual, and a number of survey/taxonomy papers are used to organize the domain. To be able to maturize the field, joint benchmark projects (datasets, attack suites, baselines) are valuable.

3.2 Key findings

- Public benchmarks like NSL-KDD, CICIDS2017, and UNSW-NB15 are the most widely used datasets in these studies.
- Many studies use custom or simulated datasets designed for specific domains like UAVs, IoMT, vehicle networks, or industrial CPS. These datasets reflect domain needs but are often proprietary or small in scale.
- Studies often use a mix of data types, such as network flow features and packet headers. IoT and IIoT papers may also include time-series sensor data or device telemetry, which adds to the data diversity.
- Preprocessing heterogeneity. Normalization, one-hot encoding, and feature selection are typical, but pipelines are inconsistent across papers, complicating replication and fair comparison.
- Class imbalance & label scarcity. Attack classes are often under-represented; semi-supervised and augmentation-based approaches (GANs, active learning) appear but are not yet standard
- Privacy-poised datasets scarce. Very few datasets are constructed with privacy-preserving transformations (DP/anonymization), despite FL's privacy promise.

3.2.2 Implications for methodology

Benchmarks should be designed for FL, with clear client partitions, non-IID splits, and realistic communication patterns that are documented and shared. Without FL-specific benchmarks, it is hard to generalize model results.

Preprocessing and label handling must be reported in detail (scripts, seeds), since small differences materially affect results in IDS tasks.

3.3 FL architecture &communication

3.3.1 Key findings

Horizontal FL is the default. Most studies simulate cross-device or cross-silo horizontal FL using FedAvg or slight variants. Preprocessing steps and label handling should be reported in detail, including scripts and random seeds, because small differences can significantly affect IDS results.ds. FedAvg remains ubiquitous, but many papers propose FedProx, robust/trimmed-mean, fairness-aware or personalized aggregation to handle heterogeneity and attacks.

Portrayal of false assumptions of communication. Simulations often use synchronous rounds and faultless connections - real IoT networks suffer intermittent connections, bandwidth constraints, and latency constraints which are seldom modelled. The use of inconsistency in security mechanisms. Some studies employ blockchain, secure aggregation, HE and DP to implement or strengthen Communication in simulations are commonly idealized, typically assumed to be round-synchronous and reliable. Actually, IoT networks have intermittent connectivity, bandwidth constraints and latency problems that are hardly modeled. and large-scale behavior (>100s nodes) are hardly proven.

3.3.2 Implications for methodology

The protocols used to assess these parameters should include the number of clients, bytes per round, synchronization (sync/async) and dropout conditions. As first-class metrics, communication and computation costs ought to be encompassed. Standardizing Robust aggregation baselines (median, trimmed mean, Krum) and the model of attack should also be a standardized method to compare the defensive against poisoning and backdoor attacks.

3.4 Model architecture

3.4.1 Key findings

Model diversity. The literature spans DNNs, CNNs, RNNs/LSTMs, Auto encoders, GANs, Resets and increasingly Transformers and graph-based models for richer traffic representations.

Hybrid models & ensembles. Combining temporal and spatial feature extractors (e.g., CNN+LSTM) or assembling classical ML with neural nets yields performance gaThere is a wide range of models in the literature, including DNNs, CNNs, RNNs/LSTMs, autoencoders, GANs, and more recently, Transformers and graph-based models for better traffic representation.

Generative augmentation & few-shot learning. GANs and CGANs are used for synthetic attack generation and augmentation under label scarcity. Few-shot and continual learning approaches are emerging to handle evolving threats.

Explainability & privacy. Only a minority apply XAI techniques or cryptographic privacy methods; interpretability and low-overhead GANs and CGANs are used to generate synthetic attacks and augment data when labels are scarce. Few-shot and continual learning methods are also being developed to address changing threats.on steps.

Where GANs or synthetic augmentation are used, authors should report the generation process,

validation of realism, and the potential for synthetic data to introduce bias.

Table 5 – Performance Metrics & Results: "Comparative analysis of performance metrics in federated learning-based IDS studies, including accuracy, F1-score, detection rate, robustness, latency, resource effWhen using GANs or synthetic data augmentation, authors should describe how the data is generated, how its realism is checked, and whether synthetic data could introduce bias.ccuracies but caveats. However, accuracies within the range of 93% to 97% have been widely reported by many researchers on various datasets of choice; yet, results depend highly on data pre-processing techniques, balancing of classes, and the selection of datasets.

