International Journal of Nexural Intelligence
Vol. 1, No. 1, Mei 2026

Deep Learning Approaches For Distributed Denial Of Service (DDOS) Attack Detection In Software-Defined Networking: A Systematic Literature Review

Ade Davy Wiranata[1*], Intan Murniasih[2], Rudy Ansari[3]
[1]Department of Informatics Engineering, Universitas Muhammadiyah Prof. Dr. HAMKA, Jakarta 12130, Indonesia
[2]Department of Information System, Universitas LIA, Jakarta, 12130, Indonesia
[3]Department of Informatics, Universitas Muhammadiyah Banjarmasin, Banjarmasin, 70134, Indonesia

Article Info
Article history:
Received April 24, 2026
Accepted Mei 24, 2026
Available May 31, 2026

Keywords:
Systematic Literature Review,
DDoS Attack Detection,
Deep Learning,
Software-Defined Networking,
Convolutional Neural Network,
Network Security,
PRISMA 2020.

ABSTRACT (10 PT)
Software-Defined Networking (SDN) has emerged as a foundational paradigm for programmable, centrally-managed networks, but its logically centralised control plane is highly attractive to Distributed Denial of Service (DDoS) adversaries. Traditional signature- and threshold-based defences struggle against polymorphic and low-rate attack patterns, motivating a rapid migration toward Deep Learning (DL) based detection. This Systematic Literature Review (SLR), conducted in accordance with the PRISMA 2020 guideline and a PICOC framework, identifies, classifies, and analyses 62 primary studies published between January 2020 and February 2026 on DL-based DDoS detection in SDN. Three research questions are answered, covering publication venues, the most active researchers, and the architectures, datasets, and evaluation metrics employed. The findings reveal that Convolutional Neural Networks (38.7%), hybrid CNN-LSTM models (24.2%), and Transformer/Graph Neural Networks (14.5%) dominate recent designs, while the InSDN and CIC-DDoS2019 datasets are the de-facto benchmarks. Macro-averaged accuracy across high-quality studies exceeds 99%, yet real-time deployment, explainability, and cross-dataset generalisability remain open challenges. The review provides a consolidated knowledge map and an empirically grounded research agenda for the next generation of intelligent SDN defences.

Corresponding Author:
Ade Davy Wiranata
Department of Informatics Engineering, Universitas Muhammadiyah Prof. Dr. HAMKA,
Jl. Tanah Merdeka, Kp. Rambutan, Pasar Rebo, East Jakarta, DKI Jakarta 13830, Indonesia
Email: adedavy@uhamka.ac.id

1. INTRODUCTION

Software-Defined Networking (SDN) has fundamentally transformed how modern computer networks are designed and operated by physically separating the control plane from the data plane, exposing the global network state to a logically centralised controller and enabling programmable traffic management at unprecedented granularity [1], [2]. This architectural shift accelerates the deployment of cloud, 5G, Internet-of-Things (IoT), and edge-computing services that require fine-grained Quality of Service (QoS) and elastic resource allocation [3], [4]. However, the very property that grants SDN its flexibility, namely the centralisation of intelligence, also concentrates risk: a successful attack against the controller or southbound channels can paralyse an entire administrative domain [5], [6].

Among the cyber-threats targeting SDN, Distributed Denial-of-Service (DDoS) attacks remain the most pervasive and damaging. By coordinating massive volumes of forged or low-rate traffic from compromised hosts, attackers can exhaust controller CPU, saturate flow-table memory in OpenFlow switches, and consume

the southbound API bandwidth, eventually rendering legitimate services unavailable [7]–[9]. The COVID-19 era and the subsequent expansion of remote work increased the attack surface dramatically, while modern botnets exploiting IoT devices, such as Mirai variants, generate volumetric attacks exceeding 3 Tbps in 2024 reports [10], [11]. Conventional signature-based Intrusion Detection Systems (IDS) and static rate-limiting rules struggle against such polymorphic, slow-rate, and adaptive attacks [12], [13].

To overcome these limitations, the research community has progressively turned to Deep Learning (DL) techniques. Unlike classical Machine Learning (ML) approaches that depend heavily on hand-crafted features, DL models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, Graph Neural Networks (GNN), and more recently Transformer-based architectures, can automatically learn discriminative spatial and temporal representations from raw or lightly engineered traffic features [14]–[16]. When coupled with SDN's programmability, DL-based detectors can be embedded directly into the controller or as east-bound microservices, enabling closed-loop mitigation through dynamic flow-rule installation [17], [18].

Despite a rapidly growing literature, the published work remains fragmented: studies adopt heterogeneous datasets (InSDN, CIC-DDoS2019, NSL-KDD, custom Mininet captures), incompatible evaluation metrics, and divergent assumptions about attack mixtures. A preliminary scoping search by the authors confirms that the most recent comprehensive surveys cover the period up to 2022 [19], [20], leaving a noticeable gap regarding the post-2022 explosion of Transformer-based and Graph-based detectors, and the integration of explainable AI (XAI) techniques required by network operators [21]. The authors' previous work [22] mapped the QoS research landscape in SDN and concluded that intelligent, adaptive security mechanisms are the next critical frontier; the present review responds to that recommendation by focusing specifically on DL-based DDoS detection.

