Malaysian Journal of Computing, 10 (1): 2038-2058, 2025
Copyright © UiTM Press
eISSN: 2600-8238

DISTRIBUTED DENIAL OF SERVICE (DDOS) FRAMEWORK IN SOFTWARE-DEFINED NETWORKING (SDN): A COMPREHENSIVE REVIEW, CHALLENGES AND FUTURE DIRECTIONS

Kanqi Xie[1] , Mohamad Yusof Darus [2*], Boxun Liao[3], Nan Ding [4] and Azlin Ramli [5]

[1,2,3,4,5]College of Computing, Informatics and Mathematics*
Universiti Teknologi MARA (UiTM), 40450 Shah Alam

[1]2022650826@student.uitm.edu.my, [2*]yusof_darus@uitm.edu.my,
[3]2022298642@student.uitm.edu.my,
[4]2022636766@student.uitm.edu.my, [5]azlin.ramli.study@gmail.com

ABSTRACT

Distributed Denial of Service (DDoS) attacks represent a major threat to network security.. In response, this paper examines the potential of countering DDoS attacks through the integration of Software-Defined Networking (SDN). SDN separates the network control logic from the underlying routers and switches, which facilitates the communication between software components. Moreover, the synergy of SDN with Machine Learning (ML) and Deep Learning (DL) technologies provide a promising approach for effective threat mitigation. This systematic review explores the evolving landscape of information security defense frameworks within the context of Internet of Things (IoTs) security. Over the past five years, numerous articles have contributed to the understanding of SDN based DDoS defense architecture. This review encompasses various aspects, including the design of SDN based DDoS frameworks, implementation steps, data analysis methods, DDoS data sources, and application scenarios of defense frameworks. Performance and characteristics of different defense technologies are analyzed, addressing common challenges in the research field. This study provides a valuable reference for researchers to develop efficient and reliable DDoS defense frameworks in SDN mode.

Keywords: *Software Defined Networks (SDN), Distributed Denial of Service (DDos), IoT，Machine Learning and Deep Learning.*

Received for review: 02-01-2025; Accepted: 18-03-2025; Published: 01-04-2025
DOI: 10.24191/mjoc.v10i1.4422

1. Introduction

IoT is the latest technology trend that has emerged in the last decade, attracting researchers and developers (Kadri et al., 2024). It enables interconnection between heterogeneous devices and provides the opportunity to connect to the Internet. It has seen significant growth in various applications such as smart homes, smart cities, and smart vehicles (Zormati et al., 2024). Areas such as health care will also grow in the coming years (Neto et al., 2024; Sousa & Gonçalves, 2024). With the rapid growth and widespread adoption of IoT, these devices can be found in homes, offices, transportation, healthcare, telecommunications, agriculture, and other environments.

In the home intelligence, home security, video surveillance, product networking and tracking has an amazing growth. According to Cisco Systems, Machine-To-Machine connections (M2M) will grow 2.4 times from 6.1 billion in 2018 to 14.7 billion in 2023. Mobile M2M connections will increase fourfold from 1.2 billion in 2018 to 4.4 billion in 2023, at a compound annual growth rate of 30%. The growth of IoT devices is increasing compared to non-IoT devices (Saied et al., 2024). IoT will significantly change our attitude towards technology and the environment. By 2025, there are expected to be 30 billion IoT devices (Aldhaheri et al., 2024). These devices can communicate and interconnect with each other to exchange data. But most IoT devices have never been designed to handle security threats. Most of them are limited by resources, which makes them a potential attack surface for attackers. The risk of data leakage due to the often-insufficient processing and storage capacity of IoT devices is also increasing, resulting in the IoT being far more vulnerable to malicious attacks than traditional networks, and collecting and analyzing data to maintain the security of these devices will become increasingly important (Pisal, N et al., 2022). Because of this, IoT security has become a top priority.