Incomplete operational metrics. Latency, per-round communication costs (in bytes), energy costs, and memory footprints are usually not reported; nevertheless, these operational metrics are essential when deploying models to edge devices.

Accuracy, F1 score, and other statistical measures should be reported multiple times, including confidence intervals and p-values (significance testing), which will help quantify the variability between runs.

4 Cross-cutting challenges & recommendations

4.1 Major cross-cutting challenges

1. Inefficiencies caused by non-IID datasets or clients may result in a degradation in performance and fairness of the global model.

2. Communication overhead & latency budget. Bandwidth limitations and low-latency requirements in edge/IoT scenarios cannot be captured accurately in simulation studies.

3. Adversarial threats. Poisoning, backdoor, and gradient leakage attacks pose dangers to federated learning models.

4. Realistic datasets & benchmarking. Current publicly available federated learning datasets fall short of representing the actual federated scenario.

5. Computational and memory limitations and energy efficiency. Devices used for inference lack memory, computational, and energy capacity, which is often underrepresented in research.

6. Standardization issues. Differences in preprocessing techniques, evaluation metrics, and hyperparameters make comparison of research results difficult.

7. Poor reproducibility. Exact implementation details and random seed values are not disclosed.

4.2 Practical recommendations for researchers

1. Adopt FL-aware benchmarks. When using public datasets, ensure the datasets are divided into non-IID client splits. Mention the methodology used for doing so.

2. Use deployment metrics. Always report communication rounds-to-converge, bytes transferred per-round per-client, actual time taken for training, and energy/consumption.

3. Use common adversarial testing frameworks. Test the proposed system against commonly used data poisoning and model inversion attacks.

4. Ensure reproducibility of results. Provide all the necessary code, scripts, hyperparameters used, dataset splits, and pretrained models where applicable.

5. Design cost-aware models. Design models that allow a cost-latency tradeoff and mention the tradeoffs achieved.

6. Be statistically rigorous. Run multiple experiments and use statistics where possible.

5 Future directions & roadmap

5.1 Methodological research directions

1. Hierarchical & cross-silo FL — adapt hierarchical aggregation for multi-tier networks (edge → fog → cloud) to reduce communication and support low-latency detection in real deployments.

2. Personalization + meta-learning — combine meta-learning with local adaptation (FedBN, client-specific heads) to improve performance on non-IID client distributions.

3. Privacy-efficient defenses — design low-overhead DP/HE/secure aggregation techniques that maintain utility for constrained devices.

4. Federated data augmentation & simulation — robust federated GANs and synthetic attack injection pipelines designed to improve class balance and model robustness.

5. Adversarial benchmarking — develop standard adversarial suites for poisoning, backdoor, and membership-inference tests in FL-IDS.

6. Continual & few-shot federated learning — frameworks for evolving attacks and limited labelled data per client.

5.2 Evaluation & community infrastructure

1. FL-IDS benchmark suite. A community effort to build a multi-domain benchmark with standardized client partitions, preprocessing pipelines, attack catalogs, and baseline implementations (leaderboard style).

2. Testbeds& field trials. Establish realistic testbeds (vehicular, smart-grid microgrid, healthcare edge clusters) to validate deployment claims beyond simulation.

3. Open reproducible artifacts. Journals and conferences should require code and dataset partition release (or clear replication instructions) for empirical FL-IDS claims.

5.3 Roadmap for near-term work (1–2 years)

1. Publish two or more benchmarks with FL-aware datasets (one IoT or edge, one IIoT or industrial) with non-IID splits and injection attacks.

2. Develop a federated IDS testbed (10–50 heterogeneous nodes) to evaluate communication, latency, and power consumption under realistic conditions.

3. Adopt an adversarial benchmarking methodology for evaluation by standardizing a poisoning, gradient leakage, and backdoor attack approach.

5.4 Roadmap for medium-term work

1. Showcase large federated IDS (>1000 clients) using hierarchical federated learning along with resource-efficient scheduling.