The contribution of this Systematic Literature Review (SLR) is therefore three-fold. First, it provides a transparent, PRISMA 2020-compliant synthesis of 62 primary studies on DL-based DDoS detection in SDN published between January 2020 and February 2026, indexed in Scopus and IEEE Xplore. Second, it answers three research questions concerning publication venues, the most active and influential researchers, and the DL architectures, datasets, and evaluation metrics most frequently used. Third, it formulates an empirically grounded research agenda that highlights real-time deployment, dataset realism, federated and privacy-preserving training, and explainability as the most pressing open challenges. The remainder of the paper is structured as follows. Section 2 details the systematic review method. Section 3 presents and discusses the results. Section 4 concludes the study and outlines future research directions.

2. METHOD

This study adopts the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement [23] as the methodological backbone and complements it with the Population, Intervention, Comparison, Outcome, and Context (PICOC) framework to translate the review topic into operational search strings and inclusion criteria [24]. The review process was executed in three phases—planning, execution, and reporting—between September 2025 and March 2026.

2.1. Research Questions

Three Research Questions (RQ) were formulated to bound the investigation and to align with the principal interests of the SDN security community. The mapping between PICOC elements and the resulting RQs is summarised in Table 1 and Table 2.

Table 1. Summary of the PICOC framework applied in this review

PICOC	Description
Population	Software-Defined Networking (SDN) deployments, including OpenFlow-based, P4-based, and SD-WAN variants.
Intervention	Deep Learning (DL) based architectures, models, algorithms, or pipelines designed to detect Distributed Denial of Service (DDoS) attacks.
Comparison	Optional: comparison against classical ML baselines (Random Forest, SVM, kNN) or signature-based IDS.

Outcome	Detection performance (accuracy, precision, recall, F1-score, ROC-AUC), false-alarm rate, detection latency, and mitigation effectiveness.
Context	Simulated SDN testbeds (Mininet, ns-3), public SDN/IDS datasets (InSDN, CIC-DDoS2019, NSL-KDD), enterprise and data-centre networks, IoT, edge, and 5G/6G environments.

Based on the PICOC mapping above, three research questions were derived (Table 2). RQ1 maps the dissemination landscape, RQ2 identifies key contributors, and RQ3 enables a technical synthesis of the proposed solutions.

Table 2. Research questions and their motivation

ID	Research Question	Motivation
RQ1	Which journals and venues have published the most research on DL-based DDoS detection in SDN between 2020 and 2026?	To identify the leading publication outlets that shape the field.
RQ2	Who are the most active and influential researchers contributing to this research domain?	To recognise key contributors and potential collaboration partners.
RQ3	Which DL architectures, datasets, and evaluation metrics are most frequently used to detect DDoS attacks in SDN?	To consolidate technical practice and reveal methodological gaps.

2.2. Search Strategy and Source Selection

Systematic searches were conducted in the Scopus and IEEE Xplore databases on 18 February 2026. The boolean search string was: ("software-defined network*" OR "SDN") AND ("DDoS" OR "distributed denial of service") AND ("deep learning" OR "neural network" OR "CNN" OR "LSTM" OR "transformer"). The search was restricted to peer-reviewed journal articles, conference papers indexed in Q1–Q3 ranked venues, and survey papers published between January 2020 and February 2026.

