Software-Defined Networking Security Detection Strategies and Their Limitations with a Focus on Distributed Denial-of-Service for Small to Medium-Sized Enterprises

WAINWRIGHT, Ruth, BAGHERI, Maryam, SALAMA, Abdussalam and SAATCHI, Reza <http://orcid.org/0000-0002-2266-0187>

applied sciences

MDPI

Review

Software-Defined Networking Security Detection Strategies and Their Limitations with a Focus on Distributed Denial-of-Service for Small to Medium-Sized Enterprises

Ruth Wainwright [1], Maryam Bagheri [1], Abdussalam Salama [1] and Reza Saatchi [2,*]

[1] School of Computing and Digital Technologies, Sheffield Hallam University, City Campus, Sheffield S1 1WB, UK; ruth.wainwright@student.shu.ac.uk (R.W.); maryam.bagheri@shu.ac.uk (M.B.); abdussalam.salama@shu.ac.uk (A.S.)

[2] School of Engineering and Built Environment, Sheffield Hallam University, City Campus, Sheffield S1 1WB, UK

* Correspondence: r.saatchi@shu.ac.uk

Abstract

Software-defined Networking (SDN) has immense potential for network security due to its centralized control and programmability. However, this concentration provides an attractive attack vector for Distributed Denial-of-Service (DDoS), particularly in small and medium-sized enterprises (SMEs) with limited budget and network security resources. This study presents a systematic review of the articles reporting SDN-based DDoS detection and mitigation, focusing on SMEs. Querying eight major databases (2020–2025) resulted in 59 articles (14 reviews, 45 experimental). Two distinct models emerged: (i) lightweight and efficient models and (ii) high-accuracy hybrid deep learning models, with lower resource efficiency. These models were predominantly validated through simulations, raising concerns around their overfitting as SME traffic is heterogeneous and bursty. Mitigation of the attacks leveraged the programmability of SDN but has been rarely evaluated alongside detection models and almost never in live SDN-SME settings. This study's findings highlighted a lightweight screening solution at the network edge, which is resource-aware and employs a minimal trigger interface to the controller for mitigation rule insertion. This conceptual design aligns well with the constraints of SMEs by minimising the computational load on the central controller while enabling an efficient and rapid response to network security.

Keywords: software-defined networks; small and medium-sized enterprises; distributed denial-of-service attack; intrusion detection and mitigation; computer network security

Academic Editor: Luis Javier Garcia Villalba

Received: 5 October 2025
Revised: 13 November 2025
Accepted: 15 November 2025
Published: 21 November 2025

Citation: Wainwright, R.; Bagheri, M.; Salama, A.; Saatchi, R. Software-Defined Networking Security Detection Strategies and Their Limitations with a Focus on Distributed Denial-of-Service for Small to Medium-Sized Enterprises. *Appl. Sci.* **2025**, *15*, 12389. https://doi.org/10.3390/app152312389

1. Introduction

The advent of Software-defined Networking (SDN) has resulted in a huge shift in the concept of network management, with the separation of the data plane from the control plane, thus facilitating centralised configuration and traffic management. The flexibility inherent in an SDN environment provides a promising landscape for the development of network security solutions and, in particular, Distributed Denial-of-Service (DDoS) attacks, which are one of the easiest and most disruptive cybersecurity threats.

The premise behind DDoS attacks is fundamentally simple—the target network is overwhelmed with malicious traffic from a range of geographically varied sources.

Usually, this is carried out by botnets on compromised Internet of Things (IoT) or host devices. These attacks have the potential to disrupt or downgrade legitimate services, and for small and medium-sized enterprises (SMEs), the consequences can be very damaging. The addition of SDN means an attack on a central point can be detrimental to the network's operation, and the company's day-to-day business can be halted quickly. This issue is examined in more detail later in this article. In terms of the financial cost, reports (2017/18) estimated that the average cost of a "successful" DDoS attack on an SME ranged between 106,000 US dollars and 1.6 million US dollars [1], but this depends on the downtime and duration.

Having highlighted that the centralised nature of SDN can also be its security weakness, it can also offer a way to mitigate malicious attacks through programmable flow rules, which allow for dynamic traffic redirection. Some large-scale enterprises and cloud providers have started addressing SDN defence solutions, but small SMEs still encounter some unique challenges. Whilst SMEs contribute significantly to global GDP and employment, their limited resources (both financial and personnel) and the fact that they rely on third-party IT services make them appear very vulnerable to network attacks [2,3]. Current academic research has indicated quite a wide range of SDN solutions to network attacks, ranging from efficiency-conscious lightweight heuristic/machine learning models [4,5] to much more complex hybrid deep learning models, developed with high accuracy in mind [6]. However, in the articles reviewed in this study, these solutions were predominantly verified in simulated or controlled test beds, with little or no end-to-end evaluation in real-world SME SDN environments. This systematic review article is therefore contributing by exploring this proposed gap in the existing knowledge and deals with three central research questions:

- What are the predominant cybersecurity threats—particularly related to DDoS—faced by SMEs adopting SDN?
- What detection and mitigation methods for these threats were proposed in recent peer-reviewed literature (between 2020 and 2025)?
- To what extent were any of these solutions evaluated in real-world SME or resource-constrained settings?

The main purpose of this review is, therefore, to firstly consolidate and evaluate the recent research on SDN-based DDoS detection and mitigation studies which are relevant to SMEs. Secondly, to uncover the gaps in the research that must be addressed to make these solutions practicable for SMEs.

There are several articles scrutinising the security of SDN networks [7,8], but few articles are dedicated to SMEs with their associated resource constraints and the realities of integration in a small, inexpensive network. This review contributes to the existing knowledge by methodically evaluating the main detection and mitigation approaches used in SME contexts. It highlights the trade-offs that must be made between efficiency and accuracy of the model while keeping the emphasis on practical, lightweight solutions. Section 2 of this article summarises the methodology, Section 3 details the analysis of the selected articles, Section 4 discusses the key findings, and Section 5 includes recommendations for future research directions.

2. Materials and Methods

This study followed a structured literature review process. The aim was to identify the most relevant articles for review and examine them by considering SDN security threats, focusing on SMEs. A search emphasis built around DDoS detection, and its mitigation was established to produce a more focused and directed area of research. The

search strategy was multi-database, as guided by established systematic review principles.

The search considered major digital libraries, primarily IEEE Xplore, Scopus, Web of Science, ACM Digital Library, Springer, ScienceDirect, Wiley, and MDPI. The search focused on the publications between 2020 and 2025 due to the rapid onward progress of research in this area, thus ensuring that only the most relevant and current research studies were included. Boolean operators and combinations of keywords were employed, and the searches for the databases are detailed below. The search process for ScienceDirect required the removal of two search areas, "small business" and "defense" (using the American spelling). However, the Boolean searches were close enough to produce comparable results. For Wiley and MDPI, the Boolean searches were truncated to increase the search domain. A structured set of search criteria and screening processes was applied to ensure the selected articles were relevant to the objectives shown below and that the searches were reproducible. The articles that met the following conditions were included:

i. Articles addressing DDoS or related network-based threats in the context of SDN and SMEs;
ii. Articles proposing, implementing, or evaluating a detection or mitigation technique in the context of (i);
iii. Articles peer-reviewed and published in journals or conference proceedings;
iv. Articles published in English.

The database-specific Boolean search strings used to retrieve the literature were tailored to each platform. Articles were excluded if they were duplicates, non-peer-reviewed (e.g., editorials, blogs, or opinion pieces), or did not directly address the intersection of SMEs and SDN-related security challenges. The databases and search keywords used in the study are listed in Table 1.

Table 1. List of databases and keywords used in Boolean searches.

