Federated Learning for Low-rate DDoS Detection in Multi-controller Software Defined Networks: A Meta Analysis

Rikie Kartadie[1,2], Eko Marpanaji[1], and Agus Maman Abadi[1]

[1]*Universitas Negeri Yogyakarta, Indonesia,*
[2]*Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia*

https://doi.org/10.26636/jtit.2026.2.2552

Abstract — Multi-controller SDN environments suffer from a blind spot when it comes to detecting low-rate DDoS attacks. Each controller sees only its own traffic slice, meaning that an LDDoS campaign looking, at every controller, like background noise is still capable of draining the network. Federated learning (FL) is a reasonable answer to this challenge, due to such controllers sharing model updates rather than raw logs. However, the published literature on FL-based detection is fragmented enough that the results have not been systematically compared up to date. We analyze 39 papers published between 2020 and 2026. 35 of those reported quantitative results, with the pooled mean detection precision equaling 98.25% (SD ±0.91) and the mean F1 score amounting to 97.98% (SD ±1.10). Federated models averaged an accuracy score of 98.33%, compared to 98.06% for centralized approaches – a 0.27 pp gap that is practically negligible. LSTM and hybrid CNN + RNN architectures ranked the highest in terms of the most metrics. Four aggregation strategies were mentioned repeatedly: weighted aggregation, asynchronous FL, personalized FL, and standard FedAvg. The widest gap we identified was in the datasets. No available benchmark simultaneously models multi-controller SDN topology, low-rate attack patterns, and heterogeneous traffic distributions across various controllers. Until that changes, high-accuracy scores on CICIDS2017 or CICDDoS2019 should be interpreted with some caution.

Keywords — federated learning, intrusion detection systems, low-rate distributed denial-of-service, SDN security, software-defined networking

1. Introduction

Software-defined networking (SDN) has changed the way in which large-scale networks are managed. By separating the control plane from the data plane, SDN allows operators to configure routing, security policies, and traffic engineering from a central point, rather than by adopting the device-by-device approach. In cloud and IoT deployments, this matters greatly, as networks are too large and too dynamic for per-device management to be deployed at scale.

Many production SDN deployments now run multiple controllers rather than one instance only, thus distributing the control workload geographically and improving fault tolerance. However, such a design choice creates a security problem that has received less attention than it actually deserves [1], [2].

Low-rate distributed denial of service attacks (LDDoS) is the main problem here. A volumetric DDoS is easy to notice. As traffic volume spikes, the anomaly detectors are triggered. LDDoS works in the opposite manner. It sends short, periodic bursts timed to match TCP retransmission timeouts, gradually draining the target's capacity to serve legitimate requests.

No obvious spikes are identified. In a multi-controller SDN environment, the situation is even worse, as each controller observes only the traffic in its own domain. An LDDoS attack targeting the entire network may appear as a hardly noticeable background fluctuation for any single controller [3]–[5].

Federated learning (FL) addresses part of this problem. Controllers can train local detection models and share only model parameters, not raw traffic logs. This preserves privacy in administrative domains and makes collaborative detection feasible without centralizing sensitive network data [6], [7]. The catch is that the amount of literature on FL-based intrusion detection has been growing faster than the community's ability to compare the results of specific studies. Different articles use different architectures, aggregation protocols, and various datasets. Nobody has pooled the numbers.

This paper does that. We reviewed 39 studies published between 2020 and 2026, extracted performance metrics from the 35 that reported quantitative results, and calculated pooled statistics across architecture groups and learning paradigms. Four questions define the scope of the analysis.

1) Which deep learning architectures produce the highest pooled detection performance for LDDoS in federated SDN environments?
2) How do FL aggregation strategies handle data heterogeneity when traffic distributions differ between controllers?
3) What does the quantitative performance gap between federated and centralized detection actually look like?
4) Do the benchmark datasets used in this literature adequately represent LDDoS conditions in multi-controller SDN deployments?

Tab. 1. PRISMA-aligned study selection process.

Stage	Records, N	Decision criteria
Initial identification (keyword search)	187	Terms: federated learning, SDN, DDoS, intrusion detection, LDDoS
After duplicate removal	141	Cross database deduplication (IEEE Xplore, ACM DL, Springer, Scopus)
After title/abstract screening	73	Excluded: unrelated to FL or SDN security ($n = 68$)
After full-text eligibility assessment	39	Excluded: no quantitative results, purely theoretical, non-SDN environment ($n = 34$)
Included in meta-analysis	39	Satisfied all inclusion criteria; 35 empirical + 4 survey/review

Note: Record counts reflect the complete screening process from initial identification to final inclusion.

1.1. Research Design

This study uses a systematic meta-analysis research design following evidence synthesis procedures adapted from preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines, commonly adopted in computer science research [8]. The methodology combines systematic literature identification with quantitative cross-study synthesis, producing pooled descriptive statistics, group-level comparisons, and dataset coverage analysis.

Four databases were searched: IEEE Xplore, ACM Digital Library, Springer, and Scopus. The searches targeted titles, abstracts, and author provided keywords, and were limited to publications from January 2020 to March 2026. The following Boolean string was applied consistently across all databases:

```
("federated learning" OR "federated deep learning"
OR "FL") AND ("software-defined network*" OR
"SDN") AND ("intrusion detection" OR "IDS" OR
"attack detection") AND ("DDoS" OR "LDDoS" OR
"low-rate DDoS" OR "low-rate distributed denial of
service").
```

The wildcard operator (*) was used where a given database supported it in order to capture morphological variants such as networks and networking. Table 1 shows how the records were filtered at each stage.