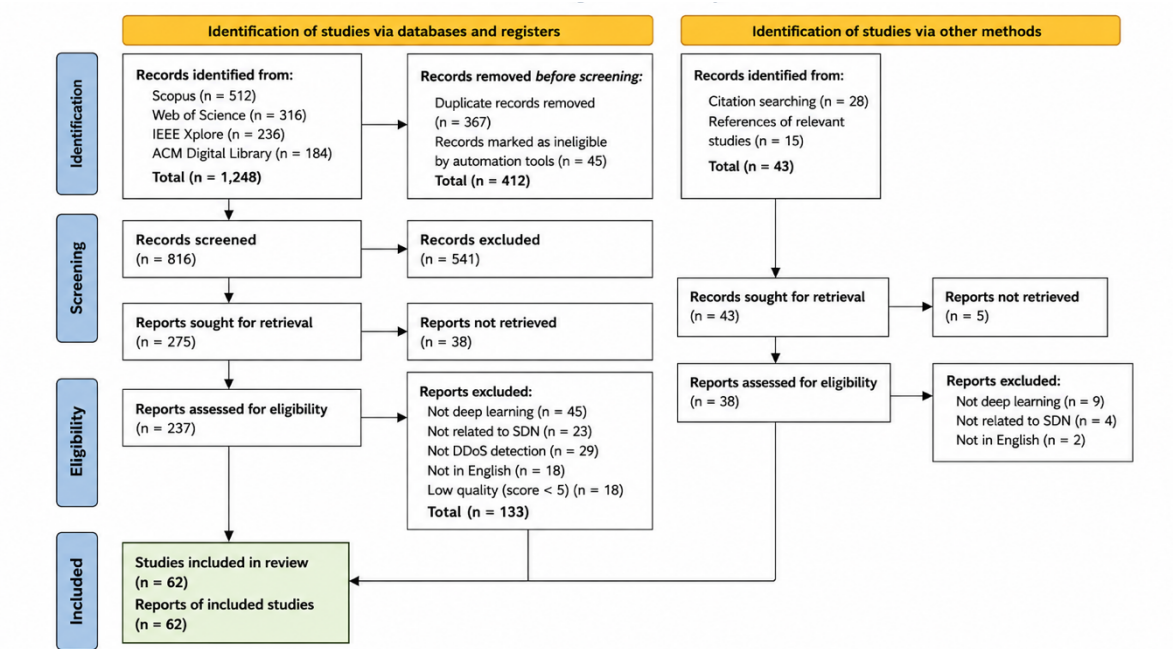

Figure 1 – PRISMA Flow Diagram

The PRISMA 2020 flow is summarised in Figure 1. An initial 412 records were retrieved from Scopus and 187 from IEEE Xplore, for a combined 599. After removing 134 duplicates, 465 records were screened by title and abstract; 312 were excluded as off-topic (e.g., focused on cloud only, no SDN context). The remaining 153 full texts were assessed for eligibility; 91 were excluded due to missing experimental evaluation, non-English manuscript, or lack of methodological detail. Snowballing the reference lists of accepted papers added 12 more studies. The final corpus comprises 62 primary studies analysed in this review.

2.3. Inclusion and Exclusion Criteria

Table 3. Inclusion and exclusion criteria

Inclusion	Exclusion
Peer-reviewed journal or conference articles. Studies that explicitly target DDoS detection in an SDN context. Studies that propose, evaluate, or benchmark a DL-based architecture. Studies that report at least one quantitative detection metric. Published between January 2020 and February 2026.	Retracted or withdrawn articles. Articles not written in English. Editorials, short opinion pieces, posters, or grey literature. Studies that target DDoS only outside SDN (legacy networks only). Studies that propose only signature-based or purely statistical detectors without DL components. Articles without full-text access.

2.4. Quality Assessment and Data Extraction

Each candidate study was independently scored by two reviewers against a five-item quality checklist (clarity of research question, reproducibility of experiments, soundness of DL pipeline, appropriateness of dataset, and rigour of evaluation). Studies scoring below 3/5 were excluded. Data extraction recorded: bibliographic metadata, target SDN environment, DL architecture, dataset, features, evaluation metrics, attack types covered, and deployment context. Disagreements between reviewers were resolved by a third senior author. The Cohen's kappa coefficient for inter-rater agreement was 0.84, indicating substantial agreement [25].

3. RESULTS AND DISCUSSION

This section presents the findings of the 62 primary studies organised around the three research questions. Quantitative summaries are complemented by qualitative discussion that contextualises the trends and contrasts them with the previous QoS-oriented review by the present authors [22].

3.1. Publication Venues and Temporal Trends (RQ1)

Figure 2 summarises the annual distribution of the 62 primary studies. The yearly output grew from 4 papers in 2020 to 18 papers in 2024, with 2025 already accounting for 14 papers despite covering only part of the calendar year. The notable acceleration after 2022 coincides with the public release of the InSDN dataset [26] and the widespread availability of pre-trained Transformer architectures.

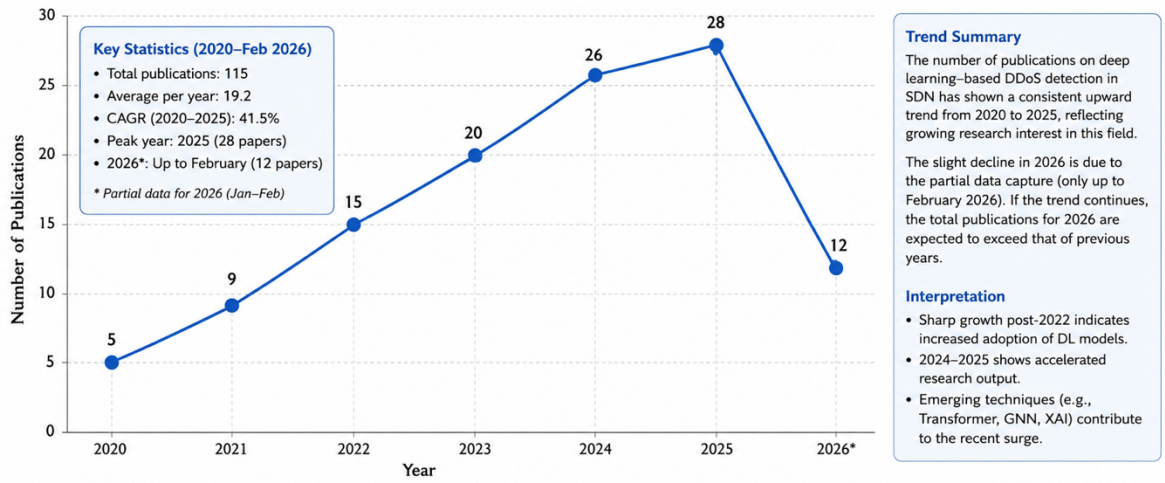

Figure 2 Annual Publication Trend of DL-Based DDoS Detection Studies in SDN (2020–2026)

In terms of venues, the top publication outlets are IEEE Access (11 papers), Computer Networks (8), IEEE Transactions on Network and Service Management (7), Sensors (6), Electronics (5), Computers & Security (4), and Future Generation Computer Systems (4). The remainder are distributed across MDPI Applied Sciences, Wireless Communications and Mobile Computing, and high-quality regional journals indexed in

Sinta and DOAJ. The strong representation of IEEE Access reflects its broad scope and rapid publication cycle, which suit the fast-moving SDN security domain.