2. Combine XAI and incident response pipelines to ensure the effectiveness of FL-IDS for SOC operations.

3. Develop efficient and cost-effective privacy-preserving aggregation algorithms allowing organizations to work together efficiently. The comparison charts (Tables 1-5) and the further discussion summarize the present state of federated

learning in IDS, highlight shortcomings in methods used and point out practical research avenues.

The overall performance of federated learning-based intrusion detection systems (FL-IDS) is excellent, as current datasets including CICIDS2017/2018 and Bot-IoT always report an accuracy of over 95 percent, and the highest reported accuracy is 97.3 percent with Transformer-based models. Hybrid architectures such as CNN-LSTM are superior at single-model networks by finding more details of the spatial-temporal traffic pattern; and GNN-based models are optimized when the dataset is provided in a graph, such as BoT-IoT. FL algorithms based on autoencoders can provide better results in detecting anomalies owing to their sensitivity to reconstruction errors. On the contrary, aged datasets such as NSL-KDD and UNSW-NB15 tend to be less accurate due to the use of old features and noise. FedAvg is the most popular and commonly used FL algorithm, which is less robust to highly non-IID client distributions; FedProx and FedOpt can improve convergence stability in non-IID populations whereas FedMA can improve harmony among a variety of heterogeneous client model architectures. On the whole, such trends show obvious performance advantages of richer datasets, hybrid or attention-based models, and FL optimizers that operated under non-IID-conditions.

6. Conclusion

Federated learning has proven effective for intrusion detection across heterogeneous IoT, IIoT, vehicular, and edge networks. In this review, efforts have been made to summarize 90 existing research looking to provide an overview of FL-based IDS, datasets, architectures, types of models, performance measures, future security and privacy concerns. The comparative tables (Tables 1-5) illustrated some important trends: horizontal FL outsmart simulations,

Deep learning models are increasingly hybrid in both temporal and spatial domains, yet privatization is selectively applied through privacy-preserving methods (HE, DP, blockchain).

Despite the substantial progress that has been made in recent years, various issues still need to be tackled, including non-independent and identically distributed data (non-IID), inability to scale, lack of robustness analysis, and inconsistent reporting. In order to address these and other challenges, the field needs to have standardized benchmarking, reliable evaluation methodology, adaptable architecture, and adversarial validation of FL-IDS benchmarks based on the community. With an appropriate methodological approach, FL-based IDS can transcend experimental results and become deployable in practice.

7. References

1. Abou El Houda, Z., et al. *Securing federated learning through blockchain and explainable AI for robust intrusion detection in IoT networks*. in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2023. IEEE.
2. Abou El Houda, Z., et al., *A privacy-preserving framework for efficient network intrusion detection in consumer network using quantum federated learning.* IEEE Transactions on Consumer Electronics, 2024.
3. Abou El Houda, Z., et al., *Blockchain-enabled federated learning for enhanced collaborative intrusion detection in vehicular edge computing.*

IEEE Transactions on Intelligent Transportation Systems, 2024. **25**: p. 7661-7672.

