FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 12, December (Special Issue), 2025, pp 604 – 620
DOI: https://doi.org/10.33003/fjs-2025-0912-4261

A SYSTEMATIC TERTIARY STUDY OF DEEP LEARNING FOR INTRUSION DETECTION IN SOFTWARE-DEFINED NETWORKS

***Maryam Yamin Ahman, Saleh El-Yakub Abdullahi and Steve Adeshina Adetunji**

Nile University of Nigeria, Abuja, Nigeria

*Corresponding authors' email: 211333005@nileuniversity.edu.ng

ABSTRACT

Deep learning (DL) has emerged as a transformative approach to enhancing Intrusion Detection Systems (IDS) in Software-Defined Networking (SDN), enabling advanced detection of evolving and sophisticated cyber threats. Over the past few years, numerous secondary studies have reviewed the application of DL and other machine learning techniques for SDN security; however, no comprehensive tertiary study has systematically synthesized these reviews to identify overarching patterns, methodological gaps, and future research priorities. This paper addresses this gap by conducting a structured review of reviews published between 2019 and 2025, focusing exclusively on DL-based IDS within SDN environments. A total of 39 review and survey papers were analyzed across major scholarly databases, including IEEE Xplore, SpringerLink, ScienceDirect, and MDPI. The study consolidates insights on SDN security challenges, datasets, evaluation metrics, and prevalent DL models while critically highlighting persistent issues such as reliance on outdated datasets, lack of real-world validation, and limited exploration of low-rate and cross-domain attack scenarios. By mapping trends and identifying underexplored directions such as federated learning, adaptive multi-controller architectures, and SDN-IoT integrations, this work serves as a roadmap for researchers and practitioners seeking to design robust, scalable, and context-aware IDS solutions for next-generation SDN environments.

Keywords: Software-Defined Networking, Intrusion Detection Systems, Deep Learning, Tertiary Review, DDoS Attacks, Machine Learning, Network Security

INTRODUCTION

As modern networks become more complex and dynamic, Software-Defined Networking (SDN) has gained popularity for offering centralized control and improved flexibility (Aslam et al., 2024). While this model brings significant benefits, it also introduces new security challenges that require advanced monitoring tools like Intrusion Detection Systems (IDS). In recent years, Deep Learning (DL) methods have shown promise in strengthening IDS performance, especially in SDN settings. The SDN is a way of managing computer networks where the decision-making is separated from the devices that move data (Jain et al., 2024). While DL is a technique that teaches machines to learn and recognize patterns from data using many layers of neural networks. The IDS on the other hand is tool that monitors a network to spot attacks or any unusual activities (Yusra Sh. Ajaj et al., 2023).

In the digital age, SDN has emerged as a transformative paradigm that separates the control plane from the data plane, enabling centralized, programmable, and dynamic network management (Aslam et al., 2024). This architecture improves agility, scalability, and responsiveness, making SDN increasingly adopted across sectors such as telecommunications, cloud computing, and enterprise networks. However, the same architectural benefits introduce unique security challenges especially the vulnerability of the centralized controller, which becomes a high-value target for attackers. Although, IDS are essential for monitoring and detecting malicious activities, traditional IDS methods often fall short in SDN environments due to their inability to adapt to dynamic and complex traffic patterns. To address these limitations, recent studies have integrated DL techniques into IDS, since the models excel at learning complex patterns, enabling more accurate, adaptive, and real-time detection of sophisticated threats. Despite these advancements, the field remains in an early stage, with several unresolved issues and implementation challenges

While numerous secondary reviews have examined DL-based IDS in SDN, there is a lack of comprehensive tertiary studies reviews of reviews that synthesize findings, highlight patterns, and critically assess the research landscape. This gap limits the ability to identify persistent shortcomings or guide future research effectively. Existing tertiary studies focus on either ML-based IDS (Kumar & Alqahtani, 2023) or offer broad taxonomies of SDN literature (Babayigit et al., 2023) but none specifically analyze DL-based IDS in SDN. Table 1 shows the analysis between the existing studies and the current study. As result of this analysis, the current study addresses this gap by presenting the first focused tertiary review of DL-IDS survey literature in SDN. Through comparative analysis, we extract key trends, identify limitations, and suggest directions for future research. This work aims to support researchers and practitioners in understanding the evolving landscape, avoiding redundant efforts, and designing scalable, effective security strategies for SDN environments.

Table 1: Comparison of This Tertiary Review with Prior Related Studies

Feature / Focus Area	(Kumar & Alqahtani, 2023)	(Babayigit et al., 2023)	This Review
Study Type	Review of reviews (tertiary)	Review of reviews (tertiary)	Review of reviews (tertiary)
Primary Focus	ML techniques in IDS for SDN	Broad SDN research literature	DL-based IDS in SDN
Review Scope	Scenario-based, technique-based, attack-based IDS reviews	All SDN-related surveys (general and specific)	IDS reviews that apply DL in SDN security
Years Covered	2007-2022	2012–2021	2019-2025
Contribution Type	Systematic comparison of ML-based IDS in SDN	Meta-analysis of all SDN survey papers	Tertiary study of DL-IDS review papers in SDN
Analysis Approach	Categorization by technique, scenario and attack	Taxonomy by publication type, topic, journal, citation	(tertiary level review) or Synthesis of review scopes, key findings, and future directions.
Application Scope (IoT, cloud, wireless, etc.)	Not emphasized	Broad SDN research areas	Emphasis on DL applications in SDN including IoT/cloud
Gaps/Challenges Addressed	Identifies implementation challenges of ML-IDS	Highlights broad SDN research trends and gaps	Highlights DL-IDS research gaps (datasets, real-world applicability, model limitations)
Future Directions Provided	Yes – for ML in IDS for SDN	Yes – for general SDN research	Yes – focused on DL-specific IDS challenges in SDN
Novelty Claim	First structured ML-IDS review of reviews	First epistemological taxonomy of SDN reviews	First tertiary analysis of DL-based IDS reviews in SDN

Software-Defined Networking

SDN is a modern approach to networking where the control plane is separated from the data plane (Dabbagh et al., 2015). In this setup, devices such as switches and routers simply forward traffic, while a central controller manages how the entire network behaves. This separation simplifies administration, supports automation, and provides a full view of network activity. Table 2 shows the basic comparison between the traditional and SDN-based networks.

Table 2: Traditional VS Software Defined Networks

Feature	Traditional Networks	SDN
Control Plane	Distributed	Centralized
Network Visibility	Limited	Complete/global
Automation	Minimal	High
Configuration Changes	Device-by-device	Centralized
Flexibility	Rigid	Highly flexible
Maintenance Cost	Higher	Lower

Table 2 highlights the fundamental differences between traditional networks and Software-Defined Networks (SDN). In traditional networks, the control plane and data plane are tightly coupled within individual devices such as routers and switches, resulting in distributed control where each device independently makes forwarding decisions. In contrast, SDN decouples the control plane from the data plane and logically centralizes network control within a software-based controller, enabling centralized policy enforcement and global network management (Kreutz et al., 2015) (Nunes et al., 2014).

This architectural separation significantly affects network visibility. Traditional networks typically offer only localized, device level views of network state, whereas SDN provides a global view of the network through the centralized controller, allowing more comprehensive monitoring and control of traffic flows (Benzekki et al., 2016).

Automation is another key differentiating factor. Traditional networks rely heavily on manual, device-by-device configuration, which limits automation and increases operational complexity. SDN, on the other hand, supports a high degree of automation through programmable interfaces and centralized control logic, enabling consistent policy deployment and reducing configuration errors (Nunes et al., 2014) (Kreutz et al., 2015)

Flexibility and maintenance costs further distinguish the two paradigms. Traditional networks are generally rigid and costly to operate due to hardware dependence and manual management processes. SDN improves flexibility and scalability while reducing operational and maintenance costs by simplifying network management and minimizing manual intervention (Kreutz et al., 2013)(Benzekki et al., 2016).Overall, these distinctions illustrate how SDN enhances efficiency, agility, and cost effectiveness compared to traditional networking models.

Additionally, the SDN architecture is a form of network virtualization where the network controlling functions and forwarding functions are decoupled (Shaghaghi Arashand Kaafar, 2020). With this separation, innovative ideas have been proposed and an infrastructure network architecture gets a new direction of network evolution. A functional three layered SDN architecture and their available components are shown in Figure 1.

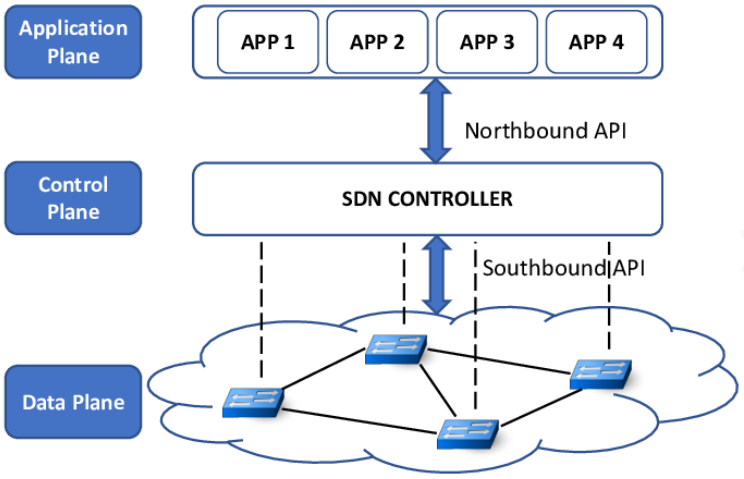

Figure 1: The SDN architecture

The Data Plane layer includes both physical and virtual switches. These devices carry out forwarding actions such as modifying, dropping, or sending packets, based on instructions from the controller. Virtual switches run in software (e.g., on Linux), while physical ones may use proprietary or open-source platforms (Shaghaghi Arashand Kaafar, 2020). However, the Control Plane Layer is the core of the SDN system. It runs controllers like OpenDaylight, Ryu, Beacon, POX, and NOX, which manage network behavior by generating flow rules and routing decisions. Moreover, it gathers information from the data plane and communicates with higher-level applications (Etxezarreta et al., 2023). While the Application Plane layer hosts network applications that define needs like bandwidth control, latency limits, or security rules. These apps communicate with the controller through APIs to influence how the network is managed (Bhuiyan et al., 2023).