Studies were included if they proposed or evaluated an FL-based IDS, targeted DDoS or LDDoS detection in an SDN or SDN-enabled environment, reported quantitative experimental results, and provided enough methodological detail to extract the model architecture and aggregation mechanism. Papers that were purely theoretical, lacked experimental evaluation, or operated in non-SDN contexts were excluded.

The selection process comprised four steps:

1) First, we identified publications using keywords related to learning.
2) Then we removed duplicates.
3) Next, we checked the titles and abstracts.
4) Finally, we assessed the text for eligibility.

Table 1 shows how many records were left at each stage following the PRISMA guidelines. The framework diagram is presented in Fig. 1.

1.2. Data Extraction and Analytical Procedure

For each included study, we extracted seven categories of information: publication location and year, network environment (SDN, SDN-IoT, telecom), deep learning architecture, federated learning aggregation mechanism, data set used for evaluation, reported detection metrics (accuracy, precision, recall, F1 score) and, where available, system efficiency indicators such as model size or convergence time.

Accuracy values stated as percentages were converted to decimal form for consistency. Where a study did not report a metric, the value was recorded as "–" rather than estimated. No imputation was applied.

The analysis was carried out in three steps. First, we computed pooled descriptive statistics, mean, standard deviation, minimum, and maximum values across all 35 empirical studies for precision, recall, and F1 score. Second, we grouped the studies by architecture type and by learning paradigm (federated vs. centralized) to identify systematic performance differences. Third, we assessed how well the benchmark datasets used in these studies actually reflect LDDoS conditions in multi-controller SDN environments, using three criteria: presence of low-rate attack patterns, simulation of multi-controller topology, and heterogeneity of traffic across controllers.

Because the reviewed studies use different data sets and evaluation setups, the synthesis is of the descriptive nature. Statistical pooling across incompatible experimental designs would not be meaningful.

2. Results

2.1. Deep Learning Architectures for LDDoS Detection

Analysis of the 35 empirical studies reporting quantitative results produced the combined descriptive statistics shown in Tab. 2.

In all studies, the pooled mean detection precision was 98.25% (SD = ±0.91; range: 96.40 – 99.93%), the mean precision was 97.96% (SD = ±0.94%), the mean recall was 98.21% (SD = ±0.89%), and the mean F1 score was 97.98% (SD = ±1.10%; range: 94.21 – 99.96%).

Recurrent architectures, particularly LSTM and Bi-LSTM, are the most frequently adopted models appearing in approx-

Tab. 2. Pooled performance statistics for all empirical studies (N = 35).

Metric	No. of studies	Mean [%]	Std Dev [±]	Min [%]	Max [%]
Accuracy	35	98.25	0.91	96.40	99.93
Precision	35	97.96	0.94	96.00	99.96
Recall	35	98.21	0.89	96.70	99.97
F1 score	35	97.98	1.10	94.21	99.96

Note: Excludes 4 survey/review studies that did not report original quantitative results.