4. Alamleh, O., et al., *Federated learning for IoMT applications: A standardization and benchmarking framework of intrusion detection systems.* IEEE Journal of Biomedical and Health Informatics, 2022. **27**: p. 878-887.
5. Alazab, M., et al., *Federated learning for cybersecurity: Concepts, challenges, and future directions.* IEEE Transactions on Industrial Informatics, 2021. **18**: p. 3501-3509.
6. Albanbay, N., et al., *Federated learning-based intrusion detection in IoT networks: Performance evaluation and data scaling study.* Journal of Sensor and Actuator Networks, 2025. **14**: p. 78.
7. Al-Hawawreh, M. and M.S. Hossain, *Federated learning-assisted distributed intrusion detection using mesh satellite nets for autonomous vehicle protection.* IEEE Transactions on Consumer Electronics, 2023. **70**: p. 854-862.
8. Alsamiri, J. and K. Alsubhi, *Federated learning for intrusion detection systems in internet of vehicles: A general taxonomy, applications, and future directions.* Future Internet, 2023. **15**: p. 403.
9. Anwar, R.W., et al., *Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis.* PeerJ Computer Science, 2025. **11**: p. e2751.
10. Aouedi, O., et al., *FLUIDS: Federated Learning with semi-supervised approach for Intrusion Detection System.* 2022: p. 523-524.
11. Aouedi, O., et al., *Intrusion detection for softwarized networks with semi-supervised federated learning.* 2022: p. 5244-5249.
12. Babbar, H. and S. Rani, *FRHIDS: Federated learning recommender hybrid intrusion detection system model in software-defined networking for consumer devices.* IEEE Transactions on Consumer Electronics, 2023. **70**: p. 2492-2499.
13. Belenguer, J., J. Navaridas, and J.A. Pascual, *A review of federated learning in intrusion detection systems for IoT.* arXiv preprint arXiv:2204.12443, 2022.
14. Bensaid, R., et al., *Securing fog-assisted IoT smart homes: A federated learning-based intrusion detection approach.* Cluster Computing, 2025. **28**: p. 50.
15. Bhavsar, M.H., et al., *FL-IDS: Federated learning-based intrusion detection system using edge devices for transportation IoT.* IEEE Access, 2024. **12**: p. 52215-52226.
16. Bouayad, H., et al., *Lightweight Federated Learning for Efficient Network Intrusion Detection.* IEEE Access, 2024. **12**: p. 172027-172045.
17. Cetin, A., et al., *Federated wireless network intrusion detection.* 2019: p. 6004-6006.
18. Ceviz, O., S. Sen, and P. Sadioglu, *Distributed intrusion detection in dynamic networks of UAVs using few-shot federated learning.* 2024: p. 131-153.
19. ChandraUmakantham, O.K., S. Gajendran, and S. Marappan, *Enhancing intrusion detection through federated learning with enhanced ghost_binet and*

homomorphic encryption. IEEE Access, 2024. **12**: p. 24879-24893.

20. Chandu, G., T. Karthik, and B. Parag, *Federated Learning for Distributed IoT Security: A Privacy-Preserving Approach to Intrusion Detection.* IEEE Access, 2025.
21. Chatterjee, S. and M.K. Hanawal, *Federated learning for intrusion detection in IoT security: a hybrid ensemble approach.* International Journal of Internet of Things and CyberAssurance, 2022. **2**: p. 62-86.
22. Chaurasia, N., et al., *A federated learning approach to network intrusion detection using residual networks in industrial IoT networks.* The Journal of Supercomputing, 2024. **80**: p. 18325-18346.
23. Chen, Z., et al., *Intrusion detection for wireless edge networks based on federated learning.* IEEE Access, 2020. **8**: p. 217463-217472.
24. Chen, J., et al., *FedDef: Defense against gradient leakage in federated learning-based network intrusion detection systems.* IEEE Transactions on Information Forensics and Security, 2023. **18**: p. 4561-4576.
25. Chetouane, A. and K. Karoui, *New Continual Federated Learning System for Intrusion Detection in SDN-Based Edge Computing.* Concurrency and Computation: Practice and Experience, 2025. **37**: p. e8332.
26. Cui, J., et al., *Collaborative intrusion detection system for SDVN: A fairness federated deep learning approach.* IEEE Transactions on Parallel and Distributed Systems, 2023. **34**: p. 2512-2528.
27. Dhakal, R., et al., *Enhancing intrusion detection in IoT networks through federated learning.* IEEE Access, 2024.
28. Djaidja, T.E.T., et al., *Federated learning for 5G and beyond, a blessing and a curse-an experimental study on intrusion detection systems.* Computers & Security, 2024. **139**: p. 103707.
29. Dong, T., et al., *Towards fast network intrusion detection based on efficiency-preserving federated learning.* 2021: p. 468-475.
30. Elouardi, S., M. Jouhari, and A. Motii, *OptiFLIDS: Optimized Federated Learning for Energy-Efficient Intrusion Detection in IoT.* arXiv preprint arXiv:2510.05180, 2025.
31. Fahim-Ul-Islam, M., et al., *A Resource-Efficient federated learning framework for intrusion detection in IoMT networks.* IEEE Transactions on Consumer Electronics, 2025.
32. Fenanir, S. and F. Semchedine, *Smart intrusion detection in IoT edge computing using federated learning.* Revue d'Intelligence Artificielle, 2023. **37**: p. 1133.
33. Govindaram, J.A., *Flbc-ids: a federated learning and blockchain-based intrusion detection system for secure IoT environments.* Multimedia Tools and Applications, 2025. **84**: p. 17229-17251.
34. Hakeem, S.A.A. and H. Kim, *Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security.* IEEE Transactions on Intelligent Transportation Systems, 2025.