Database	Boolean Search
ACM Digital Library	("SME" OR "small and medium enterprise" OR "small business") AND ("DDoS" OR "distributed denial of service" OR "network attack") AND ("detection" OR "mitigation" OR "defense" OR "security solution" OR "machine learning")
IEEE Xplore	("SME" OR "small and medium enterprise" OR "small business") AND ("DDoS" OR "distributed denial of service" OR "network attack") AND ("detection" OR "mitigation" OR "defense" OR "security solution" OR "machine learning")
Scopus	("SME" OR "small and medium enterprise" OR "small business") AND ("DDoS" OR "distributed denial of service" OR "network attack") AND ("detection" OR "mitigation" OR "defense" OR "security solution" OR "machine learning")
Springer Link	("SME" OR "small and medium enterprise" OR "small business") AND ("DDoS" OR "distributed denial of service" OR "network attack") AND ("detection" OR "mitigation" OR "defense" OR "security solution" OR "machine learning")
Web of Science	TS = ("small business" OR "resource-constrained") AND TS = ("network attack" OR DDoS) AND TS = ("detection" OR mitigation) AND TS = ("SDN")
ScienceDirect	("SME" OR "small and medium enterprise") AND ("DDoS" OR ("distributed denial of service" OR "network attack") AND ("detection" OR "mitigation") OR ("security solution" OR "machi learning")
MDPI	SDN DDoS detection Journal = Sensors
Wiley	("software defined networking" OR SDN) AND ("distributed denial of service" OR DDoS) AND (detect * OR mitigate *)

The Boolean search strings listed in Table 1 were tailored to match each database's unique syntax and indexing standards to ensure equivalent functionality rather than just using identical wording. For instance, IEEE Xplore requires capital Boolean operators, while Springer and Wiley use natural language processing. Such modifications of the Boolean search strings produced more uniform outcomes across all platforms. Therefore,

the database search strategy remained comprehensive, reproducible, and focused only on literature directly relevant to SDN-based DDoS detection and mitigation for SMEs.

In most cases, the search keywords were also capped at a certain number for each database. This did not allow for all keywords to be included in each search, and some keywords were discarded, e.g., SDN. However, these searches returned articles that included SDN technology due to the inclusion of "SME" as a keyword. This section follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure a transparent and replicable approach to the literature review. Following the Boolean searches on each database outlined above, the articles were imported into Zotero for reference management purposes. At this point, duplicate entries were automatically identified and removed. The remaining articles then underwent a two-stage screening process. Initially, the titles and abstracts of the articles were reviewed to assess their relevance, and any articles that were not deemed relevant were excluded. This was followed by a full-text review based on the predefined search criteria. The articles that did not meet the eligibility or search criteria (such as those not focused on SMEs, SDN, or DDoS-related threats) were also excluded. SciSpace was used to help with categorisation and annotation to support the synthesis of articles.

Regarding the articles published by MDPI, searches were conducted across titles including Applied Sciences, Electronics, and Information journals. Although SDN/DDoS research articles appeared in the Electronics and Applied Sciences journals, no publication between 2020–2025 met all the stated inclusion criteria. The Sensors journal was the most representative MDPI source for our focused review.

The PRISMA 2020 guidelines were adopted to ensure methodological transparency and reproducibility. Inclusion and exclusion criteria were predefined and applied consistently across all databases to identify the most relevant studies on SDN-based DDoS detection and mitigation for SMEs. Titles and abstracts were screened, followed by full-text eligibility checks, to remove duplicates and non-relevant items such as non-English, out-of-date, or non-SDN/SME-focused papers. Data extraction was conducted using a structured template capturing each article's environment, methodology, dataset, position in the network, and deployment type (Appendix A). Appendix A provides the PRISMA 2020 flow diagram summarising the identification, screening, eligibility, and inclusion processes. Of the 96 records initially assessed, 59 studies met the eligibility criteria and were included in the final synthesis. Reasons for exclusion at each stage (e.g., non-English articles, out-of-date, or lacking SME/SDN focus) are detailed in the diagram. The PRISMA table (Table 2) shows the number of articles selected from each database using the above Boolean searches. Several articles from each database search were excluded, leaving a total of 59 peer-reviewed articles and papers, which were analysed for final review and synthesis.

Table 2. PRISMA for all papers selected and quantity reviewed.

PRISMA Details	Web of Science	Springer Link	Scopus	IEEE	Science Direct	ACM	MDPI	Wiley
Records Identified	13	13	3	4	14	4	12	33
Removed After Screening	2	2		1	5			17
Not in English		1	1					
Books Excluded		1	2					
Not in Date Range				3				
Retracted	1							
Records Included	9	9	0	0	9	4	12	16
Total Articles	59							

3. Synthesis and Analysis of Information

The key information from each article was identified and summarised in Appendix A, which facilitated a structured analysis. Table 2 served as the foundation for identifying patterns across the studies, such as preferred detection approaches and the use of datasets. Of the 59 journal articles, 14 were review studies of the existing data. The remaining 45 articles described the experimental methods that implemented DDoS detection scenarios either in real-world situations (e.g., [9]) or in simulated environments (e.g., [10]). Due to this distinct split in approach between the articles in this study, the information in Appendix A has been split to show review and experimental articles.

3.1. Analysis of Review Articles

Considering the reviewed studies, the threats clustered into the following areas:

(i) High-volume and low-rate DDoS focused on the data plane;
(ii) Control plane saturation and ternary content addressable memory exhaustion via flooding of flow rules;
(iii) Topology and host discovery misuse (e.g., address resolution protocol/link layer discovery protocol spoofing, poisoning);
(iv) Misuse of northbound application programming interfaces/controller apps.

In an SME setting, the threat posed by these attack vectors is amplified by virtual private network (VPN) tunnels, uplinks with no redundancy, and limited operational capacity across the local LAN (local area network), making attacks disproportionately damaging. These categories show the multi-layered nature of SDN-based threats and illustrate the spectrum from data-plane volumetric attacks to control-plane and application-layer attacks. Some of the challenges faced by SMEs include both staffing and financial resource limitations. Table 3 shows a thematic synthesis of the 14 review articles, organised into three major areas.

Table 3. Thematic synthesis of reviewed articles.

Thematic Area	Representative Papers	Main Findings	Research Gaps/ SME Relevance
SME Cybersecurity Challenges	[11–15]	• SMEs operate with minimal or no security staff. • Remote/hybrid work expands attack surface. • Readiness mismatch affects risk response.	• No technical validation within SME networks. • Security culture and automation under researched. • Highlights need for low resource SDN solutions.
Emerging Technologies for Security	[4–6,14,16–18]	• Blockchain adds trust and data integrity. • ML and Edge AI improve adaptability and latency. • Federated/Lightweight frameworks suit constrained devices.	• Cost and scalability remain barriers. • Little empirical data for SME or Raspberry Pi use. • Integration of techniques still conceptual.
Threat Detection and Mitigation	[14,15,18–21]	• SDN enables flow-level visibility and automated response. • Ensemble ML and hybrid DL models dominate. • Experiments mostly in Mininet/Ryu.	• Rarely validated on live or resource limited systems. • Few benchmark datasets. • Overhead, latency and reproducibility issues.

3.1.1. SME Cybersecurity Challenges

Many of the reviewed articles highlighted that SMEs often operate their businesses without any dedicated IT or network security staff, which leaves them very vulnerable to a whole host of network attacks, not least of which is DDoS [11,12] and [5]. The adoption of remote working by SMEs to save on office costs and the subsequent increase in digitisation of their operations to support this have resulted in a huge increase in the possible attack surface, and there has been little or no corresponding increase in their security infrastructure [11,12]. The articles also documented a distinct misalignment between an SME's understanding of their cybersecurity risks and their ability to deal with any attacks. This means that they are open to substantial operational risks and the consequences that that may entail.

3.1.2. Emerging Technologies

There are several emerging technologies that are quickly taking the lead in the fight against cybersecurity, especially in the context of SMEs. Blockchain, machine learning, and network edge-based artificial intelligence (AI) are being used to strengthen cybersecurity in all types of networks, including resource-constrained environments, which are indicative of SMEs [16]. Several studies indicated that blockchain is becoming a standout technology in this area as it provides decentralised trust, immutable data storage, and smart contracts, which safeguard the integrity of data [4,6,16]. The research outlined in reference [17] highlighted the use of AI placed at the network edge for low-latency threat detection. This reduces the burden on central infrastructure and makes real-time detection for SMEs and IoT a possibility. Two articles [4,5] discussed the manner machine learning can adapt to both zero-day attacks and evolving threats.

3.1.3. Threat Detection and Mitigation

The study outlined by reference [13] demonstrated how traditional perimeter-based defence models were becoming less effective, and the increasing importance of adaptive detection models was growing exponentially. However, these improvements bring with them the heightened risk of hackers attacking machine learning models to evade or even poison them [4]. Overall, these technologies seem to offer significant opportunities for improved detection and automation, which is a particular selling point for SMEs. There are still challenges to be overcome with these technologies, not least of which are the scalability and cost of these solutions, which can severely impact their uptake amongst SMEs.