Deep Learning Techniques for Intrusion Detection in SDN

Deep learning (DL) has become increasingly relevant in the development of intelligent Intrusion Detection Systems (IDS) for SDN (Mwanza & Kalita, 2023). These models (refer to Figure 2) consist of multiple layers that learn complex representations of input data, enabling them to detect subtle patterns and anomalies in network traffic. Unlike traditional IDS approaches that rely on fixed rules or manually engineered features, DL models can adapt to new attack types by learning from examples, making them better suited to the dynamic and evolving nature of threats in SDN environments. However, integrating DL into IDS for SDN introduces challenges (Mwanza & Kalita, 2023). The wide variability in traffic patterns, the presence of encrypted data, and the need for timely decision-making require models that are both accurate and efficient. Moreover, selecting an appropriate DL architecture depends on the availability of labeled data, the complexity of the network, and the computational overhead the system can tolerate. According to Lansky et al., (Lansky et al., 2021), DL approaches used for IDS in SDN fall into three categories: supervised, unsupervised, and hybrid models.

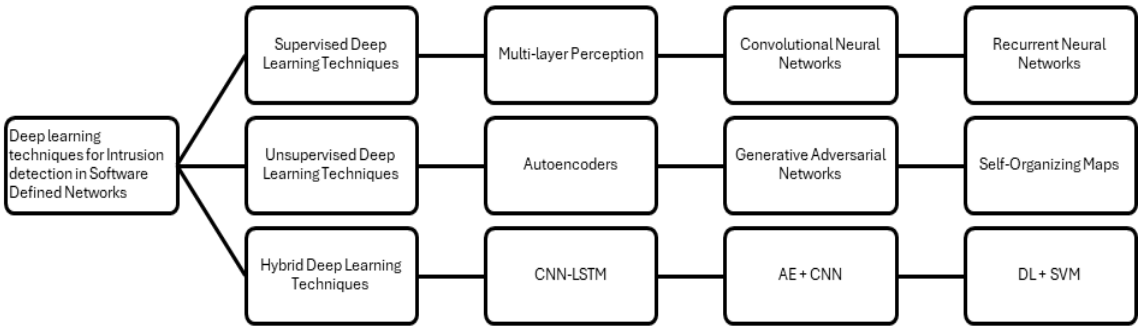

Figure 2: Deep learning techniques for Intrusion detection in Software Defined Networks

Supervised deep learning techniques rely on labeled datasets to train models that can distinguish between normal and malicious network traffic. These methods are highly effective when annotated data is available. Common architectures include the Multi-Layer Perception (MLP), which is a simple feed-forward neural network suitable for structured data, though it has limitations in handling temporal dependencies. Convolutional Neural Networks (CNNs), initially designed for image processing, have been adapted for intrusion detection due to their ability to capture spatial patterns in traffic features, while their shared weights and pooling layers enhance generalization (Sarker, 2021). Recurrent Neural Networks (RNNs) and their variant, Long Short-Term Memory (LSTM), are particularly effective for analyzing sequential traffic data, as LSTM mitigates the vanishing gradient problem and is capable of retaining long-term dependencies (Al-Selwi et al., 2024).

Unsupervised deep learning methods, on the other hand, do not require labeled datasets and are widely applied in anomaly detection. This makes them valuable in SDN environments where real-time labeling is often impractical (Aldweesh et al., 2020). Autoencoders (AE) are commonly used in this context;

they learn compressed representations of traffic data, and significant reconstruction errors can indicate anomalies. Generative Adversarial Networks (GANs), consisting of a generator and discriminator, can either produce synthetic attack data or detect irregular traffic patterns. Similarly, Self-Organizing Maps (SOM) transform high-dimensional traffic data into lower-dimensional maps, making it easier to identify abnormal clusters (Naskath et al., 2023).

Hybrid deep learning approaches combine multiple architectures to enhance detection performance by addressing the weaknesses of individual models (Mwanza & Kalita, 2023).Examples include CNN-LSTM models that capture both spatial and temporal patterns in network flows, as well as AE-CNN or GAN-CNN combinations that integrate unsupervised feature extraction with supervised classification. Some work has also demonstrated that hybrid deep learning architectures, particularly CNN–LSTM models enhanced with attention mechanisms, can effectively learn discriminative features from complex network traffic and achieve high intrusion detection accuracy, reflecting a broader shift toward adaptive and context-aware IDS designs (A. A. Ahmed et al., 2024). Another approach involves using deep learning for feature extraction followed by traditional classifiers, such as Support Vector Machines (SVM), for final prediction. These hybrid models have shown strong potential in improving accuracy and robustness, particularly when dealing with complex or imbalanced datasets.

In addition to these established techniques, several emerging methods are gaining attention. Deep Transfer Learning (DTL) enables knowledge learned in one domain to be applied to another, reducing training time and the reliance on large labeled datasets. However, its effectiveness often depends on proper domain adaptation (Sifa et al., 2018). Deep Reinforcement Learning (DRL) is another promising approach, combining reinforcement learning with deep networks to optimize decision-making. In the context of SDN, DRL can dynamically adapt intrusion detection rules or adjust controller policies based on detected threats (Liu et al., 2021)

MATERIALS AND METHODS

In conducting the literature review for this study, a systematic and comprehensive research methodology was employed. This methodology was designed to ensure the depth and relevance of the literature reviewed, focusing specifically on the intersection of deep learning techniques and Software Defined Networking (SDN). The steps to be taken are specified in the following subsections.

Search Strategy

A proper search strategy is a prerequisite for effective research (Jain et al., 2024). The search was carried out in a structured manner, which included the formulation of specific keywords, selection of appropriate databases, and a well-defined process for article inclusion and exclusion. To guide the literature search process, a combination of targeted keywords and Boolean operators was used to capture relevant review articles at the intersection of DL, intrusion detection, and SDN. The search strategy included variations of terms such as:

"*deep learning for securing SDN*," "*review or survey of deep learning in SDN*," "*IDS deep learning SDN*," "*deep learning for IDS in SDN*," and "*IDS for securing SDN review*."

To ensure inclusion of higher-level analyses, additional keywords such as "*tertiary study*," "*meta-review*," "*review of reviews*," and "*survey analysis*" were also incorporated. These terms were applied across titles, abstracts, and metadata fields within each selected digital library and search engine. This approach allowed for the identification of both secondary review and tertiary-level review of reviews studies relevant to the research focus.

Furthermore, to ensure a comprehensive and inclusive review of the literature on deep learning-based intrusion detection in SDN, this study utilized a combination of four major digital libraries and one scholarly search engine. The digital libraries; IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink were chosen for their rigorous peer-reviewed content and strong coverage of computer science and networking domains as seen in Table 3. Additionally, Google Scholar was used as a complementary search engine to widen the scope and capture relevant publications indexed across multiple platforms. Moreover, the search was limited to articles published from 2019 to 2025 to capture the most recent works and reviews in the field.

Table 3: Article Sources & Count

No.	Online Database / Source	Search Scope	Access Link	Article Count
1	IEEE Xplore / IEEE Access	Title, Abstract, Keywords	https://ieeexplore.ieee.org	8
2	SpringerLink (incl. Soft Computing)	Title, Abstract, Full Text	https://link.springer.com	11
3	ScienceDirect (Elsevier)	Title, Abstract, Full Text	https://www.sciencedirect.com	5
4	MDPI (incl. Symmetry and Sensors)	Title, Abstract, Keywords	https://www.mdpi.com	8
5	IJSER (International Journal of Scientific & Engineering Research)	Title, Abstract, Keywords	https://www.ijser.in/	1
6	International Journal of Advanced Natural Sciences and Engineering Researches (IJANSER)	Title, Abstract, Keywords	https://as-proceeding.com/index.php/ijanser/home	1
7	Soft Computing Research Society (SCRS)	Title, Abstract, Keywords	https://scrs.in	1
8	International Journal of Computer and Information (IJCI)	Title, Abstract, Keywords	https://ijci.journals.ekb.eg	1
9	International Journal of Innovative Science and	Title, Abstract, Keywords	https://www.ijisrt.com	1

No.	Online Database / Source	Search Scope	Access Link	Article Count
	Research Technology (IJISRT)			
10	International Journal of Network Security (IJNS)	Title, Abstract, Keywords	http://ijns.femto.com.tw	1
11	Conference Proceedings (ICEENG – Int'l Conf. on Electrical Engineering)	Title, Abstract	https://www.iceeng.cu.edu.eg	1
			Total	39

Study Selection and Screening Process

A structured multi-phase screening approach was adopted to identify and select relevant review articles focusing on the application of DL techniques in IDS within SDN environments. The initial pool comprised over 100 review and survey articles, including peer-reviewed journal publications, conference proceedings, preprints, and book chapters. These were retrieved from recognized scholarly databases and refined using specific inclusion parameters to maintain consistency and academic rigor.

The screening process was conducted in three stages. First, titles and abstracts were reviewed to exclude studies unrelated to deep learning, SDN, or network security, while those with partial relevance were retained. Next, full-text reviews were carried out to ensure the studies met most of the inclusion criteria, with papers lacking sufficient deep learning coverage or focusing on unrelated technologies being removed. Finally, the remaining papers underwent a detailed eligibility assessment to confirm their alignment with the research focus, technical depth, and contribution to the field, and only those fully meeting the criteria were included in the final analysis.

Inclusion and Exclusion Criteria

To ensure the precision and relevance of the selected literature, the following inclusion and exclusion criteria were applied:

Inclusion Criteria

i. Studies published between 2019 and 2025.
ii. Review or survey articles that focused on deep learning techniques for securing SDN.
iii. Articles discussing SDN security in relation to advanced machine learning models, with explicit analysis or application of deep learning methods.
iv. Papers that reviewed both ML and DL approaches were only included if the deep learning aspects were clearly discussed in the SDN context.
v. Studies that provided detailed descriptions of methodologies, summarized findings, and identified research gaps or future directions.

Exclusion Criteria

i. Articles that did not explicitly address SDN, or focused solely on traditional machine learning without incorporating deep learning.
ii. Publications outside the 2019–2025 time frame.
iii. Non-English language articles.
iv. Papers lacking methodological clarity or offering only superficial treatment of the subject matter.
v. Non-peer-reviewed content, such as editorials, opinion pieces, dissertations, or informal publications.