With the rapid development of the next generation network technology, the integration of computing systems and other forms of systems will bring new issues. There is an urgent need to reconstruct network strategies and upgrade equipment to cope with the coming network security challenges(Gill et al., 2024). However, in traditional networks, there is a close connection between different planes of network devices. This makes dynamic management of the network difficult, because introducing new features and upgrading existing ones requires manual reconfiguration of all network devices, which are vender-specific and require individual configuration of all devices by network administrators. In addition, a controller needs to serve multiple switches. These switches periodically send the maximum allowed number of requests and wait for a timely response. As the number of ingress switches increases, the number of requests received by the controller also increases, which may cause performance degradation. In fact, like any other centralized system, a single centralized controller faces problems of scalability and reliability. For large-scale networks, it is very arduous and complex to manage hundreds of thousands of switches through a centralized controller(El Kamel, 2024).Yet the cost of traditional network equipment is high, mainly reflected in the hardware, so a flexible means of configuration and maintenance for complex networks is needed.

SDN addresses the challenges faced in traditional networks by providing simplified and centralized network management. It originated at Stanford University in the early 2000s. Its programmability and flexibility have made it a highly adopted technology in both academic and industrial settings (Kaur et al., 2021). It also improves the scalability, flexibility, control ability and network management ability of the network by separating the control plane and the data plane. Therefore, it can dynamically change the forwarding rules of DDoS traffic and improve the security of the network (Nurwarsito & Nadhif, 2021). In addition, SDN devices are cheaper than proprietary and vendor-specific devices because SDN has an open-source network operating system, which is a revolutionary technology to make the network dynamic and programmable to suit the requirements of modern data centers.

One of the biggest challenges in information security is to provide an acceptable level of security by guaranteeing the three cornerstones of information security, namely confidentiality, integrity, and availability. Among security threats, DoS and DDoS attacks have emerged as some of the most formidable threats on the Internet. The low cost and ease of launching DDoS attacks have contributed to their exponential growth (Balarezo et al., 2022). Although SDN is a secure network architecture compared with traditional IP-based networks, SDN itself is vulnerable to multiple types of network intrusions and faces severe deployment challenges(J. Singh & Behal, 2020). Controllers in SDN play a prominent role in monitoring and preventing the network from any possible attacks or malicious activities(Indrason & Saha, 2024). The goal of SDN is to ensure manageability and centralized control in the network by providing a flexible and programmable network architecture to cope with the growing number of users. The advantages presented by SDN are accompanied by security issues caused by some vulnerabilities in its architecture. The same security issues such as DDoS attacks in SDN are becoming more and more serious and complex, trying to exploit the programmability and centralized control features of the SDN architecture, although SDN is vulnerable to attacks, SDN itself can be used to thwart attacks (Wabi et al., 2023). DDoS attacks like Slow-TCAM attack can deny service by sending packets at a very low rate of 3.2 packets per second, due to its disguised traffic rate and similar behavior to legitimate clients, it is also able to evade existing defense mechanisms (Pascoal et al., 2020).

Therefore, it is necessary to conduct a comprehensive review of the SDN-based DDoS defense field, discuss the characteristics of various means and defense frameworks to deal with DDoS attacks in the SDN environment, and discuss the development potential of this research field, as well as the current common challenges and shortcomings. It provides a reference for researchers to develop a more efficient and reliable DDoS defense framework in SDN networks. This research utilizes: IoTs, SDN, DDoS attacks, Detection and prevention framework, as keywords, 90 related research articles in the past five years were screened. This study summarizes and analyzes various frameworks developed by researchers to identify and defend against DDoS attacks within the context of IoT using Software-Defined Networking (SDN). It discusses three primary areas: first, the role of the SDN plane in different DDoS defense frameworks; second, the methodologies employed in these various frameworks; and third, the databases utilized across the different approaches. Through this comprehensive analysis, the study offers insights and prospective suggestions aimed at guiding future research in this critical area of cybersecurity.