3.2. Analysis of DDoS Detection Articles

Considering the SDN-based DDoS detection literature, it can be deduced that there are two distinct design boundaries. The first is a lightweight machine learning and heuristic-based model centred around both the SDN controller and the network edge. These detection models aim for fast but low-resource examination of traffic packets. In [22], the authors analysed flow-level features extracted from packet headers, whilst in [23], a flow analysis was used with entropy measures of packet distributions to flag abnormal traffic. Both solutions demonstrated a degree of computational efficiency. The random forest model used for low-rate/message queuing telemetry transport-based DDoS detection [24] and the feature-efficient classifiers for low-rate DDoS [25] are both convenient to design and deploy within the constraints of an SME. SDN security measures and network architectures for IoT are reviewed in [19]. It identifies defence points but does not demonstrate them in real-world scenarios. SDN with IoT is surveyed in [20], highlighting the difficulty between needing flexibility and a lightweight machine learning model on resource-constrained devices. A review of machine learning and deep learning DDoS detection models

as applied to SDNs is presented in [21]. It emphasises the prevalence of simulated evaluations and the risks of relying on private and/or curated datasets.

Most reported solutions relied only on simulations, so their effectiveness was not tried and tested in real-world environments. Most of the evaluations were tested using CICIDS2017 [26] and Bot-IoT [27] datasets, i.e., a simulated environment. These datasets have curated attacks and stable traffic mixes and models tested on them risk overfitting. SME networks will have heterogeneous software-as-a-service traffic with VPN tunnels and bursty traffic patterns that shift feature distributions and undermine any attempt at generalisation. This reliance on curated data is especially problematic, as the absence of a representative dataset for the diverse and dynamic traffic found in SME networks makes it challenging to validate even these simpler models for real-world application.

The second line can be drawn to enclose studies based on maximising accuracy with hybrid learning. Convolutional neural networks (CNNs), long short-term memory (LSTM), gated recurrent unit (GRU), and their variants lead the way [8,9], with [28] using a broadened learners' multi-resolution learning system. In [22], the authors applied multiple machine learning classifiers for DDoS detection, achieving good accuracy scores, though the added complexity may raise latency concerns for SME environments. A model located at the edge that detects malicious packets and signals the SDN controller is described in [29]. This solution takes controller load away while still giving real-time response and low latency.

The general view is that lightweight flow/counter or feature-selected models are best suited for first-stage filtering, with more complex machine learning models used only when needed and placed at the edge. However, there seem to be inadequate studies on real SME testbeds to allow consistent latency to be established and effective evaluations of real-time traffic to be undertaken. The likelihood of running SME testbeds on live networks is low, as relatively few SMEs currently run SDN. Live trials also carry unacceptable outage/compliance risks, and SMEs lack spare budget and/or staff. Therefore, the literature typically defaults to reproducible simulations and public datasets.

The review of the DDoS detection literature highlights two methodological approaches: lightweight feature-based machine learning and hybrid deep learning models. Each of these models has a performance trade-off, as summarised in Table 4.

Table 4. Comparative synthesis of SDN-based DDoS detection approaches.

Detection Approach	Representative Papers	Averaged Accuracy (%)	Resource/ Latency Profile	Dataset & Validation	Real-World Applicability (SME)	Observed Limitations
Lightweight ML/Heuristic	[22–24,28,30]	90–95	Very low CPU; <100 ms latency	CICIDS2017, Custom	Edge-deployable	Lower detection of novel patterns; limited adaptability
Hybrid Deep Learning (CNN/LSTM, ELM, GRU)	[8,9,31,32]	97–99	High GPU/CPU; >500 ms latency	CICDDoS2019, Bot-IoT	Limited (requires GPU)	Overfitting; poor scalability
Federated/Edge-AI/Adaptive	[17,29,33]	93–97	Moderate; distributed load	ToN-IoT, E-IIoT	Promising	Communication overhead; early-stage research

While hybrid models (e.g., CNN–LSTM, Transformer) consistently report 98–99% accuracy on curated datasets such as CICIDS2017, they also require up to five to 10 times higher computational cost and introduce latency, which would be detrimental to live DDoS detection. Lightweight models such as random forest/decision tree or

entropy/counter-based detection deliver lower accuracy (90–95%) but use a fraction of the available computational resources. The lightweight models, therefore, make good candidates for running at the very edge of a network using devices such as Raspberry Pi.

These comparisons indicate that most SDN DDoS detection studies optimise models for high accuracy rather than live implementation in a network. High-accuracy models can be impressive in laboratory environments but impractical for SMEs due to their high computational overheads. Therefore, lightweight models remain the most feasible direction for SME deployment, ideally placed at the network edge.

3.3. Analysis of DDoS Mitigation

As explained earlier, most studies included in this review focused on the detection of malignant traffic flows. A slightly smaller but still significant number of articles considered mitigation strategies, which can contain or even neutralise attacks once they are detected. Several of these studies proposed software-defined controller-driven responses that influence flow rules or segment the network to constrict the blast radius of any malicious traffic. A study used a network segmentation that was based on the aggregation of flows to build RAPID (Rapid Protection in Dataplane-DDoS) rule updates and, in doing so, reduced detection times from 9 s to 1 s with a manageable overhead [34]. A related study [35] proposed a cloud–SDN hybrid architecture, where attacks were detected using a deep learning-based model with semi-supervised training. Mitigation was achieved through group-level responses designed to prevent flow table overflow.

There are other studies that have combined deep-learning artificial intelligence models for detection with embedded mitigation ideas. For instance, Ref. [8] combined a deep-learning classifier with controller-pushed flow rule updates (no traceback), while [36] demonstrated an IP traceback integrated with controller-side mitigation. Ref. [37] makes use of a hybrid ensemble to identify botnet traffic before adjusting flow rules. Another study, Ref. [38], proposed a cybersecurity orchestration framework for service chains in which responses are automatic within the SDN; however, this remains a conceptual solution.

All these studies relied heavily on the programmability of SDN for their dynamic defence of the network using flow rules, traffic routing, and network segmentation. However, two gaps in the research are consistently evident. The first is that most of the proposed solutions were tested only in simulated or controlled environments. Secondly, few of these mitigation strategies were explicitly evaluated in the resource-constrained world of an average SME.

In keeping with controller-based responses, several studies paired DDoS detection with mitigation actions such as rapid flow aggregation and segmentation to reduce the blast radius of an attack [34], guided blocking [8], and lightweight online detection with controller-pushed flow rule updates [30]. Other studies proposed route obfuscation to counter Crossfire-style floods [39] and entropy-based in-plane detection signals feeding the controller [18]. The use of Ryu (software controller) with proactive rules [40] showed similar benefits. In [14], a network slicing method was used to partition services, while a one-versus-rest strategy trains separate classifiers to distinguish one class from all others [41], illustrating how mitigation could be service-aware rather than only switch-level [42]. This demonstrated ONOS-based mitigation using sFlow-RT integration for real-time traffic sampling. Reported mitigation latencies are promising (from a few milliseconds to seconds), but these results come from emulated environments; in production deployments with resource constraints, actual latencies may be significantly higher [18,42].

3.4. Integrating Detection and Mitigation

The detection and mitigation studies highlighted above show a two-stage defence that fits in well with SDN's centralisation and programmability. The detection-based research has produced a wide range of approaches. There are lightweight flow, entropy, and counter methods that enable fast initial screening, and there are many hybrid machine learning models that can be endlessly modified for greater accuracy, but which consume more resources. The mitigation studies lean into SDN's capacity for dynamic flow management and use segmentation, traceback, and flow rule updates to deal with the malicious traffic once detected.

However, there is a noticeable absence of integrated frameworks that connect detection outputs with mitigation actions in real time, particularly in resource-constrained environments such as SMEs. Most studies evaluated these two areas in isolation and nearly always in simulated environments, which mitigated the complex issues around deployment that were stated in Section 3.2. Any effective solution will likely require multiple detection and mitigation strategies that work in a resource-constrained environment, and it is this framework that remains largely unexplored. A trigger action could be defined on an interface in which the edge detector generates a minimal event tuple, e.g., (source IP address, destination IP address, destination port number, protocol, rate, confidence, time window), and the controller maps this to an action. The action could be rate-limiting, segmenting, or quarantining the traffic. For example, if the rate > 0 and confidence ≥ 0.9 over a stipulated time window of, say, 30 s, then install a temporary flow rule. Several reports theorised the use of such a solution with edge or data plane-based detectors using events (rate, confidence, etc.) presented to the controller to install flow rules. Ref. [43] used data plane processing for the machine learning model, and [42] used controller applications for mitigation. Ref. [30] uses lightweight real-time detectors that drive OpenFlow updates. This reduces round-trip times and any central CPU usage. RyuGuard [40] demonstrated proactive integration, while slice-level quarantine (the physical network is split into several virtual slices, each dedicated to a service or device) is proposed by [14]. RAPID flow aggregation [34] accelerates rule updates and provides service-aware responses. These implementations showed that integration advantages come from standardising the response from detector to controller and making sure actions are short-lived and service-aware to avoid overwhelming resources [14,30,34,40].