Data Extraction Process

After finalizing the list of eligible studies, a systematic data extraction process was conducted to synthesize insights from each paper. The extraction was structured around the following four dimensions:

i. Source and Publisher: To verify credibility and indexing status of each work (e.g., IEEE, Springer, ACM, etc.).
ii. Scope of the Review: Summarized the primary themes addressed, including focus areas such as DL model taxonomy, SDN architecture, attack types, or evaluation techniques.
iii. Key Findings: Highlighted the main contributions, synthesized trends, and significant observations made by the authors.
iv. Future Research Directions: Captured the gaps, limitations, and prospective directions for advancing the field, as proposed by the original authors.

These extracted data points enabled meaningful comparison and cross-referencing among the included studies, serving as the basis for the thematic synthesis presented in later sections of this review.

Article Source Distribution

Following the data extraction process, the final pool of 39 selected articles was categorized based on their source of publication. This classification highlights the publishing platforms most frequently contributing to the body of research on deep learning-based intrusion detection in SDN. Majority of the articles were sourced from SpringerLink, including journals such as Soft Computing, which accounted for 11 publications. This was followed by IEEE Xplore/IEEE Access and MDPI journals (Sensors, Symmetry), each contributing 8 articles, while Elsevier/ScienceDirect contributed 5 articles. A smaller number of articles were drawn from conference proceedings, and lesser-known journals such as IJSER, IJCI, and IJISRT, reflecting the broader but less frequent scholarly activity in those outlets. The visual representation in Figure 3 further illustrates the distribution, underscoring the concentration of relevant literature in a few key academic databases.

This distribution offers useful insights for future researchers seeking high-quality review papers on deep learning for SDN security, indicating that SpringerLink, IEEE, and MDPI are currently the most prolific sources for such content.

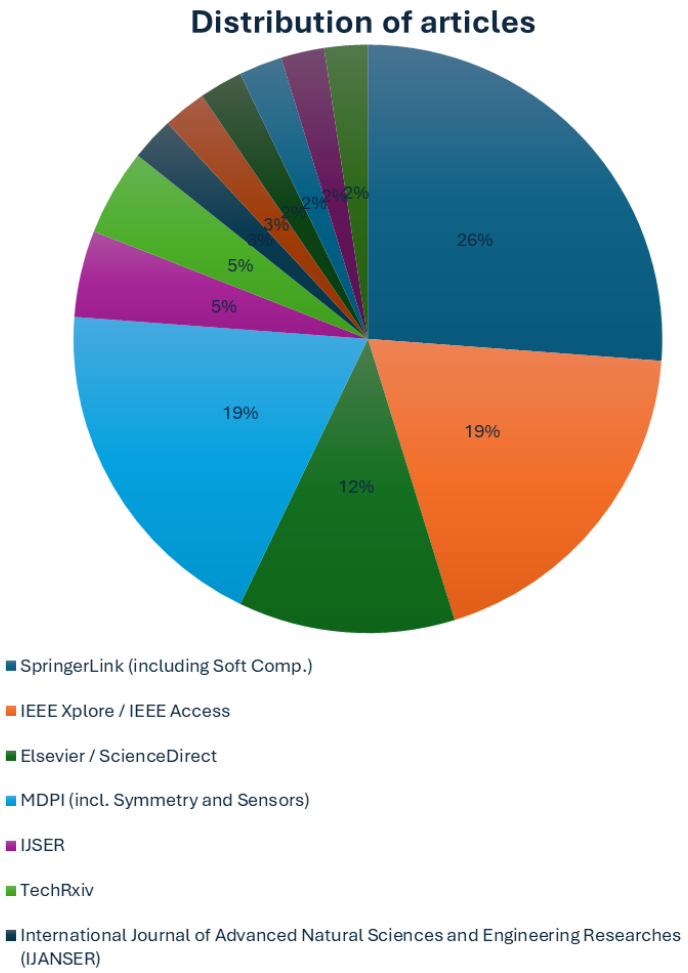

Figure 3: Summary Of Distribution of Articles

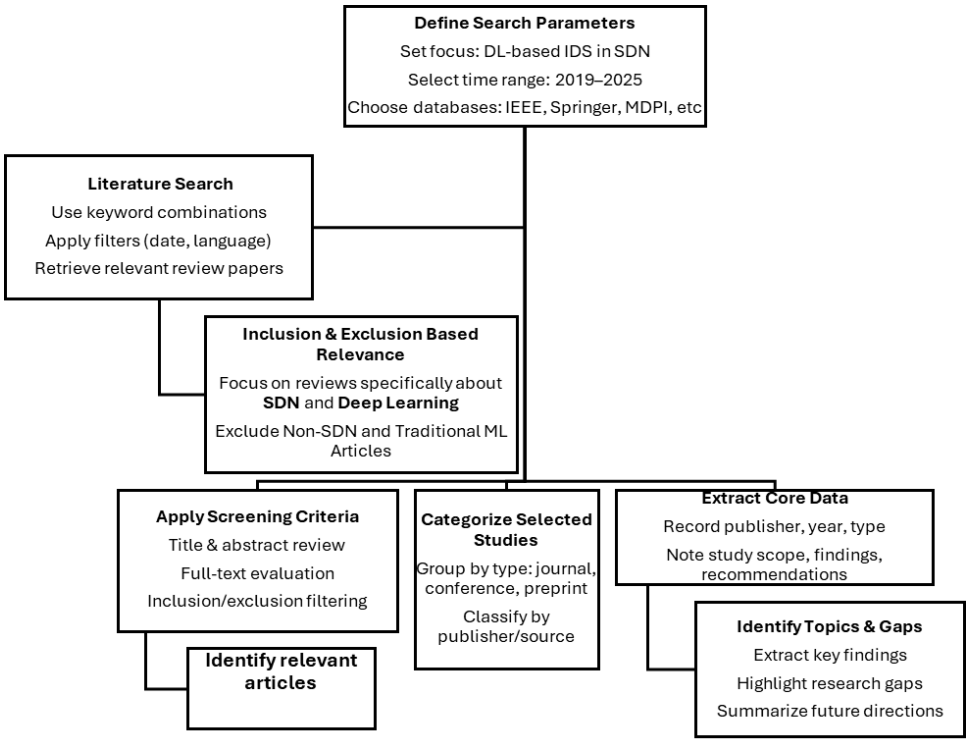

Figure 4: Summary Of Research Process

RESULTS AND DISCUSSION

Principal findings

The analysis, covering peer-reviewed literature published between 2019 and 2025, focuses only on studies that explicitly address both DL methods and SDN-specific security concerns, while excluding those lacking substantial relevance. The reviewed works are organized by scope, contributions, findings, and publication timelines to provide a clear picture of how DL has been applied in this domain, the trends and common practices observed, and the research gaps that remain. This approach highlights the current landscape of DL-based IDS for SDN, offering insights into existing progress and identifying areas where future research efforts should be directed. A consolidated summary of these findings is presented in Table 4.

Table 4: Summary of Literature Findings

Reference	Year	Scope/Focus	Key findings/Contribution
(Arevalo Herrera & Camargo, 2019)	2019	Survey of ML based SDN Security Proposals	Points out that many ML-based SDN proposals lack proper data collection mechanisms, mitigation strategies, and comprehensive attack coverage. Recommends development of open SDN-specific datasets, broader attack detection schemes, and defined implementation frameworks for ML in SDN
(Sultana et al., 2019)	2019	Evaluation of ML and DL methods for SDN-based NIDS	Highlights that existing intrusion detection datasets are outdated and inaccurate for modern SDN research. DL approaches outperform traditional ML in logical modeling, but face challenges in feature selection and efficient packet processing. Recommends future research on optimizing model parameters, improving computational efficiency, addressing controller bottlenecks, and developing feature selection strategies that enhance DL performance. Suggests designing real-time NIDS-enabled centralized controllers as a potential future direction.
(J. Singh & Behal, 2020)	2020	Overview of SDN layered architecture and DDoS vulnerabilities	Highlights controller as a key attack target and identifies persistent challenges like scalability, secure switch communication, and lack of realistic traffic datasets. Recommends secure multi-controller synchronization, improved flow authentication, low-rate DDoS detection, and realistic distributed topologies for simulation.
(Al-Mi'ani et al., 2021)	2021	Overview of SDN, its security challenges, and review of DL-based IDS	Highlights SDN's centralized vulnerability; compares IDS types and shows DL's strength in detecting unknown attacks. Recommends reducing overhead, improving QoS, and using blockchain for integrity.
(Ajiya Ahmad et al., 2021)	2021	Survey of intrusion detection techniques in SDN	Reviews various intrusion detection approaches in SDN and their strengths/weaknesses. Emphasizes that single-controller setups are unreliable for IDS and calls for comprehensive SDN-specific datasets with diverse attack types to improve detection outcomes
(Gupta & Grover, 2021)	2021	Review of ML approaches for DDoS detection in SDN	Compares ML techniques for DDoS detection in SDN, highlighting reliance on outdated datasets and lack of SDN-specific traffic. Recommends focusing on high-quality feature extraction, exploring alternatives to CNN, and integrating fuzzy logic for enhanced detection
(Cui et al., 2021)	2021	Review of DDoS detection mechanisms in SDN	Reviews various DDoS detection techniques in SDN, noting SVM and SOM dominance, neglect of feature selection, and underuse of OpenFlow for attack detection. Emphasizes the need for dynamic feature updating, low-rate and early-stage DDoS detection, and better handling of emerging attack types.
(Shinan et al., 2021)	2021	Review of ML-based botnet detection in traditional and SDN	Reviews ML techniques for botnet detection in SDN and traditional networks. Emphasizes the need for high-quality datasets, notes limitations of offline and flow-based methods, and recommends graph-based approaches for improved real-time accuracy.
(Valdovinos et al., 2021)	2021	Review of DDoS detection/mitigation strategies in SDN with taxonomy	Provides a taxonomy of DDoS strategies in SDN including ML, NFV, blockchain, and others. Highlights lack of standards for access control at the application level, and poor-quality datasets with labeling and validation issues. Recommends building SDN-specific datasets and ML frameworks suited to flow-based traffic. Advocates hybrid ML/DL with emerging tech.
(Mittal et al., 2023)	2021	Systematic review of ML/DL-based DDoS detection in SDN	Identifies missing public datasets with diverse traffic types (legit, low-rate, high-rate, flash); emphasizes class imbalance, lack of multiclass classification, inadequate preprocessing, and need for real-time validation. Recommends developing lightweight DL models and automation for defense response
(Dahiya et al., 2024)	2024	Comparative analysis of SDN applications, datasets, and ML/DL-based IDS	Highlights importance of IDS evaluation metrics and SDN's fine-grained security advantage. Warns of SDN's centralized vulnerability. Recommends creation of up-to-date datasets, advancement of ML/DL