2. Research Background

DDoS attacks are the threats that can disrupt or even disable IoT network functions, such as their ability to collect, process, and transmit data. The separation of control and data planes in SDN enables simplified management, control, dynamic rule updates, analysis, and a comprehensive network view from a centralized control point. DDoS attacks can make IoT system devices inundated with a large number of data packets. The controller's resources may be depleted due to the continuous processing of legitimate and DDoS spoofed packets. Once the controller is unable to receive new legitimate packets, the SDN architecture may have problems, resulting in the controller being unreachable. Fast and accurate detection of DDoS attacks is still an extremely challenging task. Some DDoS attackers use packets that mimic normal traffic to compromise the functionality of IoT systems. In the process of DDoS attack, the normal network hides the traffic, which makes the traditional intrusion detection system based on packet cannot identify it (Alshahrani, 2023)。

It is difficult for DDoS detection methods to find a match between accuracy and efficiency. Methods based on statistical analysis have low accuracy, while methods based on machine learning are inefficient and expensive to train (Liu et al., 2022). Intrusion detection and prevention system is also an important means of DDoS defense. These systems can be hardware-based or software-based (Bukhari et al., 2024). The model used federated learning to enhance intrusion detection performance and protect privacy. Privacy concerns are alleviated by allowing multiple sensor nodes to train a central global model without leaking private data. They suffer from detection and rule installation delays, resulting in low throughput. Some of reseachers proposed PS-IPS can deploy ML-based malware defense on a single programmable switch, utilizing the switch's CPU and forwarding pipeline to achieve line rate of packet processing to achieve high throughput and low response time (Lee et al., 2024).

DDoS attacks can come in various forms as shown in Figure 1. DDoS attacks pose a greater challenge than traditional DDoS attacks because they can hide behind a large number of unidentified devices, making them more difficult to defend against (Uddin et al., 2024).

As it shown in Figure 2, from the data of the DDOS-Guard analytical report 2023, the number of DDoS attacks is maintained at a high level, and Internet technology and arts and entertainment types of enterprises are the most vulnerable to attacks.

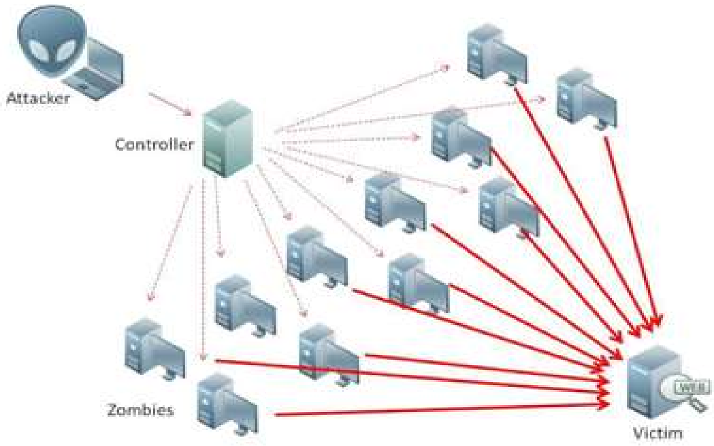

Figure 1. DDoS Attack.

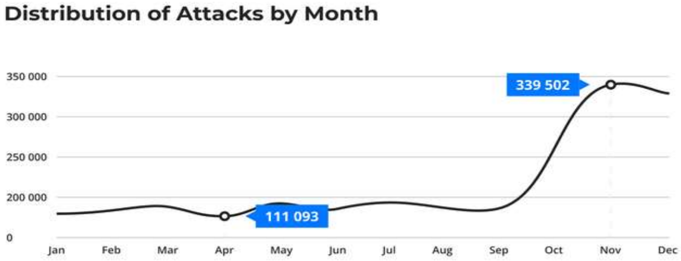

Figure 2. The attacks in the 2023 DDoS-Guard analysis report are distributed by month.

DDoS attacks are becoming more sophisticated, and the frequency and size of large-scale attacks launched each year are increasing, mainly against large organizations, data centers, and other enterprises. DDoS attacks based on new flows pose many security challenges and threats to the SDN architecture and have triggered the need for continuous research work to develop novel security defenses, thus giving rise to significant security issues in SDN(M. P. Singh & Bhandari, 2020)，therefore we need to study ways to enhance the defense of devices against DDoS.