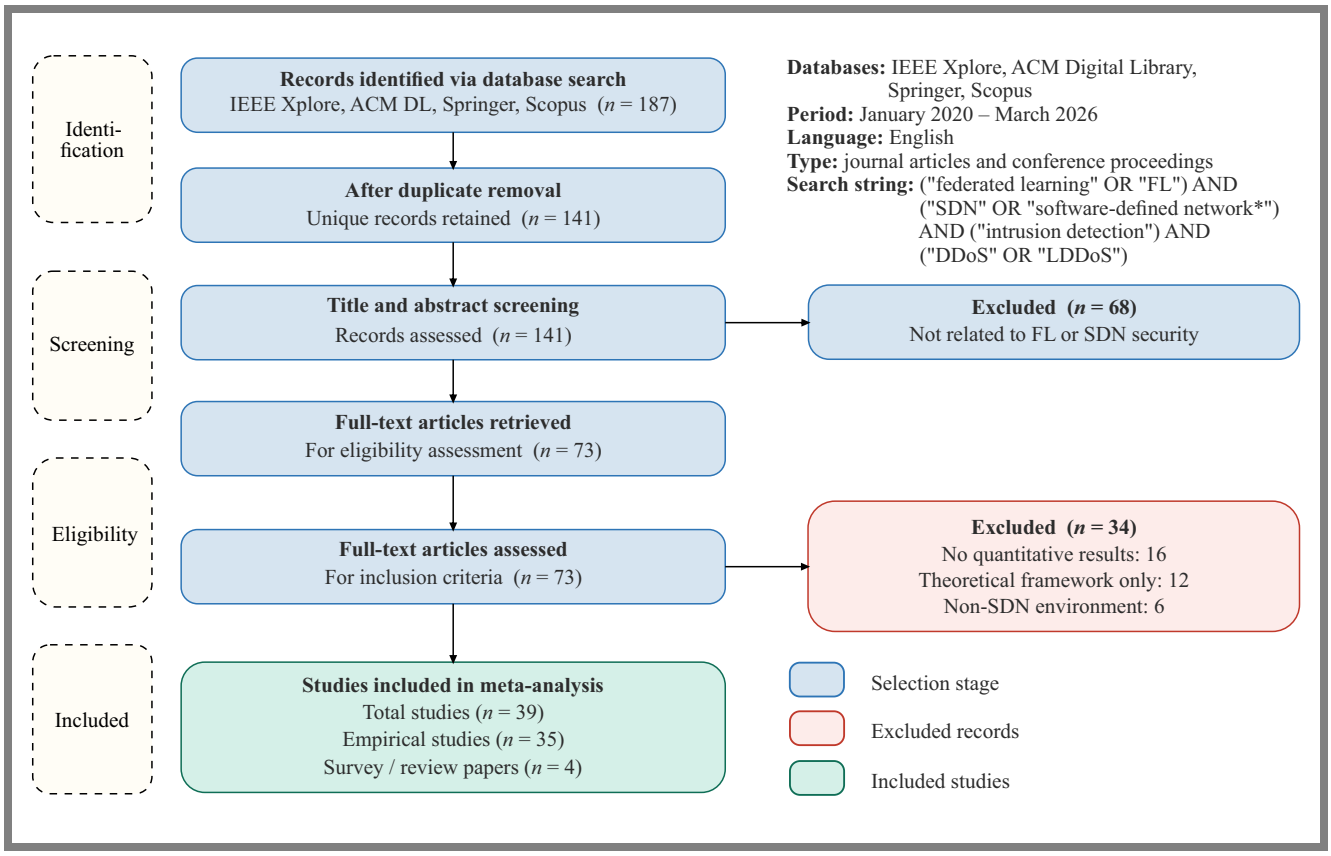

Fig. 1. Prisma framework diagram.

imately 20% of empirical studies (n = 7 of 35; see Tab. 3). This adoption pattern is consistent with the temporal nature of LDDoS attacks which exploit periodic traffic bursts rather than volumetric anomalies, requiring models capable of capturing sequential dependencies. Table 3 presents group-level performance comparisons disaggregated by architecture type.

The hybrid CNN + RRN architectures achieved the highest mean F1 score of 98.54% (±0.67; Tab. 3), followed by the LSTM / Bi-LSTM models at a mean F1 score of 97.89% (±1.55; Tab. 3). CNN-only architectures showed strong classification accuracy (mean: 99.23%) but a lower mean F1 score of 98.59%, which is consistent with prior findings according to which purely spatial models are less effective in detecting stealthy temporal attack patterns.

Graph neural network (GNN) architectures, represented by two studies, demonstrated a mean accuracy of 97.75% with a mean F1 of 97.70%, suggesting promising but early-stage applicability. Transformer-based architectures reported in [9] achieved accuracy of 99.50% and a 99.40% F1 score, indicating a strong potential to capture long-range temporal dependencies in LDDoS traffic.

2.2. Federated Learning Strategies for Handling Data Heterogeneity

The reviewed works report four primary federated learning strategies to mitigate heterogeneous traffic distributions across SDN controllers:

1) weighted aggregation,
2) asynchronous federated learning,
3) FL customized / entire FL,
4) standard FedAvg.

Weighted aggregation strategies, which dynamically adjust the contribution of model updates from individual controllers, are reported in approximately 31% of FL-based studies ($n \approx$ 9 studies). The authors of [10] demonstrated that an asynchronous FL framework (AsyncFL-bLAM) with Bi-LSTM and an attention mechanism achieved a mean F1 score on CAIDA LDDoS data, specifically addressing the synchronization delay problem in multi-controller SDNs. Work [11] showed that the adaptive FLAD framework converges significantly faster than the standard FedAvg, while achieving a 97.01% F1 score. Personalized strategies reported in [12] achieved a 98.82% F1 score on CICDoS2017 / CICDDoS2019 with asynchronous aggregation in a multi-controller SDN scenario.

2.3. Performance Trade-offs Between Federated and Centralized Detection

Table 4 presents a quantitative comparison between federated and centralized learning approaches described in the 35 studies that clearly specified their learning paradigm.

FL-based systems achieved a mean precision of 98.33% (SD = ±0.86) and a mean F1 score of 97.98% (SD = ±1.16), compared to 98.06% (SD = ±0.99) and 97.97% (SD = ±0.97) for centralized approaches. The 0.27% accuracy gap sug-

Tab. 3. Performance comparison by the deep learning architecture group.

Architecture group	No. of studies	Mean acc [±SD, %]	Min acc [%]	Mean F1 [±SD, %]	Min F1 [%]	Primary dataset
LSTM / Bi-LSTM	7	98.63 (±0.36)	97.8	97.89 (±1.55)	94.21	CAIDA, CICDDoS, Edge-IIoT
GRU / Bi-GRU	2	99.15 (±0.35)	98.8	98.55 (±0.85)	97.70	InSDN, CICDDoS2019
CNN (1D / 2D)	4	98.92 (±0.66)	97.8	98.76 (±0.62)	97.70	CICIDS2017, CICDDoS2019
Hybrid CNN+RNN	7	98.68 (±0.61)	98.1	98.54 (±0.67)	97.95	CICIDS2017, CICDDoS2019
Transformer-based	1	99.50 (±–)	99.5	99.40 (±–)	99.40	CICDDoS2019
Graph neural networks	2	97.75 (±0.15)	97.6	97.70 (±0.10)	97.60	CICIDS2017, InSDN
Other FL models	5	97.86 (±0.63)	96.8	97.61 (±0.59)	96.80	CAIDA, CICIDS2017

Note: Studies may appear in multiple architecture groups where hybrid models are employed. SD = standard deviation. "–" indicates a single study group (SD not computable).