3.5. Gaps and Future Directions

The literature review highlighted significant progress in DDoS detection and mitigation in SDN-based environments; however, several critical gaps in the research have remained. In practice, most studies depended on simulated environments and publicly available datasets (CICIDS2017 and Bot-IoT). These were easily compared as they all use the same starting points, but they did not take into consideration the assortment of challenges faced by real-world SME networks. Only a few of these studies used live networks, which leaves a considerable gap in the research with regard to practical validations.

From a technical standpoint, there seems to be a one-sided emphasis put on the accuracy of the models' metrics with little or no consideration paid to latency, scalability, and processing overhead. These factors are critical in SMEs where resources are limited and even a very small central processing unit (CPU) or memory overhead may prove a step too far. Moreover, these detection and mitigation solutions have generally been developed in isolation from each other, meaning that a one-stop shop of both malignant packet detection with dynamic flow-based mitigation is rare. Integration of such solutions into live SME networks, therefore, remains largely unaddressed.

Moving on towards the future of this research, there are some promising areas emerging from the current work. Lightweight detection models placed at the very edge

of networks seem to provide the most promising potential. They make use of such systems as selective feature extraction, federated learning, and heuristic counters, which, together, can offer a defence of the network without producing a huge increase in resource-constrained areas such as CPU and memory use. These automatic mechanisms, such as segmentation, traceback, and flow rules, have been proposed as part of a promising path to automated DDoS detection and mitigation for SMEs and SDN environments. Finally, there is still a need for real-time/real-life testing of such solutions in SME-specific networks. Such testing needs to benchmark not just the accuracy but, more importantly, the cost, latency, and ease of deployment. These areas are as important for SMEs and will take this research stream from theoretical concepts to practical solutions.

3.6. Section Summary

The reviewed research outlined several solutions put forward in the detection and mitigation of network attacks. However, it also highlighted the areas where more developments need to be undertaken to produce a practical one-stop solution for network attacks in SME and SDN environments. The research also illustrated that lightweight statistical and machine learning models can provide a very valuable solution in resource-constrained networks when compared to deep learning and hybrid techniques, which offer better accuracy but at the cost of high complexity and processing overheads. The mitigation strategies examined make use of SDN's programmability but are rarely tested on real networks and with little or no integration with the associated detection modules. The literature showed that although SDN is a promising way forward for the security of SME networks, there needs to be a low-cost, simple solution for real-time detection and mitigation of network attacks in SME network environments.

While the studies presented several potential approaches, three consistent gaps remain. Firstly, the current studies are dominated by emulation and/or public datasets [18,34,43], which means that latency and resource constraints are rarely considered. Secondly, where detection and mitigation are integrated, such integrations do not include safeguards such as flow rule expiry or rollback, and few provide any model explainability despite using machine learning [44]. Thirdly, specialised domains such as SCADA (Supervisory Control and Data Acquisition) [42] highlight promising work but also demonstrate the difficulty of transferring these solutions to real-world SME environments.

4. Discussion

SDN environments provide an excellent framework for deployment of security models in SME environments; however, it seems that current models are not aligned with the practical, real-time realities of these environments. SMEs have many challenges in managing their networks; they are being increasingly targeted by network attacks, and they have very limited budgets and in-house expertise, as discussed in the introduction to this article. These restrictions make complex or resource-intensive security solutions impractical, regardless of their efficacy.

A major problem that emerged from the review was the trade-off between the accuracy of the model and its processing efficiency. Solutions that combine deep machine learning models (e.g., convolutional neural networks and long short-term memory) provide high accuracy but often require very high computational resources and continual retraining to retain their capabilities. These conditions are generally not readily available to SMEs. On the other hand, the lightweight methods seen in the review (e.g., heuristic counter, random forest, feature-efficient classifiers) are easier to deploy but have not really been validated in real time. This means it is far from clear how these solutions would perform in live network situations.

Yet another research gap exists in the lack of integration between the detection and mitigation of malignant flows. Most articles treated these two areas completely separately and not as part of the same framework, which they would be in practice. From an SME point of view, however, this is where the critical application would lie. The value is not just in detecting network attack traffic but in having an automatic, low-latency system that can deal with this traffic without any expert human intervention. Low latency points towards a solution based at the edge, where traffic can be inspected locally and mitigation is triggered as needed to the controller. The isolated development of these two components, detection and mitigation, also means that there are no clear best practices or standardised protocols for how a detection event at the edge should seamlessly trigger a mitigation response from the central controller. This lack of a standardised interface or framework presents a significant barrier to practical, end-to-end implementation for SMEs.

As a final point, the literature reveals a quite remarkable gap in the research for SME focused test setups and evaluation systems. Whilst the datasets CICIDS2017 and Bot-IoT are the most widely used and are by far the best in class, they still lack the vast assortment of problems that can befall a network. Practices such as VPN encapsulation, asymmetric routing, and packet fragmentation, coupled with the ever-present network congestion, can distort flows and trigger false positives or missed detections. Contemporary studies [45–49] show that datasets are both balanced and "stationary", which fails to capture the fluidity of a live SME network. Without rigorous testing in real-life situations, it is unclear how these models will react in such environments.

This discussion highlights the gap between the academic progress made and the applicability of such solutions in SME settings. To bridge this gap, any future research must pursue lightweight and integrated solutions and move beyond simulation to real-world networks. The most recent studies (published 2023–2025) used simulated situations such as Mininet [50], ONOS [51], or Ryu [52]. This underlines that the research practice gap for SMEs has continued despite technical advances. The reviewed studies indicated that while technical performance is advancing rapidly, deployment feasibility within SME software-defined networks remains limited. Lightweight machine learning models could be integrated directly at the edge on devices such as Raspberry Pi, where they can locally monitor flows and trigger the installation of flow rules via the SDN controller. The low computational overhead of these models aligns well with SME resource constraints. Alternatively, hybrid deep-learning models, with their exceptional accuracy, are more suited to cloud-assisted or federated architectures, where resource allocation is not such an issue.

The review showed a significant shortcoming in using detected flows to respond to and block DDoS attacks. Many articles considered threat detection as an activity separate from the mitigation of the attack, with little or no automatic intervention by, for instance, the SDN controller. Only a limited number of articles clearly outlined the way a flow rule may be implemented and include such aspects as rule expiration, which is vital in keeping the network operating in SME environments. Future SDN frameworks should address this with a closed-loop architecture where detection of malicious flows continuously updates the mitigation process and vice versa. SDN controller safeguards, such as automatic timeout of drop rules and explainability of machine learning outputs, would prevent cascading failures and improve transparency. The integration of explainable AI methods could further assist in the understanding of flow rule implementation to block DDoS. Very few of the reviewed models incorporated explainability or self-auditing features, yet these are crucial for trust, troubleshooting, and accountability in SME operations.

Although this review identified clear distinctions between lightweight and deep learning–based approaches, the literature rarely reported comparative benchmarks of CPU load, memory consumption, or latency. Calculating these overheads is essential for

SMEs, and future work should provide experiential resource profiles to clarify the practical trade-offs between accuracy and real-time efficiency.

While this review highlighted significant distinctions between lightweight and deep learning-based approaches, the articles rarely provide comparative benchmarks of CPU consumption, memory usage, or latency. Evaluating these overheads is essential for SMEs, and future research should offer practical hardware profiles to explain the trade-offs between accuracy and real-time performance.

4.1. Future Work

Future research areas should build on the limitations outlined above and bridge the gap between simulation and live deployment in SME environments. Firstly, future research should aim to validate models in realistic SME software-defined network environments. The construction of more realistic test environments of realistic network environments that replicate SME traffic patterns to include such "abnormalities" as virtual private network tunnelling, cloud services, and variable speed uplinks. This will allow the evaluation of latency, throughput, and false positive rates under more realistic network load and activity. This then leads into the second area of future research that should focus on cost and ease of deployment so that proposed models can be realistically adopted by SMEs rather than remaining academic prototypes.

Future research should focus on the practical implementation of DDoS detection and mitigation models in active SDNs or in controlled environments that simulate genuine traffic. Testing with real traffic would significantly improve the accuracy of the models and their subsequent deployment.

While this review proposed a theoretical framework of edge-based detection with SDN controller-based mitigation, the development and evaluation of an operational prototype lie outside the scope of a systematic review. Future work should implement an integrated system to validate flow rule insertion, latency, and resource consumption in SME SDN environments.