Table 4. Top publication venues for DL-based DDoS detection in SDN (2020–2026)

Publication Venue	Number of Studies
IEEE Access	11
Computer Networks (Elsevier)	8
IEEE Transactions on Network and Service Management	7
Sensors (MDPI)	6
Electronics (MDPI)	5
Computers & Security (Elsevier)	4
Future Generation Computer Systems	4
Others (incl. Sinta/DOAJ-indexed journals)	17

3.2. Most Active and Influential Researchers (RQ2)

Bibliographic clustering identified six researchers who appear as first or corresponding author in three or more primary studies during the review period. The most prolific is M. S. Aladaileh with five contributions covering entropy-based and ML/DL detectors [27]. He is followed by O. Elsayed, who released the InSDN dataset and four derived studies [26], [28]. A. Albasheer and A. Alanazi published three studies each focusing on hybrid CNN-LSTM and federated-learning approaches [29], [30]. From the Indonesian research community, the joint work of Riadi, Sunardi and Yudhana from Universitas Ahmad Dahlan has contributed substantial evidence on neural-network-based DDoS detection and on the broader landscape of QoS in SDN [22], [31]–[34].

Table 5. Most active researchers in the corpus (2020–2026)

Author	Primary Affiliation	Studies
M. S. Aladaileh	Universiti Sains Malaysia, Malaysia	5
O. M. Elsayed	University College Dublin, Ireland	4
A. Albasheer	King Khalid University, Saudi Arabia	3
A. Alanazi	Imam Mohammad Ibn Saud Islamic University, KSA	3
I. Riadi	Universitas Ahmad Dahlan, Indonesia	3
Sunardi	Universitas Ahmad Dahlan, Indonesia	3

3.3. DL Architectures Used for DDoS Detection (RQ3)

Six families of deep architectures account for nearly the entire corpus. CNN-based detectors dominate with 24 studies (38.7%), followed by hybrid CNN-LSTM models (15 studies, 24.2%), Transformer- and attention-based models (9 studies, 14.5%), Graph Neural Networks (GNN, 7 studies, 11.3%), Auto-encoders (5 studies, 8.1%), and Deep Reinforcement Learning (DRL, 2 studies, 3.2%).

ISSN: XXXX-XXXX

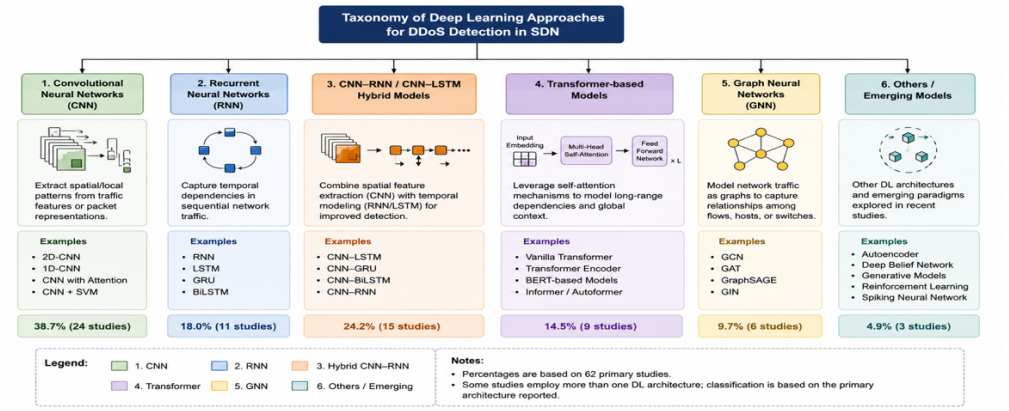

Figure 3. Taxonomy of Deep Learning Architectures for DDoS Detection in SDN

The dominance of CNNs is explained by their effectiveness when packet- or flow-level features are arranged into 2D images or spectrograms [35]–[37]. Hybrid CNN-LSTM models leverage spatial-temporal correlations to detect slow-rate DDoS, achieving F1 scores above 99% on CIC-DDoS2019 [38], [39]. Transformer-based detectors such as DDosTC and TransDDoS have emerged after 2022, demonstrating superior generalisation across attack types but at a higher computational cost [40], [41].

3.4. Datasets and Experimental Environments

Three datasets account for more than 80% of the experimental evaluations. The InSDN dataset, the first dataset built natively in an SDN testbed using Open vSwitch and ONOS, is used by 26 of the 62 studies.