Tab. 4. Quantitative comparison: federated learning versus centralized learning.

Approach	No. of studies	Mean acc [±SD,%]	Min acc [%]	Mean F1 [±SD,%]	Min F1 [%]
Federated learning	24	98.33 (±0.86)	96.8	97.98 (±1.16)	94.21
Centralized learning	11	98.06 (±0.99)	96.4	97.97 (±0.97)	96.4

Note: Studies classified as FL involve at least one FL aggregation mechanism across distributed clients. Centralized studies are trained on aggregated data sets without FL.

gests that FL achieves performance comparable to centralized training while preserving data privacy across SDN controller domains. However, federated approaches introduce additional communication overhead from model parameter exchange. The authors of [3] directly compared federated and centralized IDS in the InSDN dataset, reporting that the federated model (98.80% accuracy) closely approached centralized performance (99.10%), with a gap of only 0.30 percentage points.

2.4. How Well Do Benchmark Datasets Represent Real Life?

Table 5 shows the types of benchmark data sets that were used in the studies we analyzed. It also shows how well these datasets represent real-life LDDoS detection scenarios in multi-controller SDN environments.

Table 6 provides a structured overview of all 39 studies included in this meta-analysis. For each study, the table lists the first author, the deep learning architecture used, the federated learning aggregation strategy, the primary evaluation dataset, the best reported accuracy and the F1 score, the scope of the experimental study, and type of the study under consideration. This summary serves as primary evidence for the cross-study comparisons presented in Subsections 2.1 through 2.4. Studies classified as survey or review papers (type S) do not report original experimental results and are included for contextual reference only. Performance values marked "–" were not reported by the original study authors and were not estimated or imputed.

As shown in Tab. 6, the reviewed studies span a range of deep learning architectures, aggregation mechanisms, and evaluation datasets, reflecting the methodological diversity existing in the field. Most empirical studies ($n = 35$) report a precision level greater than 97%, with performance differences between architecture groups examined in detail in Subsection 2.1. Studies specifically addressing low-rate DDoS detection in multi-controller SDN environments (scope: LDDoS-SDN) represent a small but methodologically distinct subset, $n = 4 : [4, 12, 15, 36]$, a limitation discussed further in Subsection 2.4.

CICIDS2017 is the most used dataset (51.4% of empirical studies), followed by CICDDoS2019 (40.0%). However, both data sets were originally designed for centralized network monitoring and primarily contain volumetric DDoS variants. Only the CAIDA LDDoS dataset provides authentic low-rate attack traffic patterns, yet it is used in only 8.6% of reviewed studies and does not simulate the multi-controller SDN topology.

The InSDN dataset, used by 14.3% of studies, is the only benchmark that explicitly simulates the SDN topology, though it does not model multi-controller distributed visibility. These findings indicate that 93.7% of the reviewed studies employed

Tab. 5. Distribution of benchmark data sets and evaluation of LDDoS representativeness.

Dataset	Frequency N	Coverage [%]	LDDoS representation in SDN environment
CICIDS 2017	18	51.4	Partial – volumetric DDoS dominant; limited LDDoS patterns
CICDDoS 2019	14	40.0	Partial – multiclass DDoS; not SDN/controller-specific
InSDN	5	14.3	Moderate – SDN-specific topology; binary classification
Edge-IIoTset	4	11.4	Partial – IoT focus; no multi-controller simulation
CAIDA LDDoS	3	8.6	High – real LDDoS traffic; not multi-controller SDN
NSL-KDD	4	11.4	Low – general IDS dataset; no LDDoS or SDN specificity
Custom / other	6	17.1	Variable – domain-specific; limited reproducibility

Note: Percentage values are calculated over 35 empirical studies (studies may use multiple datasets, so the frequencies add up to > 35). LDDoS representativeness evaluated against three criteria: a) presence of low-rate attack patterns, b) multi-controller SDN topology simulation, and c) heterogeneous traffic distribution.

datasets that only partially represent the operational conditions of LDDoS detection in multi-controller SDN environments.

3. Discussion

3.1. Architecture Effectiveness

The spread of the F1 score, varying from 94.21% to 99.96% across 35 studies, is wider than the mean of 97.98% might suggest. That variance matters. It reflects real differences in how the studies were set up: which dataset and how many attack classes were considered, whether the task was binary or of the multiclass type. A single pooled mean is useful for broad comparisons of paradigms, but it may obscure cases where a particular architecture fails badly on stealthy traffic. Table 2 shows both the mean and the spread; both are worth becoming acquainted with.

The appearance of LSTM and Bi-LSTM models in 20% of empirical studies (n=7 of 35; Tab. 3) comes as no surprise. LDDoS attacks are fundamentally temporal events. They have the form of short bursts occurring at regular intervals and are designed to exploit TCP retransmission timeouts. CNN-based architectures capture spatial feature relationships well and achieve high accuracy on binary tasks, but their lower F1 scores on multiclass scenarios (Tab. 3) suggest that they can miss the periodicity that defines LDDoS. Recurrent models are built for that periodicity; it is what they were designed to capture.

The transformer result from [9] (99.40% F1) and the GNN result from [31] (97.60% F1) are both encouraging. Each of them originates from a single study. The numbers are real, but a single study cannot determine whether an architecture is generalized. Additional replication across datasets and SDN configurations is required before either approach receives a recommendation.