This review demonstrated the accuracy and resource trade-off with deep learning models. However, new hybrid AI techniques may provide improved implementation for SMEs. The evaluation of such methods is a priority for future research.

4.2. Practical SDN Tools and Implementations

Although the primary emphasis of this study was on academic research, several practical SDN controllers and supporting frameworks were either employed or referenced within the reviewed articles. Table 5 provides a summary of frequently used platforms and highlights their relevance to SMEs.

Table 5. A summary of SDN tools/frameworks their typical use in research, their strengths and limitations for SMEs.

Tool/Framework	Typical Use in Research	Strengths	Limitations for SMEs
Ryu (Python3-based, open-source)	Used for DDoS detection and flow rule automation	Lightweight, scriptable, easily deployable on Raspberry Pi or virtual hosts	Limited scalability for multi-controller or carrier-grade networks
ONOS (Open Network Operating System)	Controller for carrier-scale and cloud-SDN experiments	Modular and useful for clusters, supports APIs	Complex setup and over-provisioned for SME needs
Floodlight [53]	Legacy Java-based OpenFlow controller used in early DDoS detection prototypes	Stable and easy integration with legacy switches	Limited modern ML interfaces and slower community updates

OpenDaylight (ODL) [54]	Enterprise-grade SDN controller with NFV and RESTCONF support	Supports RESTCONF, NETCONF, NFV extensions	High memory use, heavy memory use for small setups
Mininet	Virtual SDN emulation for experimentation and testing controller logic	Widely used, reproducible and supports Ryu/ONOS/ODL	Simulated use only and lacks physical device use
sFlow-RT/Open vSwitch (OVS) [55]	Real-time traffic monitoring and flow export for anomaly detection	Enables live anomaly capture and mitigation rules	Requires controller integration for automated blocking

The review established that most research studies rely on lightweight, open-source controllers such as Ryu and Floodlight and used Mininet or OVS for lab testing. In live SME software-defined networks, Ryu is the easiest and most adaptable choice due to its small size and its compatibility with machine learning models written in Python. Conversely, the larger enterprise-scale controllers (e.g., ONOS or ODL) are better suited for multi-data centre environments where dedicated hardware and staff resources are available.

5. Conclusions

SDN offers a very strong foundation for defence against network attacks; however, the current research remains largely simulated or theoretical. Moreover, any proposed solution must consider the human factor, specifically the possible unavailability of dedicated security personnel in small and medium-sized enterprises (SMEs), which necessitates an autonomous system requiring minimal human intervention for both detection and mitigation. Therefore, future research must prioritise SME needs by focusing on resource-efficient, lightweight attack detection at the network edge with integrated mitigation and validation in real-world environments and datasets. Only then will these solutions move from promising theoretical concepts to practical, cost-effective solutions that will protect vulnerable SME networks.

Author Contributions: R.W.: conceptualisation; methodology; formal analysis; investigation; resources; writing—original draft preparation; writing—review and editing; M.B.: conceptualisation; methodology; formal analysis; investigation; resources; writing—original draft preparation; writing—review and editing; A.S.: conceptualisation; methodology; formal analysis; investigation; resources; writing—original draft preparation; writing—review and editing; R.S.: conceptualisation; methodology; formal analysis; investigation; resources; writing—original draft preparation; writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. PRISMA 2020 Flow Diagram Showing Records Identified, Screened, Excluded, and Included in the Systematic Review of SDN-Based DDoS Detection and Mitigation Strategies for SMEs.

Experimental Rollout or Review	Target Environment	Methodology—Machine Learning, Blockchain, etc.	Position in Network	Dataset Used	Simulation or Practical deployment	Article
Experimental Rollout	SDN network	Machine learning-based DDoS detection and mitigation framework	SDN controller	CICIDS2017	Simulation only	[29]
Experimental Rollout	SDN network	ML-based DDoS detection using multiple classification algorithms	SDN controller	UNSW-NB15	Simulation only	[25]
Experimental Rollout	SDN network	MULTI-BLOCK intrusion detection framework using new packet- and flow-level features	SDN controller	UNSW-NB15, BoT-IoT	Simulation only	[44]
Experimental Rollout	SDN network	Low-rate DDoS detection model using MQTT traffic features and ML classification	SDN controller	Custom dataset	Simulation only	[24]
Experimental Rollout	SDN network	ML-based DDoS detection framework with feature selection and ensemble learning	SDN controller	CICDDoS2019	Simulation only	[22]
Experimental Rollout	SDN network	Deep learning-based DDoS detection with counter-based mitigation	SDN controller	CICDDoS2019	Simulation only	[7]
Experimental Rollout	SDN network	Time-efficient ML-based DDoS detection	SDN controller	CICDDoS2019	Simulation only	[22]
Experimental Rollout	SDN network	Hybrid deep learning-based detection framework for emerging cyber threats	SDN controller	CICIDS2017, NSL-KDD	Simulation only	[9]
Experimental Rollout	SDN network	ML-driven DDoS detection and mitigation system	SDN controller in cloud	NSL-KDD	Simulation only	[35]
Experimental Rollout	SDN network	Blockchain and federated learning	Federated placement	E-IIoT and ToN-IoT	Simulation only	[10]
Experimental Rollout	SDN network	RAPID Flow aggregation with network segmentation for DDoS mitigation; algorithm for rapid flow rule install	SDN controller	Custom dataset	Simulation only	[34]
Experimental Rollout	SDN network	Hybrid CNN–ELM deep learning model + IP traceback for mitigation	SDN controller	CICIDS2017	Simulation only	[8]
Experimental Rollout	General network	Optimized hybrid classification model (Moth Flame Optimisation + Ensemble ML classifiers)	Edge/gateway	CICIoT2023	Simulation only	[37]
Experimental Rollout	General network	Integration of threat-occurrence predictive models into security risk analysis	Edge Server	Live traffic	Simulation and practical implementation	[56]
Experimental Rollout	General network	EA-based feature selection (ENTER), multi-correlation info, multiple classifiers	Security Anaytics Server	Custom dataset	Simulation only	[57]

Experimental Rollout	General network	Manifold Regularized Broad Learning System (MRBLS) with LU decomposition	IDS Module	NSL-KDD, UNSW-NB15	Simulation only	[28]
Experimental Rollout	General network	Distributed edge ML framework with task offloading and optimisation for constrained devices	Edge nodes	Live traffic	Simulation and practical implementation	[58]
Experimental Rollout	General network	Cloud Server Intrusion Detection and Response module to reduce VM-level collateral damage DDoS	Cloud servers/VM layer	CAIDA DDoS Attack 2007	Simulation only	[59]
Experimental Rollout	General network	Autonomous cybersecurity framework integrating AI/ML for detection and response	Within service chain	Live traffic	Practical implementation	[38]
Experimental Rollout	General network	Machine learning-based approach for detecting IoT-generated DDoS traffic	Edge nodes	CICIDS2017	Simulation only	[23]
Experimental Rollout	SDN network	Hybrid deep learning-based modelfor bonet detection in a fog environment	SDN Controller	N-BaloT 2018	Simulation only	[41]
Experimental Rollout	SDN Network	Flow-table overflow detection using ML classification; DTW-style flow dynamics	SDN Controller	Custom dataset	Simulation only	[60]
Experimental Rollout	SDN Network	Data-plane ML (KNN/SVM/RF) with controller coordination	SDN Controller + Switch data plane	Not stated	Simulation only	[39]
Experimental Rollout	SDN Network	Entropy features + ML classifier	SDN Controller	Not stated	Simulation only	[61]
Experimental Rollout	SDN Network	Spiking Elman neural network for intrusion/DDoS	SDN Controller	Custom dataset	Simulation only	[62]
Experimental Rollout	SDN Network	Distributed ML pipeline using Kafka/Hadoop	Controller + distributed workers	Not stated	Simulation only	[63]
Experimental Rollout	SDN Network	Continual Federated Learning IDS (edge + controller)	Edge nodes + controller	Not stated	Simulation only	[33]
Experimental Rollout	SDN Network	Optimized DNN detection + bait/decoy mitigation	Controller + decoy	Not stated	Simulation only	[64]
Experimental Rollout	SDN Network	Risk-scoring IDS with ML prioritisation	SDN Controller	Not stated	Simulation only	[65]
Experimental Rollout	SDN Network	ML on 5 flow stats; proactive rule install	Controller (Ryu)	Not stated	Simulation only	[14]
Experimental Rollout	SDN Network	Autoencoder feature learning + XGBoost; SHAP explainability	SDN Controller	CICDDoS2019	Simulation only	[40]
Experimental Rollout	SDN Network	Multi-ML detection + traceback mitigation; timing and confidence intervals reported	SDN Controller + sFlow-RT	Custom dataset	Simulation only	[42]
Experimental Rollout	SDN Network	Multi-Stage Learning Framework Using Convolutional Neural Network and Decision Tree	Supervisory Control and Data Acquisition	Custom dataset	Simulation Only	[66]
Experimental Rollout	SDN Network	DL IDS (TS-RBDM) + Streebog user authentication	SDN Controller + auth module	Not stated	Simulation only	[67]
Experimental Rollout	SDN Network	Feature engineering + ML (RF, XGBoost); Improved Binary Grey Wolf Optimisation for feature	SDN controller	CSE-CIC-IDS2018	Simulation only	[68]