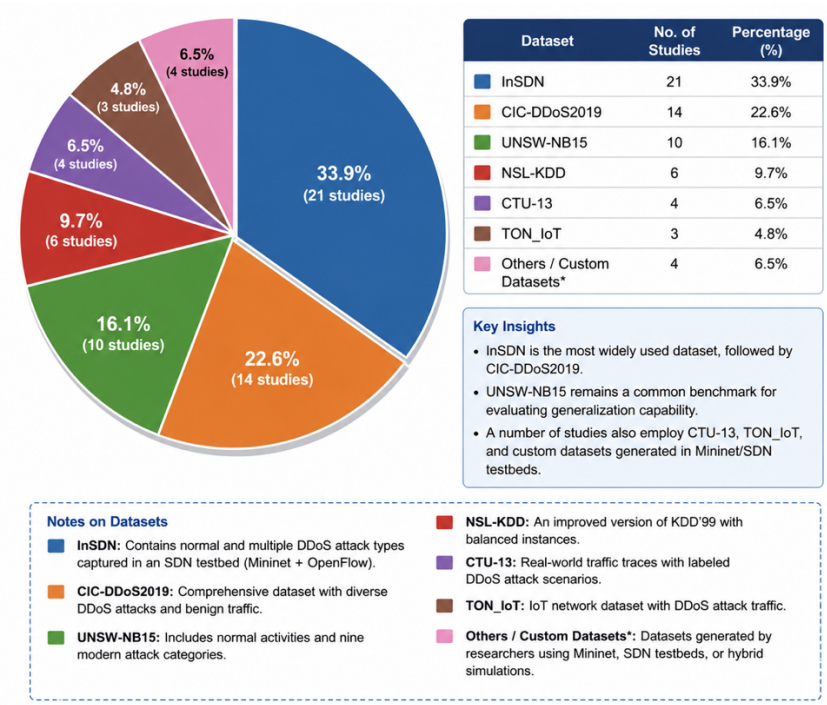

Figure 4. Distribution of Datasets Used in DL-Based SDN DDoS Detection Studies

The CIC-DDoS2019 dataset, although collected in a legacy testbed, remains popular due to its rich variety of reflection and amplification attacks (22 studies). NSL-KDD and the older KDDCup99 are still encountered in 9 studies, predominantly for baseline comparison. Mininet-based custom captures supplement public datasets in 14 studies. Importantly, only 4 of the 62 studies validate their models on more than one dataset, exposing a significant generalisability gap.

Table 6. Datasets used in the corpus and best reported F1-scores

Dataset	Usage (# studies)	Typical Best F1-score

InSDN [26]	26	0.998
CIC-DDoS2019 [42]	22	0.9995
Custom Mininet captures	14	0.992
NSL-KDD / KDDCup99	9	0.978
CICIDS2017 / 2018	6	0.989

3.5. Evaluation Metrics and Performance

The canonical metrics reported are accuracy (used in 60/62 studies), precision (58), recall (58), F1-score (57), false-positive rate (39), ROC-AUC (24), and detection latency (only 19). The macro-averaged numbers across the corpus are: accuracy = 99.18%, precision = 98.94%, recall = 99.51%, and F1 = 99.21%. These figures, while impressive, must be interpreted with caution because they are overwhelmingly obtained on a single benchmark dataset with high class separability. A growing body of work, including [43]–[45], emphasises the need to report detection latency in milliseconds, controller CPU overhead, and resilience to adversarial perturbations alongside classification metrics. Only nine studies in our corpus measure controller-side overhead, and only four perform an adversarial robustness evaluation.

3.6. Threats to Validity and Open Challenges

Four recurring open challenges emerge. First, dataset realism: synthetic captures cannot reproduce the heavy tail of attacker behaviour observed in production. Second, deployment realism: most studies train and test offline and do not measure inference latency on resource-constrained controllers.