SDN is a kind of network architecture and technology. SDN connects the underlying hardware infrastructure through the networking technology of software controller or Application Programming Interface (API) to realize the regulation of API (network traffic). This design differs from typical networks, where network traffic is managed by specific hardware devices such as routers and switches. SDN can create and manage virtual networks using software and traditional hardware.It provides a new packet routing management technology. In SDN, the control plane that decides where the traffic is transmitted is transferred to the software, while the data plane that sends the traffic remains on the hardware.By properly designing the application on the SDN controller, the underlying network attacks can be detected more effectively. A similar approach can be used in the IoT field, where the underlying network of the IoT device is monitored by the SDN controller, and the proactive defense mechanism is integrated on the SDN.

It features a three-tier structure comprising the control plane, data plane, and application plane as shown in Figure 3. Most switches support the OpenFlow protocol. Therefore, SDN switches are also called OpenFlow-enabled switches. The control plane consists of different controllers that convert these switches into smart devices such as routers, IDS, IPS, firewalls, according to the programs running on the application plane. The southbound API (usually OpenFlow) provides a switch between the control plane and the SDN.

The application can communicate with the controller through the northbound interface.

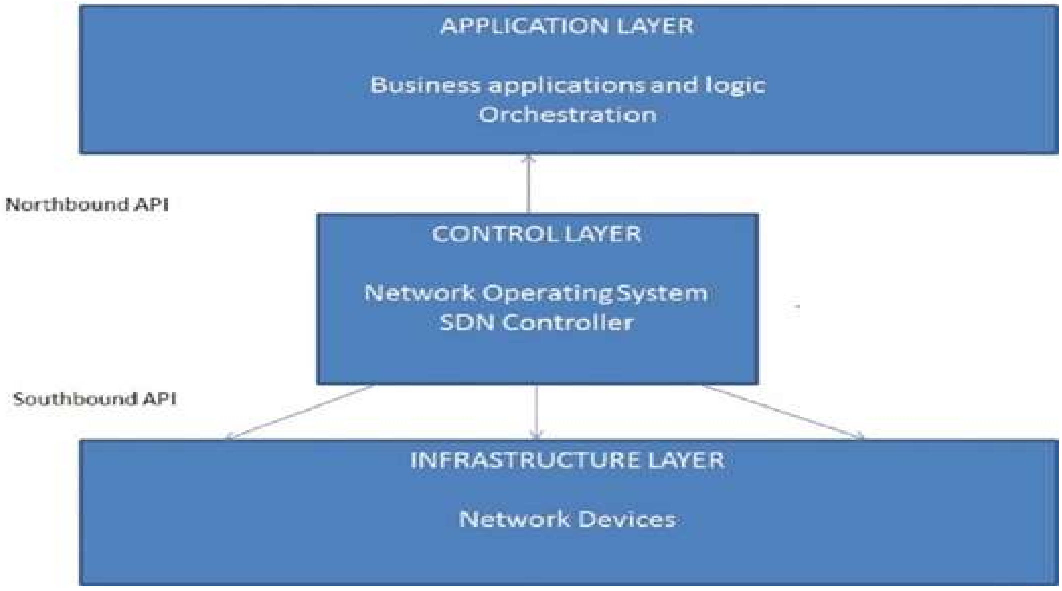

Figure 3. Architecture of SDN

SDN supports the dynamic operation control plane of the network by separating the data plane. The logical flow and efficiency of SDN is mainly based on the software controller (control plane). The network programming capabilities provided by SDN can solve many challenges of network management (Iranmanesh & Reza Naji, 2021)， In SDN, the controller has a comprehensive view of the whole network through its logically centralized architecture. A typical SDN structure is shown in Figure. 4, where the application layer is built on top of the SDN controller and is responsible for providing security measures such as detection and mitigation of network attacks. The control layer includes SDN control plane and data plane. The control plane consists of SDN controllers responsible for determining flow rules for OpenFlow-enabled switches. The SDN controller is responsible for network operations such as adding flow rules, defining network policies, etc. The physical layer consists of forwarding devices such as switches, which forward traffic according to network flow rules.