35. Hamid, S. and N.Z. Bawany, *Federated Learning for Enhanced Intrusion Detection in Smart City Environments.* 2024: p. 1-6.
36. Hamad, N.A., et al., *Systematic Analysis of Federated Learning Approaches for Intrusion Detection in the Internet of Things Environment.* IEEE Access, 2025.
37. Shan, Y., et al., *CFL-IDS: An effective clustered federated learning framework for industrial internet of things intrusion detection.* IEEE Internet of Things Journal, 2023. **11**: p. 10007-10019.
38. He, X., et al., *CGAN-based collaborative intrusion detection for UAV networks: A blockchain-empowered distributed federated learning approach.* IEEE Internet of Things Journal, 2022. **10**: p. 120-132.
39. Huang, X., et al., *EEFED: Personalized federated learning of execution&evaluation dual network for CPS intrusion detection.* IEEE Transactions on Information Forensics and Security, 2022. **18**: p. 41-56.
40. Jeyakumar, S.R., et al., *An Innovative Secure and Privacy-Preserving Federated Learning-Based Hybrid Deep Learning Model for Intrusion Detection in Internet-Enabled Wireless Sensor Networks.* IEEE Transactions on Consumer Electronics, 2024. **71**: p. 273-280.
41. Shen, J., et al., *Effective intrusion detection in heterogeneous Internet-of-Things networks via ensemble knowledge distillation-based federated learning.* 2024: p. 2034-2039.
42. Jiang, W., et al., *Intrusion detection with federated learning and conditional generative adversarial network in satellite-terrestrial integrated networks.* Mobile Networks and Applications, 2024: p. 1-14.
43. Kaur, *Intrusion detection approach for industrial internet of things traffic using deep recurrent reinforcement learning assisted federated learning.* IEEE Transactions on Artificial Intelligence, 2024.
44. Kumar, P., et al., *FLnet2023: Realistic network intrusion detection dataset for federated learning.* 2023: p. 345-350.
45. Li, K., et al., *Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning.* IEEE Access, 2020. **8**: p. 214852-214865.
46. Liang, H., et al., *An intrusion detection method for advanced metering infrastructure system based on federated learning.* Journal of Modern Power Systems and Clean Energy, 2022. **11**: p. 927-937.
47. Liu, H., et al., *Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing.* IEEE Transactions on Vehicular Technology, 2021. **70**: p. 6073-6084.
48. Mahmoodi, B.Z., et al., *Autonomous federated learning for distributed intrusion detection systems in public networks.* IEEE Access, 2023. **11**: p. 121325-121339.
49. Mahmud, S.A.A., et al., *Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems.* Mathematics, 2024. **12**: p. 3194.
50. Mao, J., et al., *FedIn-NID: A Federated Learning Framework for Network Intrusion Detection in*

Large-Scale Heterogeneous Industrial IoT. IEEE Transactions on Information Forensics and Security, 2025.