3.2. Federated vs. Centralized Performance

The 0.27 percentage point accuracy gap between federated (98.33%) and centralized (98.06%) approaches, as shown in Tab. 4, is small enough to be treated as noise in most deployment contexts. Federated learning does not sacrifice much detection performance in exchange for keeping traffic data local. This trade-off looks reasonable.

What it gives up is simplicity. Every aggregation round requires controllers to exchange model parameters with a central server. In large-scale deployments with many controllers and constrained inter-domain links, the communication cost compounds over training. None of the reviewed studies report actual bandwidth figures, making it hard to identify how significant this cost is in practice. This type of reporting should be standard in future work.

3.3. Dataset Representativeness Limitations

CICIDS2017 and CICDDoS2019 cover 51.4% and 40.0% of the evaluated studies, respectively (Tab. 5). Both of them were captured in centralized environments with volumetric attack traffic as the dominant threat class. A model trained on these datasets is essentially learning to separate high-volume attack flows from normal traffic. LDDoS attacks do not generate high-volume flows; this is the very point behind their use. A model tuned on CICIDS2017 may never see the kind of signal an LDDoS attack actually produces.

CAIDA LDDoS contains really low-rate attack traffic and is the most relevant data set in the corpus, but only 8.6% of studies used it and it does not simulate the distributed SDN topology. InSDN is the only benchmark with an SDN-specific capture environment, but it lacks multi-controller partitioning. Consequently, 93.7% of the reviewed studies were evaluated on data that do not match the deployment scenario their methods claim to address. The high accuracy figures in those studies should be interpreted accordingly.

3.4. Limitations and Threats to Validity

Publication bias is a real concern here. Studies finding that federated learning performed poorly or failing to converge are less likely to appear in indexed databases. As a result, the pooled accuracy figures shown in Tab. 2 probably lean towards the optimistic side.

Heterogeneity between studies is a deeper problem. The 35 empirical studies use different datasets, different attack mixes, different numbers of controllers, and different evaluation protocols. The pooling of their results gives a rough picture of the field, but cannot substitute for a controlled comparison. The synthesis should be read as a structured overview, not as experimental evidence.

Two narrower issues need to be taken into consideration as well: some metric values were not reported by the studies' authors and appear as "–" in Tab 6. Those gaps are real and affect coverage of certain architecture groups. The search also covered four databases (IEEE Xplore, ACM Digital Library, Springer, Scopus), making it thorough but not exhaustive. Relevant work in domain-specific venues may have been missed.

4. Conclusions

The central finding is straightforward: federated learning works for LDDoS detection in multi-controller SDN environments, and it does not sacrifice much accuracy in the process. Across 39 studies published between 2020 and 2026, federated models averaged an accuracy score of 98.33% versus 98.06% for centralized approaches. The observed gap of 0.27 percentage points is, for practical purposes, negligible.

As far as the architecture is concerned (question no. 1), LSTM-based and hybrid CNN+RNN models led the field on most metrics. Neither result is surprising. LDDoS traffic has temporal structure-periodic bursts, not volume spikes, and recurrent architectures are built to capture exactly that. Hybrid CNN+RNN models achieved the highest mean F1 score among groups with more than two studies (98.54%, ±0.67; Tab. 3). Transformer and GNN architectures showed

Tab. 6. Summary of all 39 reviewed studies: architecture, aggregation strategy, dataset, and reported performance.