Reference	Year	Scope/Focus	Key findings/Contribution
			models to improve accuracy and adaptability, and strengthening of SDN security frameworks against evolving cyber threats.
(Jain et al., 2024)	2024	Outlines SDN architecture, DDoS features, and defense strategies	Reviews SDN's DDoS vulnerabilities and defense methods. Highlights lack of attention to feature selection, low-rate DDoS attacks, and novel threats like crossfire/link flooding. Calls for adaptive, real-time DL-based models, intelligent switches, and standardized evaluation frameworks to improve DDoS detection and mitigation
(Yzzogh & Benaboud, 2025)	2025	Comparative analysis of ML -DL models for SDN-IDS	Assesses ML models tailored to attack types in SDN. Emphasizes trade-offs between accuracy and resource use. Recommends high-quality datasets, attack-specific customization, and real-time, scalable IDS solutions for detecting low-rate and zero-day attacks
(Janabi et al., 2024)	2024	Surveys ML-based IDS Implementation challenges in SDN	Highlights limitations in real-time detection due to resource strain, outdated datasets, and reliance on predefined threat models. Calls for adaptive, distributed IDS frameworks, real-world testing, encrypted traffic analysis, and AI-driven policy automation to enhance scalability and resilience.
(Vijayan & Anitha, 2025)	2025	Reviews ML and DL-based IDS techniques in SDN	Identifies LSTM as the most studied DL model with accuracy the most used performance metric, it also highlights reliance on outdated datasets like NSL-KDD. Recommends better feature selection, exploring semi/unsupervised learning, federated AI-enabled switches, and multi-attack classification using newer datasets.
(Boruah & Sarmah, 2025)	2025	Reviews ML/DL techniques for DDoS detection in SDN	Highlights strengths of ensemble and hybrid DL models (e.g., CNN-LSTM) for detecting low- and high-rate DDoS attacks. Notes limited real-world testing and challenges with stealthy threats. Recommends use of DRL, decentralized detection across controllers, and unified frameworks for robust DDoS mitigation
(C. Singh & Jain, 2024)	2024	Survey of DDoS attacks detection & mitigation in SDN-IoT network	Highlights difficulty in real-time differentiation of malicious vs. legitimate traffic. Notes lack of adaptive mitigation and underexplored SDN-IoT collaboration. Recommends advanced detection, dynamic defense strategies, cross-layer cooperation, and adaptable SDN-IoT infrastructure
(Alasali & Dakkak, 2023)	2023	Review of Emerging DDoS threats and defense gaps in SDN	Analyzes modern DDoS forms and challenges in SDN defense. Emphasizes controller bottlenecks, low-rate attack detection, lack of SDN-specific datasets, and ANN parameter burden. Recommends distributed detection using info-theory metrics, multi-controller load balancing, and enhanced switch-level security modules
(Ali et al., 2023a)	2023	Comparative analysis of ML vs. DL for DDoS in SDN	Compares CNN and SVM for DDoS detection in SDN, noting SVM's superior consistency and CNN's training complexity. Recommends custom, diverse datasets and real-time hybrid ML/DL models tested on actual SDN traffic
(Ali et al., 2023b)	2023	Systematic review of ML/DL-based DDoS detection in SDN	Highlights limited reporting on training/testing time and heavy use of offline datasets. Emphasizes need for real-world validation, balanced SDN-specific datasets, and portable, dynamic DL models that can adapt to evolving threats like zero-day attacks.
(Yusra Sh. Ajaj et al., 2023)	2023	Review of DL-based cyber-attack detection in SDN-IoT	Emphasizes the need for AI-driven detection in IoT networks. Highlights the gap in IoT-specific datasets, noting MQTT/AMQP traffic as critical. Recommends development of custom SDN-IoT datasets to enhance detection reliability and accuracy
(Sharma & Saxena, 2022)	2022	Comparative analysis of DDoS detection in SDN	Evaluates DDoS detection models across metrics and classifiers. Highlights controller overhead, high dimensionality, and feature selection challenges. Confirms Deep CNN outperforms conventional methods, recommending deeper exploration of DL for accurate and efficient detection.
(Nadeem et al., 2023)	2023	Comparative analysis of DL methods for botnet DDoS in SDN	Analyzes DL methods for detecting botnet-based DDoS in SDN, identifying CNN as effective for real-time detection with manageable training time. Recommends extending to low-rate and spoofed attacks using hybrid DL models and multi-controller SDN setups
(Latif Yaser et al., n.d.)	2022	Comparative analysis of ML-based DDoS detection in SDN	Reviews ML-based methods for DDoS in SDN. Highlights RNN's suitability for time-series data and CNN's accuracy in threat detection. Recommends combining CNN with other ML models (e.g., ANN) to improve accuracy and reduce classification latency

Reference	Year	Scope/Focus	Key findings/Contribution
(Mwanza & Kalita, 2023)	2023	Survey of DL techniques for DDoS detection in SDN	Evaluates DL use for detecting DDoS in SDN. Notes weaknesses in experimental setups (virtual vs. physical), dataset design flaws (e.g., IP removal), and generalization limits for zero-day attacks. Recommends continuous model updating, leveraging GPUs, and applying transfer/multi-task learning to improve accuracy and efficiency.
(Hirsi Abdi et al., n.d.)	2023	Review of traditional and AI-based security in SDN	Surveys traditional and AI-based security mechanisms in SDN. Highlights critical threats like DoS, side-channel, and topology poisoning, and control plane vulnerabilities. Recommends developing secure data plane architectures, AI-based IDS, multi-controller designs, and interoperability frameworks to fortify SDN security.
(N. Ahmed et al., 2022)	2022	Review of ML/DL-based NIDS in SDN	Reviews advancements in ML/DL-based NIDS for SDN. Notes DL's superiority in feature selection and accuracy, but highlights CNN's complexity, real-time detection issues, outdated datasets, and SDN controller bottlenecks. Recommends lightweight DL models, standardized evaluation frameworks, improved dataset generation, and strategies to reduce data processing overhead in large-scale SDN environments.
(Negera et al., 2022)	2022	Review of ML/DL techniques for botnet detection in SDN-IoT networks	Investigates ML/DL approaches for botnet detection in SDN-enabled IoT. Notes RF's popularity for ML, and DNN's strength in DL for detecting unseen attacks in real time. Stresses the need for benchmark datasets and the development of lightweight models to support efficient real-time detection.
(Bahashwan et al., 2023)	2023	Systematic review of ML/DL-based DDoS detection in SDN	Reviews ML, DL, and hybrid approaches to DDoS detection in SDN. Finds a shift from ML to DL for better performance with large data. Identifies lack of realistic datasets, limited focus on low-rate/prevention strategies, and controller overload. Recommends use of distributed controllers, P4-programmed switches, and blockchain to enhance resilience and scalability.
(Alashhab et al., 2022)	2022	Survey of ML-based LDDoS detection in SDN	Surveys ML approaches for LDDoS detection in SDN. Highlights shift in DDoS behavior to low-rate patterns, lack of SDN-specific LDDoS datasets, and limitations of single-controller setups in simulations. Recommends building realistic LDDoS datasets, testing in large-scale SDN settings, and developing lightweight DL models for scalable and adaptive detection
(Musa et al., 2024)	2024	Survey of DoS detection in SDN using ML/DL	Reviews ML and DL approaches for DoS detection in SDN, noting most are evaluated on short-term or synthetic datasets, lacking real-world validation. Stresses the need for integration with existing security mechanisms, use of adversarial ML, and creation of scalable solutions with robust datasets.
(Wang & Li, 2024)	2024	Systematic review of recent DDoS detection progress in SDN environments	Highlights the scarcity of real, large-scale SDN-specific datasets; most studies emphasize high-rate DDoS and detection accuracy while neglecting LDDoS, scalability, efficiency, and deployment constraints. Recommends adaptive feature selection, scalable multi-controller systems, optimized switch-based detection, broader metrics (e.g., detection time), and targeted security approaches for IoT, 5G, and blockchain-integrated SDNs
(Su et al., 2024)	2024	Reviews technologies for DDoS attack detection and mitigation in current SDN environments	Emphasizes that most detection occurs at the control/data plane and is limited to single-controller simulations. Identifies challenges in distinguishing DDoS from flash events and highlights the lack of standardized security protocols. Recommends enhancing application-plane security, improving multicontroller synchronization and load balancing, and creating clearer detection strategies to differentiate between malicious and legitimate traffic spikes.
(Da Silva Ruffo et al., 2024)	2024	Empirical literature review of state-of-the-art deep learning-based NIDS for SDN security	Highlights overreliance on outdated public datasets, underuse of unsupervised DL and RL techniques, and lack of diversity in DL models. Recommends future research on newer models (e.g., GCNs, AEs), generative models (e.g., WGAN), integration of explainable AI (e.g., SHAP, LIME), and exploration of decentralized NIDS to improve scalability, explainability, and accuracy in real-world SDN settings
(Aslam et al., 2024)	2023	Detailed taxonomy of SDN DDoS detection and mitigation methods	Identifies gaps such as lack of SDN-specific datasets, underexplored feature selection, overreliance on simulated/single-controller setups, and limited real-world validation. Recommends creating SDN-tailored datasets with proper feature subsets, focusing on low-rate DDoS detection, building scalable DL-based solutions for multi-