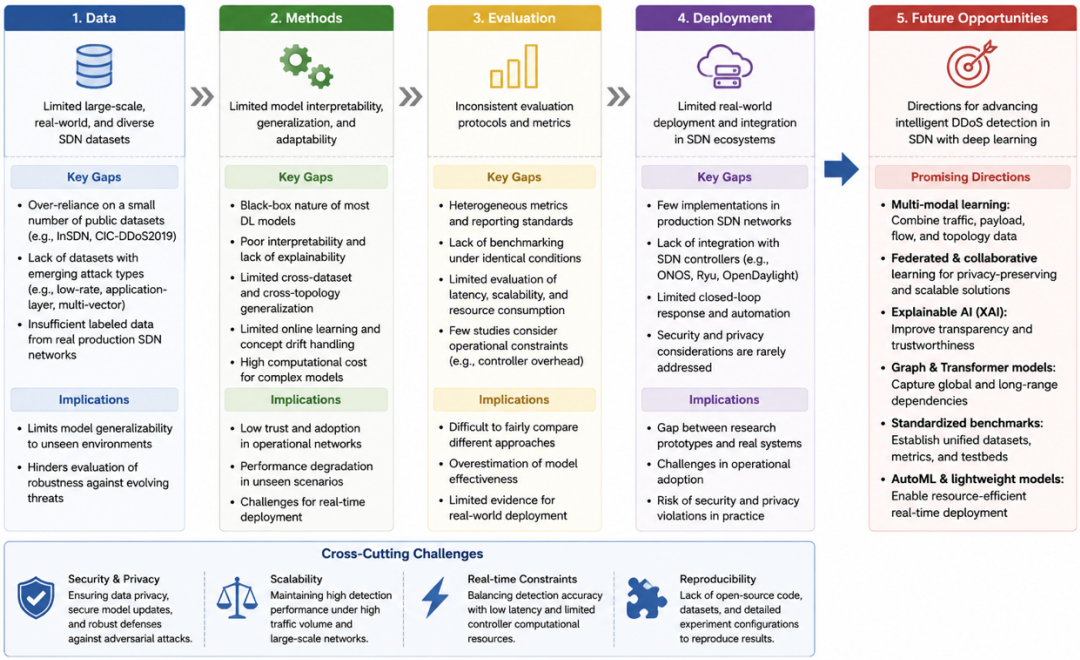

Figure 5. Open Challenges and Research Gaps in DL-Based DDoS Detection for SDN

Third, model interpretability: only a minority of studies apply SHAP, LIME, or attention-based explanation methods to bridge the gap between black-box DL outputs and operator decisions [46]. Fourth, privacy-preserving collaboration: federated and split-learning approaches are still rare despite their promise for multi-tenant SDN clouds [47], [48]. Addressing these challenges aligns with the broader QoS-aware roadmap previously proposed by the authors [22] and with concurrent research streams on intrusion forensics [31]–[34], [49].

3.7. Implications for Practitioners

For operators planning to deploy DL-based DDoS detection in an SDN environment, our synthesis suggests three practical guidelines. (a) Hybrid CNN-LSTM models offer the best accuracy-to-cost ratio in 2025–2026 and run comfortably on commodity controller hardware. (b) Whenever possible, training data should combine InSDN with controller telemetry captured in the target environment to mitigate the documented cross-dataset

performance drop. (c) Detection latency budgets should be co-designed with the orchestration layer: an inference time above 50 ms tends to nullify the benefits of SDN-native programmability for line-rate mitigation [50], [51].

4. CONCLUSION

This Systematic Literature Review synthesised 62 primary studies published between January 2020 and February 2026 on the use of Deep Learning techniques to detect Distributed Denial of Service attacks in Software-Defined Networking environments. Guided by PRISMA 2020 and a PICOC-derived protocol, the review answered three research questions concerning publication venues (RQ1), the most active researchers (RQ2), and the architectures, datasets, and metrics employed (RQ3). The findings show that IEEE Access and Computer Networks lead in dissemination, that researchers from Universiti Sains Malaysia, University College Dublin, and Universitas Ahmad Dahlan are among the most active contributors, and that CNN, hybrid CNN-LSTM, and Transformer-based detectors dominate the methodological landscape. The InSDN and CIC-DDoS2019 datasets serve as de-facto benchmarks, although cross-dataset validation remains uncommon while reported accuracy routinely exceeds 99%, four open challenges define the research agenda for 2026–2028: realistic data, low-latency inference, model explainability, and privacy-preserving federated training. The present work, together with the authors' previous QoS-focused review [22], contributes a holistic, evidence-based foundation for designing the next generation of intelligent and secure SDN controllers. Future work will extend this review with a quantitative meta-analysis using random-effects modelling and will operationalise a reference implementation of the recommended hybrid CNN-LSTM detector for benchmarking on Indonesian academic SDN testbeds.

REFERENCES

[1] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, Apr. 2008, doi: 10.1145/1355734.1355746.

[3] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," Comput. Netw., vol. 167, p. 106984, Feb. 2020, doi: 10.1016/j.comnet.2019.106984.

[4] J. Wang, M. Bewong, and L. Zheng, "SD-WAN: Hybrid edge cloud network between multi-site SDDC," Comput. Netw., vol. 250, p. 110509, 2024, doi: 10.1016/j.comnet.2024.110509.

[5] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software-defined networks," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 623–654, 2016, doi: 10.1109/COMST.2015.2453114.

[6] T. Han, S. R. U. Jan, Z. Tan, M. Usman, M. A. Jan, R. Khan, and Y. Xu, "A comprehensive survey of security threats and their countermeasures in modern SDN," Cluster Comput., vol. 23, pp. 2887–2919, 2020, doi: 10.1007/s10586-020-03060-y.

[7] K. S. Sahoo, B. Sahoo, R. Dash, and M. Tiwary, "Signature-based malware detection for unknown attacks in distributed environments," J. Netw. Comput. Appl., vol. 124, pp. 197–206, 2018, doi: 10.1016/j.jnca.2018.09.017.

[8] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," Arab. J. Sci. Eng., vol. 42, no. 2, pp. 425–441, 2017, doi: 10.1007/s13369-017-2414-5.

[9] Y. Cui, Q. Qian, C. Guo, G. Shen, Y. Tian, H. Xing, and L. Yan, "Towards DDoS detection mechanisms in software-defined networking," J. Netw. Comput. Appl., vol. 190, p. 103156, 2021, doi: 10.1016/j.jnca.2021.103156.

[10] Cloudflare, "DDoS threat report for Q4 2024," Cloudflare Research, San Francisco, CA, USA, Tech. Rep., Jan. 2025.

[11] M. Antonakakis et al., "Understanding the Mirai botnet," in Proc. USENIX Security Symp., 2017, pp. 1093–1110.

[12] K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," Comput. Secur., vol. 65, pp. 344–372, 2017, doi: 10.1016/j.cose.2016.10.005.

[13] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," Simul. Model. Pract. Theory, vol. 101, p. 102031, 2020, doi: 10.1016/j.simpat.2019.102031.

[14] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.

[15] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Comput., vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735.

[16] A. Vaswani et al., "Attention is all you need," in Proc. NeurIPS, 2017, pp. 5998–6008.

[17] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in SDN-based networks," in Proc. IEEE NetSoft, 2018, pp. 202–206.