Study	Architecture	Aggregation strategy	Dataset	Acc [%]	F1 [%]	Scope	Type
[1]	Hybrid CNN+LSTM	FedAvg	CICIDS2017	98.71	98.50	DDoS-SDN	E
[2]	GRU	FedAvg	CICIDS2018	98.30	97.90	DDoS-IoT	E
[3]	CNN+LSTM	FedAvg/Cent.	InSDN	98.80	98.70	DDoS-SDN	E
[4]	LSTM	FedAvg	Edge-IIoTset	98.50	97.80	LDDoS-SDN	E
[5]	CNN (2D)	FedAvg	CICIDS2017	99.23	98.59	DDoS-SDN	E
[6]	Survey	N/A	Multiple	–	–	IDS-general	S
[7]	Bi-LSTM	Centralized	NSL-KDD	98.90	98.60	IDS-general	E
[8]	Survey	N/A	Multiple	–	–	IDS-general	S
[9]	Transformer	FedAvg+CL	CICDDoS2019	99.50	99.40	DDoS-SDN	E
[10]	Bi-LSTM+Attn.	AsyncFL (bLAM)	CAIDA LDDoS	98.55	98.55	LDDoS-SDN	E
[11]	CNN (1D)	Adaptive FL (FLAD)	CAIDA LDDoS	97.10	97.01	DDoS-gen.	E
[12]	LSTM	Async FedAvg	CICDDoS2019	99.10	98.82	DDoS-SDN	E
[13]	Multi-model FL	Multi-model Agg.	CICIDS2017	98.00	97.95	DDoS-SDN	E
[14]	XGBoost+LSTM	Centralized	Custom	97.80	97.50	IDS-general	E
[15]	MLP	Weighted Agg. FL	Custom	97.10	97.00	DDoS-SDN	E
[16]	CNN+Attention	FedAvg	CICIDS2017	98.40	98.20	DDoS-IoT	E
[17]	Hybrid DL	Centralized	CICIDS2017	99.10	99.00	DDoS-SDN	E
[18]	Multi-agent DL	Adaptive FL	CICIDS2018	98.40	98.30	IDS-general	E
[19]	LSTM	FedAvg (robust)	N-BaIoT	97.60	97.40	DDoS-IoT	E
[20]	Hybrid CNN+RNN	Centralized	CICDDoS2019	99.20	99.10	DDoS-SDN	E
[21]	CNN (1D)	Centralized	NSL-KDD	98.50	98.30	DDoS-IoT	E
[22]	Survey	N/A	Multiple	–	–	IDS-general	S
[23]	CNN (1D)	Centralized	NSL-KDD	99.20	–	IDS-general	E
[24]	RNN	FedAvg	Custom (telecom)	96.80	96.70	DDoS-tel.	E
[25]	Survey	N/A	Multiple	–	–	IDS-general	S
[26]	CNN+RNN	Centralized	CICIDS2017	98.10	97.80	DDoS-gen.	E
[27]	Hybrid DL	Centralized	CICIDS2017	98.80	98.60	DDoS-SDN	E
[28]	GRU	FedAvg	CICDDoS2019	98.80	98.35	DDoS-SDN	E
[29]	CNN+LSTM	Adaptive FL	CICDDoS2019	98.20	98.00	DDoS-SDN	E
[30]	ML (SVM/RF)	Centralized	Custom (SDN)	96.10	–	LDDoS-SDN	E
[31]	GNN (GowFed)	FedAvg	CICIDS2017	97.60	97.60	DDoS-SDN	E
[32]	LSTM	FedAvg	CICDDoS2019	98.90	98.80	DDoS-SDN	E
[33]	ML (framework)	Centralized	Custom (SDN)	96.40	–	DDoS-SDN	E
[34]	CNN+LSTM (MFFLR)	Centralized	Custom (SDN)	97.40	97.20	LDDoS-SDN	E
[35]	G-Network	Decentralized FL	CICIDS2017	97.00	96.90	IDS-general	E
[36]	CNN+XAI	FedAvg + XAI	CICIDS2018	97.80	97.70	IDS-SDN	E
[37]	GNN (ensemble)	Multi-view FL	N-BaIoT	97.90	97.80	DDoS-IoT	E
[38]	Survey	N/A	Multiple	–	–	DDoS-SDN	S
[39]	Autoencoder+FL	FedAvg	CICIDS2018	98.20	98.10	DDoS-SDN	E

Note: Scope: LDDoS-SDN=low-rate DDoS in multi-controller SDN [4, 15, 32, 36]; DDoS-SDN=general DDoS in SDN; DDoS-IoT=DDoS in IoT network; DDoS-tel.=telecom cloud; DDoS-gen.=general DDoS (non-SDN); IDS-general=generic IDS without SDN focus; IDS-SDN=IDS with SDN component. Type: E=empirical; S=survey/review. Acc and F1: best values per study; "–"= not reported.

strong individual results, but each appeared in only one or two studies, which is not enough to draw firm conclusions.

As far as aggregation strategies (question no. 2) are concerned, weighted aggregation, asynchronous FL, and personalized FL all appeared repeatedly and each of them addressed a different version of the heterogeneity problem, unequal data distributions, synchronization delays, and domain-specific traffic patterns, respectively. The standard FedAvg remained a common baseline. Evidence suggests that asynchronous and adaptive strategies tend to outperform FedAvg when con-

trollers operate under genuinely different conditions, though direct comparisons within single studies are limited.

The data set situation (question no. 4) is the field's clearest weak point. No available benchmark simultaneously models low-rate attack patterns, multi-controller SDN topology, and heterogeneous traffic distributions. CICIDS2017 and CICDDoS2019 dominate the literature despite not being designed for LDDoS or distributed SDN scenarios. Until better evaluation data is available, the accuracy figures reported on these benchmarks overstate how ready these methods are for deployment.

Three things would improve future work in this area the most. A benchmark dataset built for LDDoS detection in multi-controller environments, with distributed traffic capture and varied attack periodicity, would make cross-study comparison genuinely meaningful. Studies should routinely report communication overhead and convergence time alongside detection metrics; right now, those numbers rarely appear in the literature. Pre-registering the analysis protocol before data extraction would also reduce the risk of post-hoc decision making that inflates reported performance.

References

[1] X. Zhou, X. Mao, and Y. Chen, "A DDoS Attack Detection Method Combining Federated Learning and Hybrid Deep Learning in Software Defined Networking", *The Computer Journal*, vol. 68, pp. 1463–1475, 2025 (https://doi.org/10.1093/comjnl/bxaf049).

[2] A. Alhasawi and S. Alghamdi, "Federated Learning for Decentralized DDoS Attack Detection in IoT Networks", *IEEE Access*, vol. 12, pp. 42357–42368, 2024 (https://doi.org/10.1109/access.2024.3378727).

[3] M. Shamim *et al.*, "A Comparison Study on federated Learning and Centralized Learning-based Intrusion Detection System for Software Defined Networking", *2025 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC)*, Seoul, South Korea, 2025 (https://doi.org/10.1109/ITC-CSCC66376.2025.11137775).

[4] Z. Alashhab *et al.*, "Low-rate DDoS Attack Detection Using Deep Learning for SDN Enabled IoT Networks", *International Journal of Advanced Computer Science and Applications*, vol. 13, 2022 (https://doi.org/10.14569/ijacsa.2022.0131141).