Reference	Year	Scope/Focus	Key findings/Contribution
			controller environments, and implementing/test mitigation strategies in real-world SDN setups to balance detection accuracy, scalability, and system efficiency.
(Taheri et al., 2023)	2023	Comprehensive survey on deep learning algorithms for securing SDN	Identifies the need for large-scale, high-quality datasets as a core challenge for DL effectiveness. Highlights the high computational demands of DL training and the limited focus on attack types beyond DDoS. Notes the potential of VNFs to enhance SDN security but underscores the lack of standard interfaces between SDN and NFV. Recommends creating labeled datasets from production networks, exploring online and transfer learning (DTL), and standardizing SDN-NFV interfaces.
(Chetouane & Karoui, 2022)	2022	Survey of ML methods used for DDoS detection in SDN environments	Highlights scalability and reliability challenges in SDN due to single-controller limitations. Emphasizes the lack of high-quality datasets and effective feature selection strategies. Notes vulnerabilities of ML/DL to training set poisoning and the time-consuming nature of DL training. Recommends implementing distributed multi-controller platforms, clusters to prevent single-point failure, enhancing communication security, and developing robust defenses against data poisoning attacks
(Mostafa et al., 2024)	2024	Literature survey on SDN-based IDSs and their ML/DL implementations	Reviews recent implementations of IDS using DL models on modern datasets (e.g., CICIDS2017, CICDDoS2019, INSDN2020). Emphasizes the need for improved security mechanisms to better detect SDN-specific attacks. Highlights how GPU acceleration improves inference time during model training/testing. Suggests future research should focus on optimizing DL architectures using modern GPU capabilities for better performance.
(Mustafa et al., 2024)	2024	Comprehensively surveys ML and DL algorithms used for intrusion detection in SDN	Highlights limited availability of real-world SDN datasets. Notes that SVM is the most used algorithm, followed by K-means, while DNN stands out due to its high performance with large datasets. Recommends improving dataset quality, developing adaptive learning techniques, and implementing real-time analysis methods. Suggests exploring distributed IDS architectures and scalable ML solutions for growing SDN environments.

According to Table 4, the main findings from the reviewed literature were grouped into recurring themes to show how DL is being applied to improve SDN security, particularly through IDS. These themes highlight the key areas of focus in current research and reveal gaps that require further investigation:

DDoS and DoS Detection in SDN Using Deep Learning

The centralization of the control plane in SDN makes them highly vulnerable to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, including more evasive variants like Low-Rate DDoS (LDDoS). Such attacks can overwhelm the SDN controller, resulting in network degradation or failure. To address this, numerous studies have explored the use of DL to develop robust, adaptive, and intelligent detection and mitigation frameworks tailored for SDN environments. Several studies have reviewed these approaches such as C. Singh & Jain (C. Singh & Jain, 2024) in the year 2024 which explored DDoS detection and mitigation in SDN-IoT systems between 2014–2023, highlighting attack variations and challenges unique to SDN-IoT networks. Similarly, J. Singh & Behal in 2020 (J. Singh & Behal, 2020) examined 70 papers between 2013–2020 and discussed SDN's layered architecture strengths and vulnerabilities in the face of DDoS, including evolving attack variants. J. Singh & Behal in 2023 (Alasali & Dakkak, 2023) presented an in-depth review of DDoS attacks targeting SDN, drawing from 70 papers between 1948–2020 and emphasizing deployment challenges and open research issues. The work of Ali et al., 2023 (Ali et al., 2023a) (Ali et al., 2023b) all conducted comparative analyses of DL and ML approaches across two studies: the first compared 10 key papers (2016–2020), highlighting the superior accuracy of SVM-based models; the second analysed 45 papers (2018–2022), stressing critical gaps such as lack of real-world validation, high training times (especially for CNNs), and poor zero-day attack detection. They called for portable, balanced, and efficient DL models backed by robust preprocessing and online training strategies.

Furthermore, Sharma & Saxena in 2022 (Sharma & Saxena, 2022) evaluated 15 studies from 2018 to 2022, focusing on performance metrics, while Nadeem et al., 2023 (Nadeem et al., 2023) only focused on botnet-based DDoS attacks in SDN, proposing lightweight DL approaches using accessible features. In 2021, Gupta et al., (Gupta & Grover, 2021) reviewed 18 articles of 2016 to 2020, providing a comparative assessment of ML techniques, and Latif et al., (Latif Yaser et al., n.d.) reviewed 10 papers between 2018–2020, offering recommendations based on ML-based detection systems. It is evident that Mwanza & Kalita in 2023 (Mwanza & Kalita, 2023) surveyed 19 papers from 2018 to 2022, identifying weaknesses in current DL-based detection techniques. So also the work of Cui et al., 2021 (Cui et al., 2021) conducted one of the largest reviews (143 papers from 2010 to 2022) covering generational processes, advantages, and open issues in DDoS detection strategies. In 2023, Bahashwan et al., (Bahashwan et al., 2023) systematically analyzed 70 papers between 2014 to 2022, categorizing ML, DL, and hybrid methods, while in 2022, Alashhab et al., 2022 (Alashhab et al., 2022) focused only on 10 studies between 2019 to 2022 specifically addressing LDDoS threats in SDN using ML.

Moreover, other reviews brought diverse perspectives such as the work of Valdovinos et al., 2021 (Valdovinos et al., 2021) which categorized DDoS detection techniques into statistical,

SDN-specific, and emerging technologies like blockchain and NFV; Musa et al., 2024 (Musa et al., 2024) surveyed 50 papers between 2020 to 2023 covering both ML and DL strategies and emphasized future research directions; Mittal et al., 2023 (Mittal et al., 2023) analyzed 32 DL-focused studies between 2018 to 2021; and recently Wang & Li in 2024 (Wang & Li, 2024) provided a comprehensive overview of DDoS detection methods and preprocessing techniques in 52 papers between 2015 to 2023. Further contributions include Su et al., 2024 (Su et al., 2024) who reviewed 91 studies from 2003 to 2023, identifying critical findings across detection technologies, Aslam et al., 2024 (Aslam et al., 2024) developed a taxonomy of 268 DDoS defense solutions between 1994 to 2023, and Chetouane & Karoui in 2022 (Chetouane & Karoui, 2022) concentrated on ML-based DDoS detection in SDN environments. A moment ago, Jain et al., 2024 (Jain et al., 2024) synthesized 114 works from 2004 to 2024, critiquing overemphasis on accuracy at the expense of adaptability and evaluation consistency. They stressed the need for real-time traffic analysis, dynamic flow control, and intelligent switches. And Boruah & Sarmah in 2025 (Boruah & Sarmah, 2025) assessed 15 studies between 2019 to 2024, highlighting effective methods like ensemble learning, hybrid CNN-LSTM models, and adaptive bandwidth control. However, they raised concerns about reliance on custom datasets and lack of generalizability to real-world deployments. Future directions included exploring deep reinforcement learning and developing distributed detection systems.

Deep Learning-Based Intrusion Detection Systems (IDS) for SDN

Intrusion detection remains a critical element in securing SDN, where the centralized control plane, while beneficial for network programmability and management, also introduces new vulnerabilities. The programmability of SDN facilitates dynamic and scalable IDS, particularly Network Intrusion Detection Systems (NIDS), which are capable of monitoring and analyzing traffic across multiple layers for real-time anomaly detection. As threats grow more complex, researchers have increasingly applied ML and DL to improve the effectiveness and adaptability of these systems. For instance, the work of Ajiya et al., 2021 (Ajiya Ahmad et al., 2021) conducted a review of 23 papers between 2015 and 2021, highlighting the strengths and limitations of various intrusion detection techniques and recommending improvements in scalability and detection accuracy. They noted inconsistencies in dataset selection and underreporting of model generalization. Again, the work of Ahmed et al., 2022 (N. Ahmed et al., 2022) further reviewed 47 papers between 2011 and 2021, focusing specifically on ML/DL-based NIDS in SDN. They emphasized the need for intelligent systems capable of adapting to evolving threats.

Additionally, Silve et al., 2024 (Da Silva Ruffo et al., 2024) offered a review of 105 papers published between 2021 and 2024. Their analysis of DL-based NIDS solutions underscored emerging techniques and recommended improved model efficiency and practical deployments. In 2019, Sultana et al., (Sultana et al., 2019) reviewed only 5 studies between 2011 and 2016, evaluating DL approaches in SDN-NIDS and identifying the potential of deep models to detect unknown attacks. They proposed future enhancements such as integration with blockchain and improvements in Quality of Service (QoS) during traffic analysis. In 2021, Al-Mi'ani et al., (Al-Mi'ani et al., 2021) reviewed 32 articles published between 2018 and 2021, classifying intrusion detection mechanisms into host-based, network-based, signature-based, anomaly-based, specification-based, and hybrid systems. Their study confirmed the effectiveness of DL in detecting complex threats and suggested blockchain integration and reduced operational overhead as future research directions. In 2024, Dahiya et al., (Dahiya et al., 2024) reviewed 17 papers between 2010 and 2022, highlighting the benefits of SDN for granular security control. They emphasized the role of up-to-date datasets and evaluation metrics and recommended further studies on scalable and adaptive IDS frameworks tailored to evolving attack vectors.

Furthermore, Yzzogh & Benaboud in 2025 (Yzzogh & Benaboud, 2025) conducted a comparative analysis of 34 papers between 2016 and 2023, focusing on ML-based IDS model performance. They revealed that behavioral profiling and predictive analytics yield higher detection accuracy, but often at the cost of computational efficiency. Their findings highlighted the trade-off between detection accuracy and real-time resource constraints, with simpler models proving more suitable for deployment. In 2024, Janabi et al., 2024 (Janabi et al., 2024) reviewed 30 papers between 2015 and 2023, identifying several IDS limitations, including excessive resource consumption, dependency on outdated datasets, and reduced effectiveness against novel attacks. The review called for distributed IDS architectures, privacy-preserving traffic analysis, and real-world validation of AI-enabled IDS models. While in recent time, Vijayan et al., 2025 (Vijayan & Anitha, 2025) et al analyzed 20 studies between 2019 and 2023. Their review showed that 35% of models employed LSTM, followed by CNN (10%) and Random Forest (20%). NSL-KDD remained the most used dataset despite its age, while CICIDS2017 and INSDN datasets were underutilized despite offering more realistic traffic patterns. The authors advocated for better feature selection, semi-supervised learning, federated learning, and the expansion of models to detect diverse and evolving threats. Also, in (Mustafa et al., 2024) has evaluated 19 studies between 2014 and 2020, pointing out dataset limitations and emphasizing the effectiveness of SVM, K-Means, and Deep Neural Networks (DNN) in intrusion detection for SDNs. They recommended adaptive learning, load balancing, and distributed ML frameworks to accommodate network growth and threat evolution. Lastly, in (Mostafa et al., 2024) presented a review at ICEENG, covering IDS developments between 2016 and 2023. They analyzed DL-based detection models using datasets like CICIDS2017, CICDDoS2019, and INSDN2020. Their findings stressed the role of GPU acceleration in improving inference performance and suggested exploring next-generation architectures and novel deep learning methods for optimized SDN security.