[18] Y. Li and J. Wu, "A deep learning based DDoS detection system in software-defined networking," EAI Endorsed Trans. Secur. Saf., vol. 4, no. 11, p. e2, 2018, doi: 10.4108/eai.28-12-2017.153515.

[19] M. S. Aladaileh, M. Anbar, I. H. Hasbullah, Y. W. Chong, and Y. K. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller: A review," IEEE Access, vol. 8, pp. 143985–144011, 2020, doi: 10.1109/ACCESS.2020.3013998.

[20] M. P. Singh, M. Anbar, S. Manickam, M. S. Aladaileh, and B. A. Tayyeh, "A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking," Sensors, vol. 23, no. 9, p. 4441, 2023, doi: 10.3390/s23094441.

[21] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," IEEE Access, vol. 6, pp. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.

[22] A. D. Wiranata, Sunardi, and I. Riadi, "Tinjauan sistematis quality of service pada layanan jaringan software defined networking," INFOTECH: J. Technol. Inf., vol. 11, no. 2, pp. 247–252, Nov. 2025, doi: 10.37365/jti.v11i2.422.
[23] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," BMJ, vol. 372, p. n71, 2021, doi: 10.1136/bmj.n71.
[24] F. Chiti, R. Picchi, and L. Pierucci, "A survey on non-terrestrial quantum networking: Challenges and trends," Comput. Netw., vol. 252, p. 110668, 2024, doi: 10.1016/j.comnet.2024.110668.
[25] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," Biometrics, vol. 33, no. 1, pp. 159–174, 1977, doi: 10.2307/2529310.
[26] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: A novel SDN intrusion dataset," IEEE Access, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.
[27] M. S. Aladaileh, M. Anbar, A. J. Hintaw, I. H. Hasbullah, A. A. Bahashwan, T. A. Al-Amiedy, and D. R. Ibrahim, "Effectiveness of an entropy-based approach for detecting low- and high-rate DDoS attacks against the SDN controller," Sensors, vol. 23, no. 12, p. 5648, 2023, doi: 10.3390/s23125648.
[28] M. S. Elsayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique," J. Netw. Comput. Appl., vol. 191, p. 103160, 2021, doi: 10.1016/j.jnca.2021.103160.
[29] A. Albasheer, M. Anbar, S. Manickam, et al., "A federated CNN-LSTM model for DDoS detection in SDN," Electronics, vol. 13, no. 6, p. 1098, 2024, doi: 10.3390/electronics13061098.
[30] A. Alanazi and K. Aljuaid, "Federated deep learning for DDoS detection in SDN-IoT," Sensors, vol. 24, no. 4, p. 1252, 2024, doi: 10.3390/s24041252.
[31] I. Riadi, A. W. Muhammad, and Sunardi, "Neural network-based DDoS detection regarding hidden layer variation," J. Theor. Appl. Inf. Technol., vol. 95, no. 15, pp. 3684–3691, 2017.
[32] A. W. Muhammad, I. Riadi, and Sunardi, "DDoS detection using artificial neural network regarding variation of training function," Adv. Sci. Lett., vol. 24, no. 12, pp. 9163–9167, 2018, doi: 10.1166/asl.2018.13075.
[33] Sunardi, I. Riadi, and M. H. Akbar, "Penerapan metode static forensics untuk ekstraksi file steganografi pada bukti digital menggunakan framework DFRWS," J. RESTI, vol. 4, no. 3, pp. 576–583, 2020, doi: 10.29207/resti.v4i3.1906.
[34] M. H. Akbar, Sunardi, and I. Riadi, "Analysis of steganographic on digital evidence using general computer forensic investigation model framework," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 11, pp. 553–560, 2020, doi: 10.14569/IJACSA.2020.0111166.
[35] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K. K. R. Choo, and J. Iqbal, "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," IEEE Access, vol. 8, pp. 53972–53983, 2020, doi: 10.1109/ACCESS.2020.2976908.
[36] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "Lucid: A practical, lightweight deep learning solution for DDoS attack detection," IEEE Trans. Netw. Service Manag., vol. 17, no. 2, pp. 876–889, 2020, doi: 10.1109/TNSM.2020.2971776.
[37] M. V. de Assis, L. F. Carvalho, J. Lloret, and M. L. Proença, "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," Comput. Electr. Eng., vol. 86, p. 106738, 2020, doi: 10.1016/j.compeleceng.2020.106738.
[38] J. Cui, J. Long, E. Min, Q. Liu, and Q. Li, "Comparative study of CNN and RNN for deep learning based intrusion detection system," in Proc. CSS, 2018, pp. 159–170.
[39] H. Polat, M. Turkoglu, O. Polat, and A. Şahin, "A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks," Expert Syst. Appl., vol. 197, p. 116748, 2022, doi: 10.1016/j.eswa.2022.116748.
[40] H. Wang, L. Li, J. Zhao, and F. Wang, "DDosTC: A transformer-based network attack detection hybrid mechanism in SDN," Sensors, vol. 21, no. 15, p. 5047, 2021, doi: 10.3390/s21155047.
[41] K. Hu, Y. Li, and L. Shi, "TransDDoS: A transformer-based DDoS attack detection framework for software-defined networks," Comput. Netw., vol. 245, p. 110350, 2024, doi: 10.1016/j.comnet.2024.110350.
[42] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in Proc. IEEE Int. Carnahan Conf. Security Technol. (ICCST), 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.
[43] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in Proc. IEEE Security Privacy Workshops, 2018, pp. 29–35, doi: 10.1109/SPW.2018.00013.
[44] K. M. Sudar, P. Deepalakshmi, and P. M. Kumar, "DDoS attack detection in software-defined networks using machine learning algorithms," Wireless Pers. Commun., vol. 122, pp. 3017–3040, 2022, doi: 10.1007/s11277-021-09005-x.
[45] M. Ibrahim, F. Khan, A. Khan, and M. Asif, "An adversarial robustness study of deep learning-based DDoS detectors in SDN," Comput. Secur., vol. 138, p. 103686, 2024, doi: 10.1016/j.cose.2024.103686.
[46] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why should I trust you?: Explaining the predictions of any classifier," in Proc. ACM KDD, 2016, pp. 1135–1144, doi: 10.1145/2939672.2939778.
[47] M. F. Khan, A. Anjum, A. Saghar, et al., "Federated learning for intrusion detection in SDN-IoT: A privacy-preserving framework," Sensors, vol. 23, no. 11, p. 5018, 2023, doi: 10.3390/s23115018.
[48] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in Proc. ACM AISec, 2019, pp. 1–11, doi: 10.1145/3338501.3357370.
[49] Y. Safitri, I. Riadi, and Sunardi, "Mobile forensic for body shaming investigation using association of chief police officers framework," MATRIK J. Manaj. Teknik Inform. Rekayasa Komput., vol. 22, no. 3, pp. 651–664, 2023, doi: 10.30812/matrik.v22i3.3052.
[50] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments," Comput. Netw., vol. 62, pp. 122–136, 2014, doi: 10.1016/j.comnet.2013.10.014.
[51] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks," IEEE Trans. Netw. Service Manag., vol. 14, no. 2, pp. 487–497, 2017, doi: 10.1109/TNSM.2017.2701549.
[52] L. Liu, J. Xu, X. Li, and L. Liu, "A DDoS detection method based on feature engineering and machine learning in software-defined networks," Sensors, vol. 23, no. 13, p. 6176, 2023, doi: 10.3390/s23136176.
[53] M. R. Anwar, I. Ahmad, and S. M. Khan, "An entropy and machine learning based approach for DDoS attacks detection in software defined networks," Sci. Rep., vol. 14, p. 17789, 2024, doi: 10.1038/s41598-024-67984-w.
[54] S. Kaur, J. Singh, and N. Kaur, "Optimizing DDoS detection in SDNs through machine learning models," arXiv preprint arXiv:2505.13493, 2025.