[5] Z. Lv *et al.*, "DDoS Attack Detection Based on CNN and Federated Learning", *International Conference on Advanced Cloud and Big Data*, Xi'an, China, 2022 (https://doi.org/10.1109/cbd54617.2021.00048).

[6] V. R *et al.*, "A Comprehensive Tutorial and Survey of Applications of Deep Learning for Cyber Security", *TechRxiv*, 2020 (https://doi.org/10.36227/TECHRXIV.11473377.V1).

[7] S. Muthunambu *et al.*, "A Novel Eccentric Intrusion Detection Model Based on Recurrent Neural Networks with Leveraging LSTM", *Computers Materials and Continua*, vol. 78, pp. 3089–3127, 2024 (https://doi.org/10.32604/cmc.2023.043172).

[8] A. Khraisat *et al.*, "Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions", *ACM Computing Surveys*, vol. 57, pp. 1–38, 2024 (https://doi.org/10.1145/3687124).

[9] M. Fan *et al.*, "DDoS Attack Detection in SDN-assisted Federated Learning Environment Based on Contrastive Learning", *IEEE Access*, vol. 13, pp. 108798–108814, 2025 (https://doi.org/10.1109/access.2025.3582445).

[10] Y. Liu *et al.*, "An Asynchronous Federated Learning Arbitration Model for Low-rate DDoS Attack Detection", *IEEE Access*, vol. 11, pp. 18448–18460, 2023 (https://doi.org/10.1109/ACCESS.2023.3247512).

[11] R. Doriguzzi-Corin and D. Siracusa, "FLAD: Adaptive Federated Learning for DDoS Attack Detection", *Computers & Security*, vol. 137, art. no. 103597, 2023 (https://doi.org/10.1016/j.cose.2023.103597).

[12] Y.S.N. Fotse, V.K. Tchendji, and M. Velempini, "Federated Learning Based DDoS Attacks Detection in Large Scale Software-defined Network", *IEEE Transactions on Computers*, vol. 74, pp. 101–115, 2024 (https://doi.org/10.1109/tc.2024.3474180).

[13] A.A. Al-Ameer and W.S. Bhaya, "Intelligent Intrusion Detection Based on Multi Model Federated Learning for Software Defined Network", *International Journal of Safety and Security Engineering*, vol. 13, pp. 1135–1141, 2023 (https://doi.org/10.18280/ijsse.130617).

[14] R. Amin, G. El-Taweel, A. Ali, and M. Tahoun, "A Hybrid Extreme Gradient Boosting and Long Short-term Memory Algorithm for Cyber Threats Detection", *Mendel*, vol. 29, pp. 307–322, 2023 (https://doi.org/10.13164/mendel.2023.2.307).

[15] K. Ramya *et al.*, "An Efficient Infiltration and Denial of Service Detection Using Dynamic Weighted Aggregation Federated Learning", in *Recent Trends in Network Security*, 2024 (https://doi.org/10.1201/9781003565024-13).

[16] N.T. Cam and N.G. Trung, "An Intelligent Approach to Improving the Performance of Threat Detection in IoT", *IEEE Access*, vol. 11, pp. 44319–44334, 2023 (https://doi.org/10.1109/access.2023.3273160).

[17] J. Malik *et al.*, "Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN", *IEEE Access*, vol. 8, pp. 134695–134706, 2020 (https://doi.org/10.1109/ACCESS.2020.3009849).

[18] M. Moradi *et al.*, "A Multi Agent Adaptive Deep Learning Framework for Online Intrusion Detection", *Cybersecurity*, vol. 7, art. no. 9, 2024 (https://doi.org/10.1186/s42400-023-00199-0).

[19] R. Yang *et al.*, "Dependable Federated Learning for IoT Intrusion Detection Against Poisoning Attacks", *Computers & Security*, vol. 132, art. no. 103381, 2023 (https://doi.org/https://doi.org/10.1016/j.cose.2023.103381).

[20] A. Elubeyd and D. Yiltas-Kaplan, "Hybrid Deep Learning Approach for Automatic dos DDoS Attacks Detection in Software Defined Networks", *Applied Sciences*, vol. 13, art. no. 3828, 2023 (https://doi.org/10.3390/app13063828).

[21] M. Aswad *et al.*, "Deep Learning in Distributed Denial of Service Attacks Detection Method for Internet of Things Networks", *Journal of Intelligent Systems*, vol. 32, 2023 (https://doi.org/10.1515/jisys-2022-0155).

[22] H. Zhang *et al.*, "Survey of Federated Learning in Intrusion Detection", *Journal of Parallel and Distributed Computing*, vol. 195, art. no. 104976, 2024 (https://doi.org/10.1016/j.jpdc.2024.104976).

[23] U. Qazi, A. Almorjan, and T. Zia, "A One-dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection", *Applied Sciences*, vol. 12, art. no. 7986, 2022 (https://doi.org/10.3390/app12167986).

[24] A.A Maiga, E. Ataro, and S. Githinji, "Secured Federated Learning for DDoS Detection in Heterogeneous Telecom Cloud Networks Using Recurrent Neural Networks", *International Journal of Electrical and Electronics Engineering*, vol. 10, pp. 54–64, 2023 (https://doi.org/10.14445/23488379/ijeee-v10i12p106).