Deep Learning Techniques and Architectures Applied to SDN Security

The integration of SDN has brought about a paradigm shift in network management by decoupling the control and data planes, enabling centralized control and dynamic programmability. Deep learning's ability to model complex and non-linear patterns in high-dimensional data makes it particularly suitable for addressing the evolving threat landscape in SDN. Although, these features introduced new and sophisticated security vulnerabilities. However, the traditional security mechanisms often fall short in responding to the dynamic and distributed nature of SDN environments. As a result, there has been growing interest in leveraging DL techniques to enhance the detection, mitigation, and prevention of security threats in SDN ecosystems. According to literatures, numerous reviews have evaluated the role of DL in enhancing SDN security, analyzing its performance across

various use cases such as intrusion detection, botnet mitigation, and adaptive threat response. For instance, the work of Arevalo Herrera Juliana & Camargo in 2019 (Arevalo Herrera Juliana & Camargo, 2019) surveyed 23 papers published between 2013 and 2019, classifying them into two broad categories: machine learning techniques for identifying general anomalies or specific attacks, and IDS frameworks tailored to SDN. They identified the common datasets, experimental testbeds, and supporting tools frequently used by researchers, thus providing a foundational reference for further development in the field.

Yusra Sh. Ajaj et al (Yusra Sh. Ajaj et al., 2023) surveyed 19 articles published between 2016 and 2021, exploring the use of deep learning in detecting and preventing cyber-attacks within SDN-based IoT environments. They focused on the threats to SDN-IoT systems, identifying significant challenges in current research, especially the overreliance on outdated or non-IoT-specific datasets. The authors emphasized the need for realistic and IoT-relevant datasets that include modern communication protocols such as MQTT and AMQP. They proposed hybrid dataset generation techniques that combine public data sources with customized traffic, and recommended standardized frameworks for dataset creation, labeling, and sharing to improve reproducibility and cross-study comparability.

Furthermore, the work of Hirsi et al., (Hirsi Abdi et al., n.d.) reviewed 82 papers published from 2019 to 2023. The study first surveyed traditional SDN security solutions including encryption, authorization, authentication, firewalls, and secure protocols before transitioning to AI-based approaches. They evaluated how ML and DL techniques are being applied to detect advanced threats in SDN environments. The review also investigated Moving Target Defense (MTD) mechanisms for enhancing security at both the data and control planes, offering insights into dynamic protection strategies. In 2022, Nagera et al., 2022 (Negera et al., 2022) analyzed 50 studies published from 2016 to 2022, with a focus on preventing botnet attacks in SDN-enabled IoT networks using ML. The study offered targeted recommendations, particularly in regard to improving real-time detection capabilities and system adaptability. While in 2021, Shinan et al., 2021 (Shinan et al., 2021) reviewed 28 papers published between 2006 and 2021, examining machine learning techniques for detecting botnets across both traditional and SDN networks. The study provided a comparative analysis and identified gaps in generalization and detection speed, proposing future research directions to improve botnet identification accuracy. Recently in 2023, Taheri et al., 2023 (Taheri et al., 2023) conducted a comprehensive survey of 38 papers published between 2017 and 2022. The review focused on the utilization of various DL algorithms for SDN security, including models like CNNs, RNNs, and hybrid architectures. The study identified key research gaps, such as insufficient use of real-time data, limited model scalability, and a lack of cross-platform validation. The authors proposed solutions such as model lightweighting, multi-layered detection frameworks, and greater emphasis on attack type generalization to enhance the robustness and deployment readiness of DL models. Consequently, all these reviews affirm the growing maturity of DL applications in SDN security. However, recurring challenges remain, including the scarcity of standardized and context-relevant datasets, high computational overhead of deep models, and limited real-world testing. Addressing these issues through collaborative dataset initiatives, model optimization, and real-time evaluation frameworks is critical for enabling effective and scalable DL-based security solutions for SDN.

Research Gaps and Discussions

We thoroughly identified research gaps from the existing literature within the specified period. The following subsections outlines these gaps by providing descriptions and proposed solutions based on research findings.

Detection Challenges

Addressing detection challenges is essential for building robust, efficient, and trustworthy DL-driven IDS solutions capable of securing dynamic SDN environments. In this aspect, we are going to discuss these challenges in different ways as follows:

Challenges in Real-Time Traffic Classification

According to (C.Singh & Jain, 2024), (Shinan et al., 2021), (J.Singh & Behal, 2020), and (Ali et al., 2023b) current detection techniques struggle to accurately differentiate legitimate traffic from malicious traffic, particularly in real-time contexts and lack of dynamic strategies that adapts to changing patterns or evolving attacks like zero-day or unknown attacks. This challenge is exacerbated by the adaptive nature of DDoS attacks, especially low-rate DDoS (LDoS) variants, which often mimic regular traffic patterns, making real-time differentiation difficult. As a result, many studies prioritize detection accuracy, focusing on simpler binary classification models, but these methods often overlook the complexities of multiclass classification (Mittal et al., 2023) (Md.Rayhan Ahmed et al., n.d.). Furthermore, there is limited focus on the trade-offs between accuracy and efficiency (Wang & Li, 2024). While high accuracy is desirable, overly complex models that achieve it may significantly compromise processing speed and real-time performance, making them impractical for operational use.

Low-rate DDoS (LDoS) Detection

It is evidenced that a substantial amount of research has focused on detecting high-rate DDoS attacks, there remains a significant gap in the detection of low-rate DDoS attacks, (Alasali & Dakkak, 2023), (Cui et al., 2021), (Wang & Li, 2024), and (Bahashwan et al., 2023). These attacks are growing in prevalence and are difficult to detect as they are designed to blend in with regular traffic, evading detection by traditional methods. Despite their potentially damaging impact, research into LDoS detection remains limited. This emphasizes the need for tailored detection approaches capable of identifying these subtle and adaptive threats.

Data Overlap and Confusion

In this aspect, a major challenge in DDoS detection arises from the similarity between malicious traffic and legitimate traffic spikes, often referred to as flash events (Alashhab et al., 2022). This overlap can result in high false positive rates, where normal traffic is incorrectly flagged as malicious, or false negatives, where actual attacks go undetected. Thus, addressing this data overlap is crucial for developing reliable detection systems that minimize both false alarms and missed attacks, ultimately ensuring more effective network security.

Hyperparameter Tuning

The successful deployment of ML and DL models for intrusion detection hinges on effective hyperparameter tuning to optimize model performance. However, this aspect is often overlooked in research, particularly in DL-based IDS studies. Without proper hyperparameter optimization, models may fail to adapt effectively across different network environments, limiting their overall performance. Proper tuning ensures that

these models can deliver both accuracy and efficiency in real-world, production-level deployments.

Lack of Comprehensive Solutions
It's noticeable that significant gap in the current research is the overwhelming focus on detection without considering comprehensive solutions that incorporate attack prevention and mitigation (Arevalo Herrera & Camargo, 2019), (Bahashwan et al., 2023), and (Aslam et al., 2024). Few studies address the integration of automated defensive responses to detected attacks, which could significantly enhance overall network resilience (Mittal et al., 2023). Developing and implementing automated response mechanisms would allow SDN systems to automatically defend against attacks, making them more adaptive and resilient in the face of evolving threats.

Data and Datasets
Despite the advances in literature, challenges remain in terms of dataset imbalance, scalability, and representativeness of emerging threats, highlighting the critical role of comprehensive and domain-specific datasets in improving the performance and generalization of DL-based IDS in SDN. These challenges are as follows:

Lack of Quality Datasets
There is a pronounced need for standardized, high-quality datasets that reflect real-world SDN environments (N. Ahmed et al., 2022), (Mittal et al., 2023), (Alashhab et al., 2022), (Mustafa et al., 2024), (J. Singh & Behal, 2020), (Arevalo Herrera Julianaand Camargo, 2019), (Alasali & Dakkak, 2023), (Aslam et al., 2024), (Sultana et al., 2019), (Chetouane & Karoui, 2022), and (Valdovinos et al., 2021). As a result, many datasets used in studies suffer from class imbalance, missing attributes, unlabeled out of date data and fail to adequately represent diverse traffic types, such as legitimate, high-rate, and low-rate traffic (Valdovinos et al., 2021). The lack of realistic and comprehensive datasets limits the effectiveness of training and evaluation for intrusion detection models. Without sufficient variation in the data, models cannot generalize well across different network scenarios, making them less reliable when deployed in operational settings. Future research should focus on creating realistic up to date data sets that represent actual SDN flow.

Feature Selection Issues
Effective feature selection remains a critical challenge in intrusion detection systems (Sharma & Saxena, 2022) (Cui et al., 2021) (Valdovinos et al., 2021). Many traditional ML models struggle to identify the most relevant features for improving detection accuracy, leading to suboptimal model performance. This issue is compounded by the use of outdated datasets that do not capture the latest attack patterns, making it difficult to develop models that can detect emerging threats. Improving feature selection techniques is vital for enhancing the accuracy and robustness of both traditional and deep learning-based IDS.

Preprocessing Limitations
Preprocessing is a crucial step in optimizing DL model training, yet many studies have not applied suitable preprocessing techniques (Mittal et al., 2023). Datasets used in many studies are generated through simulated environments, often relying on a single SDN controller in a virtual setup, and data is typically collected over very short timeframes sometimes only one day (Musa et al., 2024), (Su et al., 2024), (Aslam et al., 2024), and (Alashhab et al., 2022). This approach does not accurately reflect the complexity or the dynamic nature of real-world SDN networks. Furthermore, many studies fail to report training and testing times, which are essential for assessing the feasibility of these models in real-world or production environments (Ali et al., 2023b). The lack of this information makes it difficult to evaluate the efficiency and scalability of proposed methods, which are critical for large-scale and real-time applications.