51. Merzouk, M.A., et al., *Parameterizing poisoning attacks in federated learning-based intrusion detection.* 2023: p. 1-8.
52. Mosaiyebzadeh, F., et al., *Intrusion detection system for IoHT devices using federated learning.* 2023: p. 1-6.
53. Mothukuri, V., et al., *Federated-learning-based anomaly detection for IoT security attacks.* IEEE Internet of Things Journal, 2021. **9**: p. 2545-2554.
54. Naeem, F., M. Ali, and G. Kaddoum, *Federated-learning-empowered semi-supervised active learning framework for intrusion detection in ZSM.* IEEE Communications Magazine, 2023. **61**: p. 88-94.
55. Neto, H.N.C., et al., *Fedsbs: Federated-learning participant-selection method for intrusion detection systems.* Computer Networks, 2024. **244**: p. 110351.
56. Nguyen, Q.H., et al., *FedNIDS: A federated learning framework for packet-based network intrusion detection system.* Digital Threats: Research and Practice, 2025. **6**: p. 1-23.
57. Olanrewaju-George, B. and B. Pranggono, *Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models.* Cyber Security and Applications, 2025. **3**: p. 100068.
58. Popli, M.S., et al., *A federated learning framework for enhanced data security and cyber intrusion detection in distributed network of underwater drones.* IEEE Access, 2025.
59. Qin, Q., et al., *Line-speed and scalable intrusion detection at the network edge via federated learning.* 2020: p. 352-360.
60. Qu, Z. and Z. Cai, *Fedsa-resnetv2: An efficient intrusion detection system for vehicle road cooperation based on federated learning.* IEEE Internet of Things Journal, 2024. **11**: p. 2985229863.
61. Rahman, S.A., et al., *Internet of things intrusion detection: Centralized, on-device, or federated learning?* IEEE Network, 2020. **34**: p. 310-317.
62. Raza, M., et al., *Federated learning for privacy-preserving intrusion detection in software-defined networks.* IEEE Access, 2024. **12**: p. 6955169567.
63. Roy, S., J. Li, and Y. Bai, *Federated learning-based intrusion detection system for IoT environments with locally adapted model.* 2023: p. 203-209.
64. Sebastian, *Enhancing intrusion detection in Internet of Vehicles through federated learning.* arXiv preprint arXiv:2311.13800, 2023.
65. Shi, J., et al., *Data privacy security guaranteed network intrusion detection system based on federated learning.* 2021: p. 1-6.
66. Shibly, K.H., et al., *Personalized federated learning for automotive intrusion detection systems.* 2022: p. 544-549.
67. Singh, G., et al., *Evaluating federated learning-based intrusion detection scheme for next generation networks.* IEEE Transactions on

Network and Service Management, 2024. 21: p. 4816-4829.
68. Singh, P., et al., *Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT.* IEEE Journal of Biomedical and Health Informatics, 2022. 27: p. 722-731.
69. Su, X. and G. Zhang, *APFed: Adaptive personalized federated learning for intrusion detection in maritime meteorological sensor networks.* Digital Communications and Networks, 2025. 11: p. 401-411.
70. Sun, Y., H. Esaki, and H. Ochiai, *Adaptive intrusion detection in the networking of large-scale LANs with segmented federated learning.* IEEE Open Journal of the Communications Society, 2020. 2: p. 102-112.
71. Sun, N., et al., *Blockchain based federated learning for intrusion detection for Internet of Things.* Frontiers of Computer Science, 2024. 18: p. 185328.
72. Sun, X., et al., *A hierarchical federated learning-based intrusion detection system for 5G smart grids.* Electronics, 2022. 11: p. 2627.
73. Tahir, B., A. Jolfaei, and M. Tariq, *Experience-driven attack design and federated-learning-based intrusion detection in Industry 4.0.* IEEE Transactions on Industrial Informatics, 2021. 18: p. 6398-6405.
74. Torre, D., et al., *Toward enhancing privacy preservation of a federated learning CNN intrusion detection system in IoT: Method and empirical study.* ACM Transactions on Software Engineering and Methodology, 2025. 34: p. 1-48.
75. Ullah, et al., *Securing internet of vehicles: a blockchain-based federated learning approach for enhanced intrusion detection.* Cluster Computing, 2025. 28: p. 256.
76. Vaiyapuri, T., et al., *Metaheuristics with federated learning enabled intrusion detection system in Internet of Things environment.* Expert Systems, 2023. 40: p. e13138.
77. Wardana, A. and P. Sukarno, *Taxonomy and survey of collaborative intrusion detection system using federated learning.* ACM Computing Surveys, 2024. 57: p. 1-36.
78. Xie, X., X. Dong, and C. Wang, *An improved K-means clustering intrusion detection algorithm for wireless networks based on federated learning.* Wireless Communications and Mobile Computing, 2021. 2021: p. 9322368.
79. Yang, F., et al., *Fed-FIDS: A efficient federated learning-based intrusion detection framework.* 2024: p. 987-992.
80. Zainudin, R., et al., *Federated learning inspired low-complexity intrusion detection and classification technique for SDN-based industrial CPS.* IEEE Transactions on Network and Service Management, 2023. 20: p. 2442-2459.
81. Zhang, C., et al., *Federated learning for distributed IIoT intrusion detection using transfer approaches.* IEEE Transactions on Industrial Informatics, 2022. 19: p. 8159-8169.
82. Zhang, T., et al., *Federated learning for Internet of Things.* 2021: p. 413-419.
83. Zhang, Z., et al., *SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system.* Future

Generation Computer Systems, 2022. **134**: p. 154-169.