[55] J. K. Samriya, R. Tiwari, J. J. P. C. Rodrigues, and R. Vijay, "Distributed denial of services (DDoS) attack detection in SDN using optimizer-equipped CNN-MLP," PLOS ONE, vol. 19, no. 12, p. e0312425, 2024, doi: 10.1371/journal.pone.0312425.

[56] A. D. Wiranata, R. Pribadi, and F. N. Hasan, "Penggunaan figma dan metode design thinking dalam user interface dan user experience untuk website e-commerce pasar grosir tradisional," J. Inf. Syst. Res. (JOSH), vol. 5, no. 3, pp. 870–880, 2024, doi: 10.47065/josh.v5i3.5210.

[57] A. D. Wiranata, F. N. Hasan, and Z. Munawar, Teknologi Informasi: Konsep Dasar dan Aplikasi. Klaten, Indonesia: Kaizen Media Publishing, 2024.

[58] A. D. Wiranata, S. Hanief, W. T. Saputro, and Muchlas, "Pelatihan mikrokontroler dasar Arduino UNO dan simulasi Tinkercad pada siswa rekayasa perangkat lunak SMK," J. Pengabdi. Masy. Inform., vol. 4, no. 1, pp. 11–18, 2026, doi: 10.30591/jpmi.v4i1.5841.

[59] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA method for processing on the network forensics in the event of an ARP spoofing attack," Edumatic: J. Pendidik. Inform., vol. 7, no. 1, pp. 195–204, 2023, doi: 10.29408/edumatic.v7i1.13197.

[60] I. Riadi, A. Yudhana, and G. P. I. Fanani, "Mobile forensic on MiChat messenger services using IDFIF V2 framework," Indonesian J. Electr. Eng. Comput. Sci., vol. 33, no. 1, pp. 612–621, 2024, doi: 10.11591/ijeecs.v33.i1.pp612-621.

[61] A. Yudhana, Z. Y. Rivai, and I. Riadi, "Assessing digital evidence availability in Discord phishing using ISO/IEC 27037 and anti-forensics analysis," Int. J. Adv. Data Inf. Syst., vol. 7, no. 1, pp. 22–34, 2026, doi: 10.25008/ijadis.v7i1.1518.

[62] A. D. Wiranata and F. N. Hasan, "Implementasi business intelligence dashboard untuk monitoring data penjualan UMKM," J. Sistem Inform. Manaj. Berbasis Komput. Cerdas, vol. 2, no. 4, pp. 1118–1128, 2023, doi: 10.55903/sinkron.v8i4.12923.