Modeling Techniques
Normally, modeling techniques improve SDN-based IDS by enhancing accuracy, adaptability, and resilience against both known and unknown attacks. The challenges bounded in these modelling techniques are as follows:

Deep Learning Advantages
Deep Learning techniques have demonstrated superior performance in detecting attacks, achieving higher accuracy compared to traditional ML models (Mwanza & Kalita, 2023). However, they require substantial computational resources and extensive training times, which can present a barrier for real-time detection (Taheri et al., 2023). Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs) are some of the most popular models used because of their ability to detect unseen attacks (Negera et al., 2022) . These models are particularly effective in detecting novel or unseen attack patterns, making them suitable for adaptive and dynamic security solutions. However, these approaches still face the challenge of long training times, which can affect their usability in real-time applications.

Insufficient Exploration of Unsupervised Deep Learning techniques
Despite the promising potential of unsupervised DL in identifying novel or zero-day attacks, there remains a significant gap in the research landscape. Most studies still rely heavily on supervised learning techniques, limiting the scope of detection strategies (da Silva Ruffo et al., 2024). Despite their promise, unsupervised deep learning remains underexplored. Expanding research into unsupervised learning could enhance the diversity and resilience of IDS models, making them more effective at detecting emerging and previously unseen threats.

Implementation Challenges
The following implementation challenges show that while many solutions look promising in theory, they still need to prove themselves in real-world SDN environments:

Single Point of Failure
According to (Alashhab et al., 2022) and (Wang & Li, 2024), reliance on a single SDN controller introduces a single point of failure which create vulnerabilities that can severely impact detection and mitigation efforts. If the controller becomes compromised or overwhelmed, it could lead to system-wide failures. While implementing a multi-controller setup can help mitigate this risk by distributing the workload and enhancing network resilience. However, this approach introduces additional complexities, including the need for efficient synchronization between controllers and the management of load balancing, which could complicate system implementation and increase overhead.

Scalability Issues
It's evident in (Singh & Behal, 2020) and (Chetouane & Karoui, 2022) that as SDN networks continue to grow in size and complexity, scalability becomes a major challenge for

IDS. While as the volume of network traffic increases, it requires the IDS model to handle larger datasets with more diverse attack patterns, and higher throughput. Moreover, it ensure that IDS systems can continue to operate effectively across larger, distributed networks while maintaining low latency and high accuracy remains an unresolved challenge that requires further exploration.

Real-time Intrusion Detection

As in (Ali et al., 2023b), a significant limitation of current intrusion detection methods is their reliance on offline datasets, which are not conducive to real-time detection. When the network threats evolve rapidly, the ability to detect and respond to attacks in real-time is critical for effective security. Improving the real-time capabilities of IDS is essential to meet the demands of modern SDN networks, where speed and accuracy are vital for preventing widespread damage.

Limited Evaluation of Solutions

Several works proposed IDS models and techniques that have not been adequately tested in realistic SDN environments. Although, some of them rely on simulated environments that fail to capture the operational complexities and real-world conditions of actual SDN networks (Musa et al., 2024). Without realistic testing, it is difficult to assess the true effectiveness and practicality of these models for deployment in live systems. Future research must focus on evaluating proposed solutions in realistic environments to ensure their reliability and performance in operational settings.

CONCLUSION

The integration of DL into SDN-based intrusion detection has significantly advanced the state of network security, offering sophisticated tools for identifying both known and novel threats. However, this review highlights that despite considerable progress, several critical challenges remain unresolved. Chief among these are real-time traffic classification difficulties, the persistent threat of low-rate DDoS attacks, and a lack of reliable, high-quality datasets that accurately represent modern SDN environments. Many current detection models emphasize accuracy but neglect operational efficiency, scalability, or deployment viability in live network conditions. Furthermore, there is limited attention to the full security lifecycle detection, prevention, and mitigation leaving SDN infrastructures vulnerable to fast-evolving attacks. The underutilization of unsupervised DL techniques, inadequate feature selection strategies, and insufficient preprocessing practices continue to hinder model robustness and generalizability. In parallel, practical implementation faces barriers such as single-point controller vulnerabilities, real-time detection constraints, and a lack of large-scale evaluation in real-world SDN environments. These limitations call for a paradigm shift in how IDS are designed, trained, and validated within the SDN context. The future research should prioritize the following directions:

i. Development of Lightweight and Adaptive Detection Models: There is a pressing need for models that balance high detection accuracy with low computational overhead to enable real-time intrusion detection without compromising network performance. Exploring hybrid models and energy-efficient architectures can bridge this gap.
ii. Enhanced Focus on Low-Rate DDoS Detection: Given their stealthy nature and increasing prevalence, future studies should prioritize tailored techniques for identifying low-rate DDoS attacks, including behavioral and temporal traffic analysis approaches.
iii. Creation and Standardization of Realistic Datasets: To improve model training and evaluation, researchers should develop standardized SDN-specific datasets that reflect real traffic conditions, include diverse attack types (especially modern and multi-vector threats), and are collected over extended timeframes using varied topologies and multiple controllers.
iv. Exploration of Unsupervised and Semi-Supervised Learning: Given the dynamic threat landscape, deeper exploration of unsupervised and semi-supervised deep learning methods is essential. These approaches can improve detection of zero-day and previously unseen attacks, increasing the adaptability of IDS frameworks.
v. Integration of Automated Mitigation Mechanisms: Future IDS frameworks should go beyond passive detection by integrating automated, context-aware response mechanisms. This would enable SDN systems to proactively adapt to threats in real time, significantly improving network resilience.
vi. Real-World Evaluation and Benchmarking: Emphasis should be placed on validating detection models in realistic, large-scale SDN environments rather than limited simulation settings. This includes using multi-controller architectures and varied network traffic scenarios to assess scalability, latency, and accuracy under operational stress.
vii. Improved Feature Engineering and Preprocessing Pipelines: Refining feature selection processes and adopting rigorous preprocessing techniques will enhance model performance. Leveraging metaheuristic optimization methods and dimensionality reduction can further strengthen detection robustness and generalizability.

By addressing these open challenges, future research can lay the groundwork for more practical, scalable, and intelligent IDS solutions that are truly suited for the dynamic and programmable nature of SDN environments. The ultimate goal remains the creation of holistic, real-time security systems capable of not only identifying but also preventing and neutralizing threats autonomously without compromising the performance or agility that make SDN so valuable.

REFERENCES

Ahmed, A. A., Aliyu, A. A., Ibrahim, M., Abdulkadir, S., Ahmad, M. A., Tanko, S. A., & Umaru, I. A. (2024). Enhancing Network Security Through Integrated Deep Learning Architectures And Attention Mechanisms. Fudma Journal Of Sciences, 8(6), 407–415. https://doi.org/10.33003/fjs-2024-0806-3010

Ahmed, N., Ngadi, A. Bin, Sharif, J. M., Hussain, S., Uddin, M., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Ullah, S. S., & Zuhra, F. T. (2022). Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction. In Sensors (Basel, Switzerland) (Vol. 22, Issue 20). NLM (Medline). https://doi.org/10.3390/s22207896

Ajiya Ahmad, A., Boukari, S., Musa Bello, A., & Aliyu Muhammad, M. (2021). A Survey of Intrusion Detection Techniques on Software Defined Networking (SDN). International Journal of Innovative Science and Research Technology, 6(8), 521–533. www.ijisrt.com

ALASALI, T., & DAKKAK, O. (2023). EXPLORING THE LANDSCAPE OF SDN-BASED DDOS DEFENSE: A HOLISTIC EXAMINATION OF DETECTION AND MITIGATION APPROACHES, RESEARCH GAPS AND PROMISING AVENUES FOR FUTURE EXPLORATION. International Journal of Advanced Natural Sciences and Engineering Researches, 7(4), 327–349. https://doi.org/10.59287/ijanser.726

Alashhab, A. A., Zahid, M. S. M., Azim, M. A., Daha, M. Y., Isyaku, B., & Ali, S. (2022). A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. In Symmetry (Vol. 14, Issue 8). MDPI. https://doi.org/10.3390/sym14081563

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 105124. https://doi.org/10.1016/j.knosys.2019.105124

Ali, T. E., Chong, Y. W., & Manickam, S. (2023a). Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN. Applied Sciences (Switzerland), 13(5). https://doi.org/10.3390/app13053033

Ali, T. E., Chong, Y. W., & Manickam, S. (2023b). Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. Applied Sciences (Switzerland), 13(5). https://doi.org/10.3390/app13053183

Al-Mi'ani, N., Anbar, M., Sanjalawe, Y., & Karuppayah, S. (2021). Securing Software Defined Networking Using Intrusion Detection System - A Review. Communications in Computer and Information Science, 1487 CCIS, 417–446. https://doi.org/10.1007/978-981-16-8059-5_26

Al-Selwi, S. M., Hassan, M. F., Abdulkadir, S. J., Muneer, A., Sumiea, E. H., Alqushaibi, A., & Ragab, M. G. (2024). RNN-LSTM: From applications to modeling techniques and beyond—Systematic review. Journal of King Saud University - Computer and Information Sciences, 36(5), 102068. https://doi.org/https://doi.org/10.1016/j.jksuci.2024.102068

Arevalo Herrera, J., & Camargo, J. E. (2019). A Survey on Machine Learning Applications for Software Defined Network Security. In International Conference on Applied Cryptography and Network Security (pp. 70–93). Springer. https://doi.org/10.1007/978-3-030-29729-9_4

Arevalo Herrera Juliana and Camargo, J. E. (2019). A Survey on Machine Learning Applications for Software Defined Network Security. In R. and L. Z. and M. S. and M. W. and W. L. and Z. K. Zhou Jianying and Deng (Ed.), Applied Cryptography and Network Security Workshops (pp. 70–93). Springer International Publishing.