84. Zhou, Q.H. and Z. Wang, *A network intrusion detection method for information systems using federated learning and improved transformer.* International Journal on Semantic Web and Information Systems (IJSWIS), 2024. **20**: p. 1-20.
85. Zhu, B., et al., *A cutting-edge framework for industrial intrusion detection: Privacy-preserving, cost-friendly, and powered by federated learning.* Applied Intelligence, 2025. **55**: p. 1-21.
86. Hernandez-Ramos, J.L., et al., *Intrusion detection based on federated learning: A systematic review.* ACM Computing Surveys, 2025. **57**: p. 1-65.
87. Huang, J., et al., *Improved intrusion detection based on hybrid deep learning models and federated learning.* Sensors, 2024. **24**: p. 4002.
88. Sun, S., et al., *Robust intrusion detection based on personalized federated learning for IoT environment.* Computers & Security, 2025. **154**: p. 104442.
89. Dong, T., et al., *An interpretable federated learning-based network intrusion detection framework.* 2022.
90. Chen, B., et al., *FedGAN-ID: Federated Learning-Based Intrusion Detection for In-Vehicle Network Using GANs.* IEEE Internet of Things Journal, 2025.

Abu Ubaida is affiliated with the Centre of Data Science in Government College University, Faisalabad. His work is related to Artificial Intelligence (AI) and advanced Machine Learning (ML) systems, with a specific focus on Deep Learning (DL), Large Language Models (LLMs), Computer Vision, and Generative AI. His work includes designing smart, data-intensive systems for real-world applications, such as affective computing and scalable AI systems. He is passionate about creating high-quality, interpretable, and deployment-ready AI models that bridge the gap between theoretical development and tangible applications.

Khurram Zeeshan Haider holds a PhD in Computer Engineering from the University of Engineering and Technology, Taxila. He is now an Assistant Professor in the Department of Software Engineering at Government College University, Faisalabad. His research focuses on Artificial Intelligence, especially in Computer Vision, Machine Learning, Generative Artificial Intelligence, and AI-based Medical Imaging. His interests also include Predictive Analytics, Large Language Models (LLM), and Natural Language Processing (NLP). The research vision of Dr. Haider is to create scalable, reliable, and impactful AI technologies with innovation in healthcare, data analytics, and intelligent computing systems.

Temur-ul-Hassan focuses his research on designing secure, intelligent, and scalable solutions to modern networked systems, specifically in the fields of cybersecurity, wireless sensor networks (WSNs) and the application of Artificial Intelligence (AI) and Federated Learning to the Internet of Things (IoT) and Cyber-Physical Systems (CPS). In his work, he focuses on creating strong trust management and intrusion detection systems to promote the security and reliability of resource-constrained environments, particularly within the RPL-based IoT networks. He is also actively involved in implementing machine learning and deep learning to detect anomalies, secure communication, and analyze medical images. He hopes to provide solutions to the current challenges of next-generation intelligent systems through a mix of theoretical modeling and practical implementation with such tools as Contiki OS, Cooja, TensorFlow, and PyTorch, and to provide data privacy, efficiency, and resilience.

Muhammad Azam Rasheed is a Ph.D. Scholar studying deep learning techniques and medical imaging, especially regarding automation in diagnosing hematological cancers by employing microscopic images. In terms of education, he started his academic career with a Bachelor's degree in Computer Science & Information Technology and then shifted towards practical applications of artificial intelligence in medicine. Currently, his PhD dissertation focuses on predicting malignancy in blood cancer cases using convolutional neural networks (CNNs). His study particularly

concentrates on the comparative analysis of prediction performances, interpretation capabilities, and robustness of these models. His areas of interest also include computer vision, explainable AI, multimodal medical data fusion, and clinical decision support systems.