		selection; controller installs drop rules				
Experimental Rollout	SDN Network	Ensemble (SVM, NB, RF, kNN, LR â†’ Voting); lightweight 5-feature set; traceback + flow rules	SDN controller + Edge switch	Custom dataset	Simulation only	[34]
Experimental Rollout	SDN Network	Hybrid deep learning (Transformer + CNN) for DDoS detection	SDN controller	CICDDoS2019	Simulation only	[31]
Experimental Rollout	SDN Network	Entropy-based anomaly detection + OpenState stateful data plane; controller pushes drop rules	SDN Controller + Switch (data plane)	BigFlows, Bot-IoT + Mininet traces	Simulation only	[32]
Experimental Rollout	SDN Network	ML models (RF, DT, SVM, KNN, NB, LR); real-time detection; controller flow updates	SDN Controller	CICDDoS2019	Simulation only	[36]
Experimental Rollout	SDN Network	DT-based ensembles (AdaBoost/Bagging/RUSBoost) + feature selection; Bayesian tuning	SDN Controller	Custom dataset	Simulation only	[69]
Experimental Rollout	SDN Network	Hybrid 1D-CNN feature extractor + Decision Tree classifier	SDN Controller	Custom dataset	Simulation only	[70]
Experimental Rollout	SDN Network	SDN/NFV architecture; lightweight anomaly filter + quarantine slice for deep inspection	SDN controller + NFV edge	N/A	Simulation only	[15]
Experimental Rollout	SDN Network	Hybrid CNN-ELM for online detection; IP traceback + flow rule mitigation	SDN controller	CICIDS-2017; InSDN	Simulation only	[39]
Experimental Rollout	SDN Network	OvR ML (RF, kNN, NB, LR) with RFE feature selection; controller drop rules	SDN controller	Custom dataset	Simulation only	[18]
Experimental Rollout	SDN Network	XRDI feature selection (XGBoost/RF/DT/IG) + classic ML (DT, RF, SVM, LR); alerting	SDN controller	InSDN; CICIDS2017; CICIDS2018	Simulation only	[71]
Review	N/A	Systematic review (70 studies) on ML/DL for SDN DDoS; gaps: datasets, controller overhead	N/A	N/A	N/A	[21]
Review	N/A	Survey of SDN-IoT security including DDoS	N/A	N/A	N/A	[20]
Review	N/A	Survey of distributed DDoS frameworks	N/A	N/A	N/A	[19]
Review	N/A	Qualitative analysis of SME cybercrime perceptions, fear taxonomy, and barriers to security adoption	N/A	N/A	N/A	[11]
Review	N/A	Survey-based organisational readiness assessment for information security threats	N/A	N/A	N/A	[13]
Review	N/A	Analysis of cybersecurity threats, vulnerabilities, and mitigation strategies for SatCom in the context of IRIS	N/A	N/A	N/A	[72]
Review	N/A	Survey and statistical analysis of cybercrime prevalence, nature, and impact during pandemic	N/A	N/A	N/A	[12]

Review/empirical survey	N/A	Analysis of victims' payment decision-making processes using survey/interview data	N/A	N/A	N/A	[73]
Experimental	SDN	Optimized deep neural network for DDoS detection; bait mitigation process at switches coordinated by SDN controller.	SDN Controller	CIC-DDoS2019, SDN-specific Mininet dataset (Mendeley Data)	Simulation	[74]
Review	N/A	Comprehensive survey of blockchain-based smart contracts: applications, opportunities, and challenges	N/A	N/A	N/A	[6]
Review	N/A	Review of lightweight blockchain frameworks for security and efficiency in smart city applications	N/A	N/A	N/A	[16]
Review	N/A	Taxonomy and systematic review of Edge AI frameworks, applications, and challenges	N/A	N/A	N/A	[17]
Review	N/A	Review of cybersecurity, data privacy, and blockchain integration	N/A	N/A	N/A	[4]
Review	N/A	Survey of ML applications, challenges, and opportunities in intelligent systems	N/A	N/A	N/A	[5]

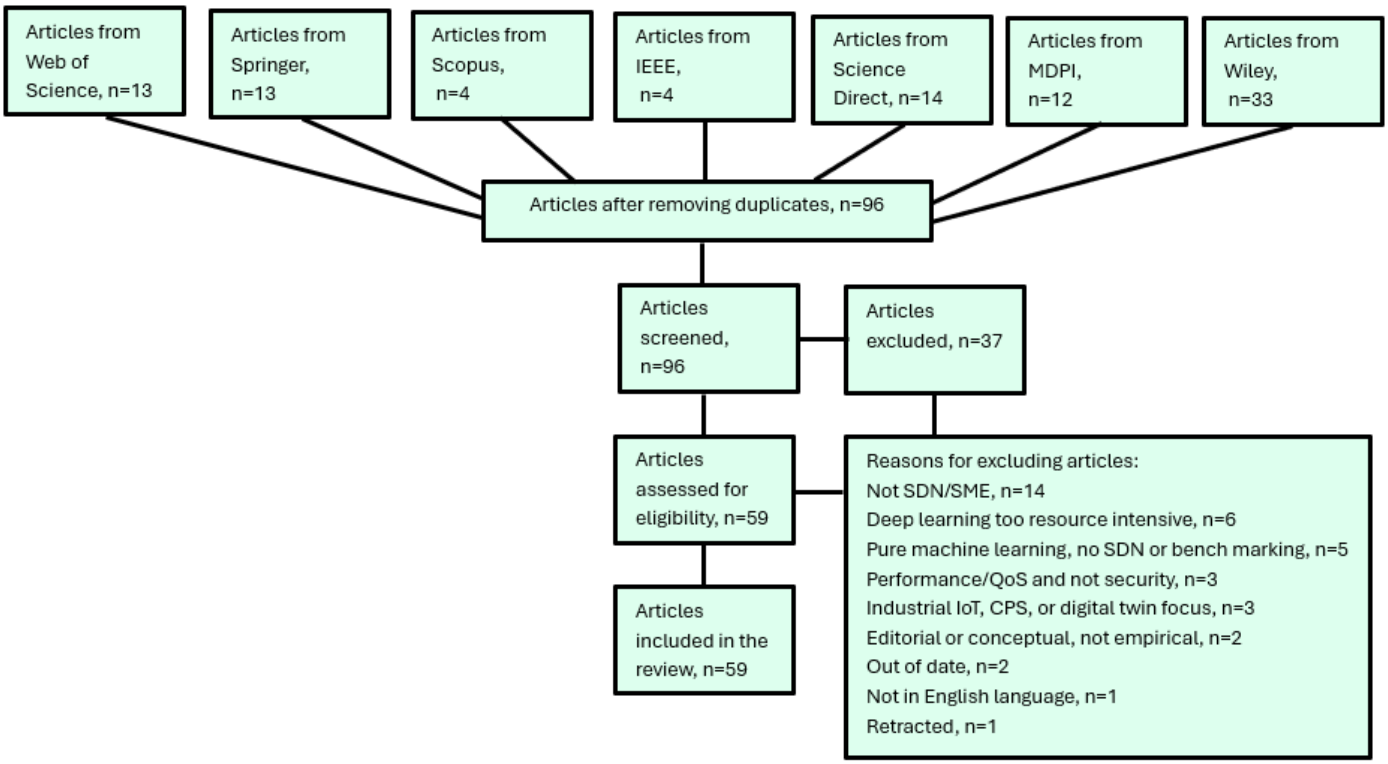

Figure A1. Structured Summary of Reviewed Studies Showing Evidence Distribution Across Key Research Divisors.