Aslam, N., Srivastava, S., & Gore, M. M. (2024). A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN. Arabian Journal for Science and Engineering, 49(3), 3533–3573. https://doi.org/10.1007/s13369-023-08075-2

Babayigit, B., Ulu, B., & Abubaker, M. (2023). Survey Studies of Software-Defined Networking: A Systematic Review and Meta-analysis. In Engineering Journal (Vol. 27, Issue 10, pp. 33–66). Chulalongkorn University, Faculty of Fine and Applied Arts. https://doi.org/10.4186/ej.2023.27.10.33

Bahashwan, A. A., Anbar, M., Manickam, S., Al-Amiedy, T. A., Aladaileh, M. A., & Hasbullah, I. H. (2023). A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. In Sensors (Vol. 23, Issue 9). MDPI. https://doi.org/10.3390/s23094441

Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. Security and Communication Networks, 9(18), 5803–5833. https://doi.org/10.1002/sec.1737

Bhuiyan, Z. A., Islam, S., Islam, Md. M., Ullah, A. B. M. A., Naz, F., & Rahman, M. S. (2023). On the (in)Security of the Control Plane of SDN Architecture: A Survey. IEEE Access, 11, 91550–91582. https://doi.org/10.1109/ACCESS.2023.3307467

Boruah, M. S., & Sarmah, S. (2025). A Review on Detection and Mitigation Strategies of DDoS Attack in SDN Environment using Machine Learning and Deep Learning. Proceedings of 2025 3rd International Conference on Intelligent Systems, Advanced Computing, and Communication, ISACC 2025, 754–761. https://doi.org/10.1109/ISACC65211.2025.10969352

Chetouane, A., & Karoui, K. (2022). A Survey of Machine Learning Methods for DDoS Threats Detection Against SDN (I. Jemili & M. Mosbah, Eds.; Vol. 1564, pp. 99–127). Springer International Publishing. https://doi.org/10.1007/978-3-030-99004-6_6

Cui, Y., Qian, Q., Guo, C., Shen, G., Tian, Y., Xing, H., & Yan, L. (2021). Towards DDoS detection mechanisms in Software-Defined Networking. In Journal of Network and Computer Applications (Vol. 190). Academic Press. https://doi.org/10.1016/j.jnca.2021.103156

da Silva Ruffo, V. G., Brandão Lent, D. M., Komarchesqui, M., Schiavon, V. F., de Assis, M. V. O., Carvalho, L. F., & Proença, M. L. (2024). Anomaly and intrusion detection using deep learning for software-defined networks: A survey. Expert Systems with Applications, 256. https://doi.org/10.1016/j.eswa.2024.124982

Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. (2015). Software-defined networking security: pros and cons. IEEE Communications Magazine, 53(6), 73–79. https://doi.org/10.1109/MCOM.2015.7120048

Dahiya, S., Sehrawat, H., Kharb, S., & Siwach, V. (2024). A comprehensive analysis of threat vectors in software-defined networking. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-024-19679-7

Etxezarreta, X., Garitano, I., Iturbe, M., & Zurutuza, U. (2023). Software-Defined Networking approaches for intrusion response in Industrial Control Systems: A survey. International Journal of Critical Infrastructure Protection, 42, 100615. https://doi.org/10.1016/j.ijcip.2023.100615

Gupta, S., & Grover, D. (2021). A Comprehensive Review on Detection of DDoS Attacks using ML in SDN Environment. Proceedings - International Conference on Artificial

Intelligence and Smart Systems, ICAIS 2021, 1158–1163. https://doi.org/10.1109/ICAIS50930.2021.9395987

Hirsi Abdi, A., Salh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (n.d.). Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. https://doi.org/10.1109/ACCESS.2023.0322000

Jain, A. K., Shukla, H., & Goel, D. (2024). A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks. Cluster Computing. https://doi.org/10.1007/s10586-024-04596-z

Janabi, A. H., Kanakis, T., & Johnson, M. (2024). Survey: Intrusion Detection System in Software-Defined Networking. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3493384

Kreutz, D., Ramos, F. M. V., & Verissimo, P. (2013). Towards secure and dependable software-defined networks. Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, 55–60. https://doi.org/10.1145/2491185.2491199

Kreutz, D., Ramos, F. M. V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103(1), 14–76. https://doi.org/10.1109/JPROC.2014.2371999

Kumar, G., & Alqahtani, H. (2023). Machine Learning Techniques for Intrusion Detection Systems in SDN-Recent Advances, Challenges and Future Directions. In CMES - Computer Modeling in Engineering and Sciences (Vol. 134, Issue 1, pp. 89–119). Tech Science Press. https://doi.org/10.32604/cmes.2022.020724

Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., Hosseinzadeh, M., & Rahmani, A. M. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, 9, 101574–101599. https://doi.org/10.1109/ACCESS.2021.3097247

Latif Yaser, A., Hussein, M., & Mousa, H. M. (n.d.). International Journal of Computers and Information (IJCI) Techniques for DDoS Attack Detection in SDNs: A Comparative Study. https://ijci.journals.ekb.eg/64

Liu, X., Yu, W., Liang, F., Griffith, D., & Golmie, N. (2021). On deep reinforcement learning security for Industrial Internet of Things. Computer Communications, 168, 20–32. https://doi.org/10.1016/j.comcom.2020.12.013

Md. Rayhan Ahmed, Salekul Islam, Swakkhar Shatabda, A. K. M. Muzahidul Islam, & Md. Towhidul Islam Robin. (2021). Intrusion Detection System in Software-Defined Networks Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques-A Using Machine Learning and Deep Learning Techniques-A Comprehensive Survey Comprehensive Survey. Tech. https://doi.org/10.36227/techrxiv.17153213.v1

Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: a systematic review. In Soft Computing (Vol. 27, Issue 18, pp. 13039–13075). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/s00500-021-06608-1

Mostafa, N., Metwally, K., & Badran, K. (2024). Survey on SDN-based Intrusion Detection Systems. ICEENG 2024 - 14th IEEE International Conference on Electrical Engineering, 317–322. https://doi.org/10.1109/ICEENG58856.2024.10566429

Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A. M., & Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks - Current Research Solutions. IEEE Access, 12, 17982–18011. https://doi.org/10.1109/ACCESS.2024.3360868

Mustafa, Z., Amin, R., Aldabbas, H., & Ahmed, N. (2024). Intrusion detection systems for software-defined networks: a comprehensive study on machine learning-based techniques. Cluster Computing. https://doi.org/10.1007/s10586-024-04430-6

Mwanza, N. P., & Kalita, J. (2023). Detecting DDoS Attacks in Software Defined Networks Using Deep Learning Techniques: A Survey. International Journal of Network Security, 25(2), 360. https://doi.org/10.6633/IJNS.202303

Nadeem, M. W., Goh, H. G., Aun, Y., & Ponnusamy, V. (2023). Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques. IEEE Access, 11, 49153–49171. https://doi.org/10.1109/ACCESS.2023.3277397

Naskath, J., Sivakamasundari, G., & Begum, A. A. S. (2023). A Study on Different Deep Learning Algorithms Used in Deep Neural Nets: MLP SOM and DBN. Wireless Personal Communications, 128(4), 2913–2936. https://doi.org/10.1007/s11277-022-10079-4

Negera, W. G., Schwenker, F., Debelee, T. G., Melaku, H. M., & Ayano, Y. M. (2022). Review of Botnet Attack Detection in SDN-Enabled IoT Using Machine Learning. In Sensors (Vol. 22, Issue 24). MDPI. https://doi.org/10.3390/s22249837

Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials, 16(3), 1617–1634. https://doi.org/10.1109/SURV.2014.012214.00180

Sarker, I. H. (2021). Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. SN Computer Science, 2(6), 420. https://doi.org/10.1007/s42979-021-00815-1

Shaghaghi Arash and Kaafar, M. A. and B. R. and J. S. (2020). Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions. In G. M. and A. D. P. and G. D. Gupta Brij B. and Perez (Ed.), Handbook of Computer Networks and Cyber Security: Principles and Paradigms (pp. 341–387). Springer International Publishing. https://doi.org/10.1007/978-3-030-22277-2_14

Sharma, A., & Saxena, P. (2022). Comparative Analysis of DDoS Attacks Detection Systems in Software defined Networks. In Artificial Intelligence and Communication

Technologies (pp. 283–296). Soft Computing Research Society. https://doi.org/10.52458/978-81-955020-5-9-29

Shinan, K., Alsubhi, K., Alzahrani, A., & Ashraf, M. U. (2021). Machine learning-based botnet detection in software-defined network: A systematic review. Symmetry, 13(5). https://doi.org/10.3390/sym13050866

Sifa, R., Paurat, D., Trabold, D., & Bauckhage, C. (2018). Simple Recurrent Neural Networks for Support Vector Machine Training (pp. 13–22). https://doi.org/10.1007/978-3-030-01424-7_2

Singh, C., & Jain, A. K. (2024). A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network. E-Prime - Advances in Electrical Engineering, Electronics and Energy, 8. https://doi.org/10.1016/j.prime.2024.100543

Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. In Computer Science Review (Vol. 37). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2020.100279

Su, Y., Xiong, D., Qian, K., & Wang, Y. (2024). A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network. In Electronics (Switzerland) (Vol. 13, Issue 4). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13040807

Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2), 493–501. https://doi.org/10.1007/s12083-017-0630-0

Taheri, R., Ahmed, H., & Arslan, E. (2023). Deep learning for the security of software-defined networks: a review. In Cluster Computing (Vol. 26, Issue 5, pp. 3089–3112). Springer. https://doi.org/10.1007/s10586-023-04069-9

Valdovinos, I. A., Pérez-Díaz, J. A., Choo, K. K. R., & Botero, J. F. (2021). Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. In Journal of Network and Computer Applications (Vol. 187). Academic Press. https://doi.org/10.1016/j.jnca.2021.103093

Vijayan, A., & Anitha, A. (2025). A Review of Intrusion Detection Systems in Software Defined Networks. 3rd International Conference on Electronics and Renewable Systems, ICEARS 2025 - Proceedings, 859–864. https://doi.org/10.1109/ICEARS64219.2025.10940260

Wang, H., & Li, Y. (2024). Overview of DDoS Attack Detection in Software-Defined Networks. IEEE Access, 12, 38351–38381. https://doi.org/10.1109/ACCESS.2024.3375395

Yusra Sh. Ajaj, Bilal R. Al-Kaseem, & Yousif Al-Dunainawi. (2023). Cyber Attacks in SDN-Based IoT Environment: A Review. Al-Iraqia Journal of Scientific Engineering Research, 2(3). https://doi.org/10.58564/ijser.2.3.2023.89

Yzzogh, H., & Benaboud, H. (2025). A comprehensive overview of machine learning for intrusion detection in software-defined networking. In Innovations in Systems and Software Engineering. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/s11334-025-00604-6