[25] A. Adedeji, A.M. Abu-Mahfouz, and A.M. Kurien, "DDoS Attack and Detection Methods in Internet Enabled Networks: Concept, Research Perspectives, and Challenges", *Journal of Sensor and Actuator Networks*, vol. 12, art. no. 51, 2023 (https://doi.org/10.3390/jsan12040051).

[26] M. Elsayed *et al.*, "DDoSnet: A Deep Learning Model for Detecting Network Attacks", *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"*, Cork, Ireland, 2020 (https://doi.org/10.1109/WoWMoM49955.2020.00072).

[27] M.W. Nadeem, H.G. Goh, Y. Aun, and V. Ponnusamy, "Detecting and Mitigating Botnet Attacks in Software-defined Networks Using Deep Learning Techniques", *IEEE Access*, vol. 11, pp. 49153–49171, 2023 (https://doi.org/10.1109/access.2023.3277397).

[28] J. Mateus, G.A.L. Zodi, and A. Bagula, "Federated Learning-based Solution for DDoS Detection in SDN", *2024 International Conference on Computing, Networking and Communications (ICNC)*, Big Island, USA, 2024 (https://doi.org/10.1109/icnc59896.2024.10556115).

[29] S.S. Kiruthika, S. Kumar, R. Fernandes, and S. Adari, "Network Flow Based Abnormal Behavior Feature Extraction for DDoS Attack Classification Using Adaptive Federated Learning Model", *Journal on Emerging trends in Modelling and Manufacturing*, vol. 9, 2023 (https://doi.org/10.46632/jemm/9/2/5).

[30] F. Perez Diaz *et al.*, "A Flexible SDN-based Architecture for Identifying and Mitigating Low-rate DDoS Attacks Using Machine Learning", *IEEE Access*, vol. 8, pp. 155859–155872, 2020 (https://doi.org/10.1109/ACCESS.2020.3019330).

[31] A. Belenguer, J.A. Pascual, and J. Navaridas, "GowFed: A Novel Federated Network Intrusion Detection System", *Journal of Network and Computer Applications*, vol. 217, art. no. 103653, 2023 (https://doi.org/10.1016/j.jnca.2023.103653).

[32] Y.S.N. Fotse, V.K. Tchendji, and M. Velempini, "Federated Learning Based DDoS Attacks Detection in Large Scale Software Defined Network", *IEEE Transactions on Computers*, vol. 74, pp. 101–115, 2024 (https://doi.org/10.1109/tc.2024.3474180).

[33] A. Kadam *et al.*, "SDN-driven Security Framework for DDoS Attack Detection and Mitigation", *International Journal for Science Technology and Engineering*, vol. 12, pp. 620–625, 2024 (https://doi.org/10.22214/ijraset.2024.65142).

[34] J. Wang, L. Wang, and R. Wang, "MFFLR-DDoS: An Encrypted LR-DDoS Attack Detection Method Based on Multi Granularity Feature Fusions in SDN", *Mathematical Biosciences and Engineering*, vol. 21, pp. 4187–4209, 2024 (https://doi.org/10.3934/mbe.2024185).

[35] M. Nakip, B.C. Gul, and E. Gelenbe, "Decentralized Online Federated G-network Learning for Lightweight Intrusion Detection", *2023 31st International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Stony Brook, USA, 2023 (https://doi.org/10.1109/MASCOTS59514.2023.10387644).

[36] K. Oki, Y. Ogawa, K. Ota, and M. Dong, "Evaluation of Applying Federated Learning to Distributed Intrusion Detection Systems through Explainable AI", *IEEE Networking Letters*, vol. 6, pp. 198–202, 2024 (https://doi.org/10.1109/lnet.2024.3465516).

[37] D.C. Attota, V. Mothukuri, R.M. Parizi, and S. Pouriyeh, "An Ensemble Multi-view Federated Learning Intrusion Detection for IoT", *IEEE Access*, vol. 9, pp. 117734–117745, 2021 (https://doi.org/10.1109/access.2021.3107337).

[38] A.A. Wabi, I. Idris, O.M. Olaniyi, and J.A. Ojeniyi, "DDoS Attack Detection in SDN: Method of Attacks, Detection Techniques, Challenges and Research Gaps", *Computers & Security*, vol. 139, art. no. 103652, 2023 (https://doi.org/10.1016/j.cose.2023.103652).

[39] J. Ma and W. Su, "Collaborative DDoS defense for SDN-based AIoT with Autoencoder-enhanced Federated Learning", *Information Fusion*, vol. 117, art. no. 102820, 2024 (https://doi.org/10.1016/j.inffus.2024.102820).

Rikie Kartadie, S.T., M.Kom.
Doctoral Program in Engineering Science
https://orcid.org/0000-0003-1947-353X
E-mail: rikie@utdi.ac.id
Universitas Negeri Yogyakarta, Indonesia
https://www.uny.ac.id
Universitas Teknologi Digital Indonesia,
Yogyakarta, Indonesia
http://www.utdi.ac.id

Eko Marpanaji, Ph.D., Assoc. Professor
Doctoral Program in Engineering Science
https://orcid.org/0009-0001-6613-4920
E-mail: eko@uny.ac.id
Universitas Negeri Yogyakarta, Indonesia
https://www.uny.ac.id

Agus Maman Abadi, Ph.D., Professor
Department of Mathematics Education
https://orcid.org/0000-0002-5488-3043
E-mail: agusmaman@uny.ac.id
Universitas Negeri Yogyakarta, Indonesia
https://www.uny.ac.id