References

1. Kaspersky Lab; B2B International. IT Security Risks Survey 2017: Protecting Your Business Against Financial and Reputational Losses with Kaspersky DDoS Protection, Kaspersky Lab Whitepaper. 2018. Available online: https://media.kaspersky.com/pdf/Kaspersky_Lab_Whitepaper_Kaspersky_DDoS_Protection_final.pdf (accessed on 19 September 2025).
2. World Bank. *Small and Medium Enterprises (SMEs) Finance*; World Bank: Washington, DC, USA, 2019. Available online: https://www.worldbank.org/en/topic/smefinance (accessed on 18 September 2025).
3. European Commission. User Guide to the SME Definition, Publications Office of the European Union. 2020. Available online: https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1 (accessed on 19 September 2025).
4. Wylde, V.; Abomhara, M.; Gerdes, R.; Morris, T.H. Cybersecurity, data privacy and blockchain: A review. *SN Comput. Sci.* **2022**, *3*, 127. https://doi.org/10.1007/s42979-022-01020-4.
5. Injadat, M.; Moubayed, A.; Nassif, A.B.; Shami, A. Machine learning towards intelligent systems: Applications, challenges, and opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3299–3348.
6. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain-based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857.
7. Cherian, M.; Varma, S. Secure SDN-IoT framework for DDoS attack detection using deep learning and counter based approach. *J. Netw. Syst. Manag.* **2023**, *31*, 54. https://doi.org/10.1007/s10922-023-09749-w.
8. Rajkumar, K.; Shalinie, S.M.; Stanly, H. SDN defense: Detection and mitigation of DDoS attack via IoT network. In Proceedings of the 25th International Conference on Distributed Computing and Networking (ICDCN '24), Chennai, India, 4–7 January 2024; pp. 371–376. https://doi.org/10.1145/3631461.3631467.
9. Javeed, D.; Gao, T.; Khan, M. SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. *Electronics* **2021**, *10*, 918. https://doi.org/10.3390/electronics10080918.
10. Kokila, K.M.; Konda, S.R.K.S. DeepSDN: Deep learning based software defined network model for cyberthreat detection in IoT network. *ACM Trans. Internet Technol.* **2025**, 1–29; ACM 1557-6051/2025/5-ART. https://doi.org/10.1145/3737875.
11. Arroyabe, M.F.; Arranz, C.F.A.; De Arroyabe, I.F.; De Arroyabe, J.C.F. Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Comput. Secur.* **2024**, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826.
12. Van De Weijer, S.; Leukfeldt, R.; Moneva, A. Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Comput. Secur.* **2024**, *139*, 103693. https://doi.org/10.1016/j.cose.2023.103693.
13. Jayarao, G.B.; Ray, S.; Panigrahi, P.K. Information security threats and organizational readiness in nWFH scenarios. *Comput. Secur.* **2024**, *140*, 103745. https://doi.org/10.1016/j.cose.2024.103745.
14. Candal-Ventureira, D.; Fondo-Ferreiro, F.; Gil-Castiñeira, F.; González-Castaño, F.J. Quarantining malicious IoT devices in intelligent sliced mobile networks. *Sensors* **2020**, *20*, 5054. https://doi.org/10.3390/s20185054.
15. Karmous, N.; Aoueileyine, M.O.-E.; Abdelkader, M.; Romdhani, L.; Youssef, N. Software-defined-networking-based one-versus-rest strategy for detecting and mitigating distributed denial-of-service attacks in Smart home internet of things devices. *Sensors* **2024**, *24*, 5022. https://doi.org/10.3390/s24155022.
16. Padma, A.; Ramaiah, M.; Ravi, V. A comprehensive review of lightweight blockchain practices for smart cities: A security and efficacy assessment. *J. Reliab. Intell. Environ.* **2025**, *11*, 13. https://doi.org/10.1007/s40860-025-00254-2.
17. Gill, S.S.; Golec, M.; Hu, J.; Xu, M.; Du, J.; Wu, H.; Walia, J.K.; Murugesan, S.S.; Ali, B.; Kumar, M.; et al. Edge AI: A taxonomy, systematic review and future directions. *Clust. Comput.* **2015**, *28*, 18.
18. Aslam, B.; Azam, M.A.; Imran, M.; Rizvi, S. Adaptive machine learning based distributed denial-of-service attacks detection and mitigation system in software-defined networks. *Sensors* **2022**, *22*, 2697.
19. Patil, P.; Kallurkar, S.; Kancharla, B. Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6197. https://doi.org/10.1002/cpe.6197.
20. Mohamed, A.; Babiker, M.; Abubakar, A. A comprehensive survey on secure software-defined network for the Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4391. https://doi.org/10.1002/ett.4391.
21. Bahashwan, S.; Alazab, M.; Jolfaei, A.; Islam, A. A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks. *Sensors* **2023**, *23*, 4441. https://doi.org/10.3390/s23094441.
22. Bhayo, J.; Jafaq, R.; Ahmed, A.; Hameed, S.; Shah, S.A. A time-efficient approach toward DDoS attack detection in IoT network using SDN. *IEEE Internet Things J.* **2022**, *9*, 3612–3630.

23. Cvitić, I.; Peraković, D.; Periša, M.; Botica, M. Novel approach for detection of IoT-generated DDoS traffic. *Wirel. Netw.* **2021**, *27*, 1573–1586.
24. Al-Fayoumi, M.; Abu Al-Haija, Q. Capturing low-rate DDoS attack based on MQTT protocol in a software-defined IoT environment. *Array* **2023**, *19*, 100316. https://doi.org/10.1016/j.array.2023.100316.
25. Segura, G.N.; Barboza, E.C. Machine learning for distributed denial of service attack detection in software-defined IoT. In Proceedings of the 2024 IEEE 42nd Central America and Panama Convention (CONCAPAN XLII), San Jose, CA, USA, 27–29 November 2024; pp. 1–6. https://doi.org/10.1109/CONCAPAN63470.2024.10933894.
26. Ahmed, I.; Uddin, M.; Alshamrani, A.; Alzahrani, B. CICIoT2023: An intrusion detection dataset for Internet of Things networks. *IEEE Access* **2024**, *12*, 11256–11269.
27. Moustafa, N.; Slay, J. The TON_IoT datasets: A new generation of realistic IoT traffic for intrusion detection research. *Future Internet* **2021**, *13*, 72.
28. Liu, Y.; Zhang, K.; Wang, Z. Intrusion detection of manifold regularized broad learning system based on LU decomposition. *J. Supercomput.* **2023**, *79*, 20600–20648.
29. Belachew, H.; Beyene, M.; Desta, A.; Alemu, B.; Musa, S.; Muhammed, A. Design a robust DDoS attack detection and mitigation scheme in SDN-edge-IoT by leveraging machine learning. *IEEE Access* **2025**, *13*, 10194–10214.
30. Wang, W.; Wang, X. SDN-Defend: A lightweight online attack detection and mitigation system for DDoS attacks in SDN. *Sensors* **2022**, *22*, 8287.
31. Santos-Neto, M.J.; Bordim, J.L.; Alchieri, E.A.P.; Ishikawa, E. DDoS attack detection in SDN: Enhancing entropy-based detection with machine learning. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8021. https://doi.org/10.1002/cpe.8021.
32. Sattari, F.; Farooqi, A.H.; Qadir, Z.; Raza, B.; Nazari, H.; Almutiry, M. A hybrid deep learning approach for bottleneck detection in IoT. *IEEE Access* **2022**, *10*, 77039–77053.
33. Karthikeyan, V.; Murugan, K. A novel machine learning-based classification approach to prevent flow table overflow attack in Software-Defined Networking. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e7878.
34. Himanshu; Saha, K.; Das, P.; De, S. A network segmentation architecture for flow aggregation and DDoS mitigation in SDN using RAPID flow rules. In Proceedings of the 25th International Conference on Distributed Computing and Networking (ICDCN '24), Chennai, India, 4–7 January 2024; pp. 232–241. https://doi.org/10.1145/3631461.3631561.
35. Ravi, N.; Shalinie, S. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet Things J.* **2020**, *7*, 3559–3570.
36. Swami, R.; Dave, M.; Ranga, V. Voting-based intrusion detection framework for securing software-defined networks. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5927.
37. Bojarajulu, B.; Tanwar, S.; Singh, T.P. Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model. *Comput. Secur.* **2023**, *126*, 103064. https://doi.org/10.1016/j.cose.2022.103064.
38. Repetto, M.; Striccoli, D.; Piro, G.; Carrega, A.; Boggia, G.; Bolla, R. An autonomous cybersecurity framework for next-generation digital service chains. *J. Netw. Syst. Manag.* **2021**, *29*, 37. https://doi.org/10.1007/s10922-021-09607-7.
39. Hormozi, M.; Erfani, S. An SDN-based DDoS defense approach using route obfuscation. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7439. https://doi.org/10.1002/cpe.7439.
40. Vadivu, D.S.; Rajagopalan, N. RyuGuard: Combining Ryu and machine learning for proactive DDoS defense in software-defined networks. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8289. https://doi.org/10.1002/cpe.8289.
41. Chetouane, A.; Karoui, K. Risk based intrusion detection system in software defined networking. *Concurr. Comput. Pr. Exp.* **2024**, *36*, e7988.
42. Aslam, B.; Azam, A.; Imran, M.; Rizvi, S. ONOS flood defender: An intelligent approach to mitigate DDoS attack in SDN. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4534. https://doi.org/10.1002/ett.4534.
43. Carvalho, C.; Verdi, F.L.; Martinello, M. DataPlane-ML: An integrated attack detection and mitigation solution for software defined networks. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7434. https://doi.org/10.1002/cpe.7434.
44. Setitra, A.; Seridi, H.; Derhab, A. An efficient approach to detect distributed denial of service attacks for software defined internet of things. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4827. https://doi.org/10.1002/ett.4827.
45. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), Funchal, Portugal, 22–24 January 2018; pp. 108–116. https://doi.org/10.5220/0006639801080116.
46. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Gener. Comput. Syst.* **2021**, *100*, 779–796.

47. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419.
48. Lashkari, A.H.; Devlin, A.; Ghorbani, A.A. A Comprehensive survey of network flow datasets for intrusion detection. *Comput. Netw.* **2022**, *210*, 108921.
49. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
50. Lantz, B.; Heller, B.; McKeown, N. A network in a laptop: Rapid prototyping for software-defined networks. In Proceedings of the 2010 ACM SIGCOMM Workshop on HotNets, Monteret, CA, USA, 20–21 October 2010; Article 19, pp. 1–6. https://doi.org/10.1145/1868447.1868466.
51. Berde, P.; Gerola, M.; Hart, J.; Higuchi, Y.; Kobayashi, M.; Koide, T.; Lantz, B.; O'Connor, B.; Radoslavov, P.; Snow, W.; et al. ONOS: Towards an open, distributed SDN OS. In Proceedings of the 2014 ACM SIGCOMM Workshop on HotSDN, Chicago, IL, USA, 22 August 2014; pp. 1–6. https://doi.org/10.1145/2620728.2620744.
52. Kubo, R.; Fujita, T.; Agawa, Y.; Suzuki, H. Ryu SDN framework-open-source SDN platform software. *NTT Technol. Rev.* **2014**, *12*, 18–22. https://doi.org/10.53829/ntr201408fa4.
53. Bredel, M. OpenFlow and the Floodlight OpenFlow controller Control Center, ADMIN 17/2013. 2013. Available online: https://www.admin-magazine.com/Archive/2013/17/OpenFlow-and-the-Floodlight-OpenFlow-Controller (accessed on 11 November 2025).
54. Medved, J.; Varga, R.; Tkacik, A.; Gray, K. OpenDaylight: Towards a model-driven SDN Controller architecture. In Proceedings of the 2014 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Sydney, NSW, Australia, 19 June 2014; pp. 1–6. https://doi.org/10.1109/WoWMoM.2014.6918985.
55. Pfaff, B.; Pettit, J.; Koponen, T.; Jackson, E.; Zhou, A.; Rajahalme, J.; Gross, J.; Wang, A.; Stringer, J.; Shelar, P.; et al. The design and implementation of Open vSwitch. In Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI '15), Oakland, CA, USA, 4–6 May 2015; pp. 117–130. Available online: https://www.usenix.org/system/files/conference/nsdi15/nsdi15-paper-pfaff.pdf (accessed on 11 November 2025).
56. Rahman, A.; Khan, S.I.; Montieri, A.; Islam, J.; Karim, R.; Hasan, M.; Kundu, D.M.; Nasir, M.K.; Pescapè, P. BlockSD-5GNet: Enhancing security of 5G network through blockchain-SDN with ML-based bandwidth prediction. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4965. https://doi.org/10.1002/ett.4965.
57. Ariffin, R.; Ahmad, A. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Forensic Sci. Int. Digit. Investig.* **2021**, *105*, 102237. https://doi.org/10.1016/j.cose.2021.102237.
58. Ashfaq, M.; Rehman, F.; Ali, Z. Enhancing security in 5G edge networks: Predicting real-time zero trust attacks using machine learning. *Sensors* **2025**, *25*, 1905. https://doi.org/10.3390/s25061905.
59. Casaril, M.; Galletta, A. Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS². *Comput. Secur.* **2024**, *140*, 103799. https://doi.org/10.1016/j.cose.2024.103799.
60. Dandotiya, M.; Makwana, R.R.S. Secured DDoS attack detection in SDN using TS-RBDM with MDPP-Streebog based user authentication. *Trans. Emerg. Telecommun. Technol.* **2025**, *36*, e70052. https://doi.org/10.1002/ett.70052.
61. Galeano-Brajones, J.; Carmona-Murillo, J.; Valenzuela-Valdés, J.F.; Luna-Valero, F. Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN an experimental approach. *Sensors* **2020**, *20*, 816. https://doi.org/10.3390/s20030816.
62. Han, D.; Li, H.; Fu, X.; Zhou, S. Traffic feature selection and distributed denial of service attack detection in software-defined networks based on machine learning. *Sensors* **2024**, *24*, 4344. https://doi.org/10.3390/s24134344.
63. Huan, H.; Zhao, J.; Yang, H.; Li, X.; Cui, Y.; Chen, G. Towards feature selection for detecting LDDoS in SD-IoT of smart grids: A multi-correlation information EA-based method. In Proceedings of the 2023 2nd International Symposium on Computing and Artificial Intelligence, ISCAI 2023, Shanghai, China, 13–15 October 2023; pp. 60–66. https://dl.acm.org/doi/10.1145/3640771.3640786.
64. Liu, Z.; Wang, Y.; Feng, F.; Liu, Y.; Li, Z.; Shan, Y. A DDoS detection method based on feature engineering and machine learning in software-defined networks. *Sensors* **2023**, *23*, 6176. https://doi.org/10.3390/s23136176.
65. Oyucu, S.; Polat, O.; Türkoglu, M.; Polat, H.; Aksöz, A.; Agdas, M.T. Ensemble learning framework for DDoS detection in SDN-based SCADA systems. *Sensors* **2024**, *24*, 155. https://doi.org/10.3390/s24010155.
66. Polat, O.; Türkoğlu, M.; Polat, H.; Oyucu, S.; Üzen, H.; Yardımcı, F.; Aksöz, A. Multi-stage learning framework using convolutional neural network and decision tree-based classification for detection of DDoS pandemic attacks in SDN-Based SCADA systems. *Sensors* **2024**, *24*, 1040. https://doi.org/10.3390/s24031040.

67. Priyadarshini, I.; Mohanty, P.; Alkhayyat, A.; Sharma, R.; Kumar, S. SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi-LSTM-CNN. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4758. https://doi.org/10.1002/ett.4758.
68. Varma, P.R.K.; Sathiya, R.R.; Vanitha, M. Enhanced Elman spike neural network based intrusion attack detection in software defined Internet of Things network. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7503. https://doi.org/10.1002/cpe.7503.
69. Toony, R.; Dandoush, A.; Salah, K. Multi-block: A novel ML-based intrusion detection framework for SDN-enabled IoT networks using new packet- and flow-level features. *Internet Things* **2024**, *23*, 101231. https://doi.org/10.1016/j.iot.2024.101231.
70. Truong, H.-H.; Truong-Huu, T.; Cao, T.-D. Making distributed edge machine learning for resource-constrained communities and environments smarter: Contexts and challenges. *J. Reliable Intell. Environ.* **2023**, *9*, 119–134. https://doi.org/10.1007/s40860-022-00176-3.
71. Figueira, P.T.; Bravo, C.L.; López, J.L.R. Improving information security risk analysis by including threat-predictive models. *Comput. Secur.* **2020**, *88*, 101609.
72. Verma, S.; Gupta, R.; Sharma, P. A request aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attack in cloud computing. *Clust. Comput.* **2021**, *24*, 2149–2163. https://doi.org/10.1007/s10586-021-03234-2.
73. Connolly, A.Y.; Borrion, H. Reducing ransomware crime analysis of victims' payment decisions. *Comput. Secur.* **2022**, *119*, 102760.
74. Perumal, K.; Arockiasamy, K. Optimized deep neural network based DDoS attack detection and bait mitigation process in software defined network. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7692. https://doi.org/10.1002/cpe.7692.