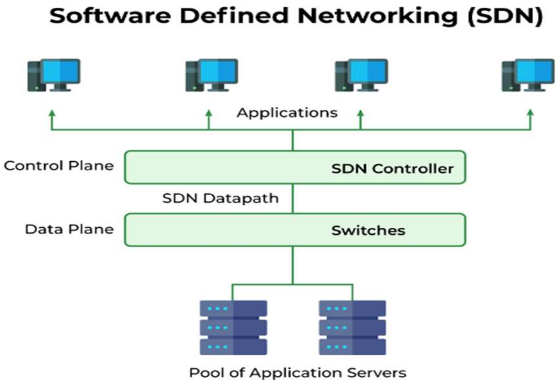

Figure 4. SDN Framework Layer

The control layer of SDN is highly vulnerable to injection attacks, where malicious hosts exploit false or invalid information or protocol messages. These attacks often stem from a lack of integrity checks on messages or events, resulting in controller DoS and policy failures. As switches are reduced to "dumb" devices, malicious hosts can inject format error messages that are not filtered by the data plane. Therefore, the switch will eventually send an exception message to the controller. The centralized design of SDN is a double-edged sword, and it is critical to develop SDN controllers with fault tolerance and the ability to verify updated state, measures that are necessary to mitigate these risks and fully exploit the benefits of centralized architectures(Kim et al., 2024). In addition, the vulnerabilities of SDN can cause DDoS attacks to launch various network attacks from the hosts connected to the switch, causing controller processing capacity overload and switch flow table flooding (El Kamel et al., 2022), Therefore, appropriate methods are needed to mitigate and even detect the damage caused by DDoS attacks.

3. Method

In order to investigate the above issues, this paper adopts a literature review and comparative analysis, hoping to find out the potential problems of the current defense framework and the future of the defense framework for IoT. Next, we discuss and analysis the characteristics of the current defense framework, and the data points involved in the framework.

3.1 Framework Analysis and Design

As shown in Figure 5, the steps to implement DDoS defense on SDN can be divided into four steps.

a. Step 1: Data Collection - Collect the traffic flowing through the SDN controller is a crucial step in monitoring, analyzing, and managing the network. To effectively collect traffic flowing through the SDN controller, it is essential to understand the types and sources of traffic. The traffic can be categorized into control plane traffic (e.g., routing protocols), data plane traffic (e.g., actual packets forwarded by switches), and management traffic (e.g., configuration updates, monitoring data). These traffic types originate from various sources, including SDN switches, hosts connected to the network, and external networks. Identifying and distinguishing these traffic types and their sources is critical for accurate data collection, analysis, and network management in an SDN environment.

b. Step 2: Data Identification – The collected data packets are parsed to extract key identifiers such as source/destination IP addresses, MAC addresses, port numbers, protocols, and flow details (e.g., 5-tuple: source IP, destination IP, source port, destination port, and protocol). Additional metadata like timestamps, TTL, ToS, and VLAN tags are also extracted, along with application-layer information using deep packet inspection (DPI). The parsed data is organized into a structured format (e.g., JSON, CSV), transforming raw packets into actionable insights for traffic analysis, anomaly detection, and network optimization.

c. Step3: Data Analysis - The parsed data is analyzed using pre-defined techniques to extract meaningful conclusions about network traffic. This includes identifying traffic patterns (e.g., peak times, common protocols), detecting anomalies (e.g., DDoS attacks, port scanning), calculating performance metrics (e.g., latency, packet loss), and analyzing flow-level data to optimize routing and identify bottlenecks.

d. Step 4: Countermeasure - Pre-defined coping strategies are applied to address issues identified during analysis, such as optimizing performance or enhancing security. This involves determining the target function (e.g., mitigating congestion, blocking attacks), implementing strategies like traffic rerouting, rate limiting, or dynamic flow rule updates via the SDN controller, and leveraging automation for real-time responses. The effectiveness of these measures is monitored and refined through feedback, ensuring the network adapts to changing conditions, mitigates threats, and maintains optimal performance within the framework.

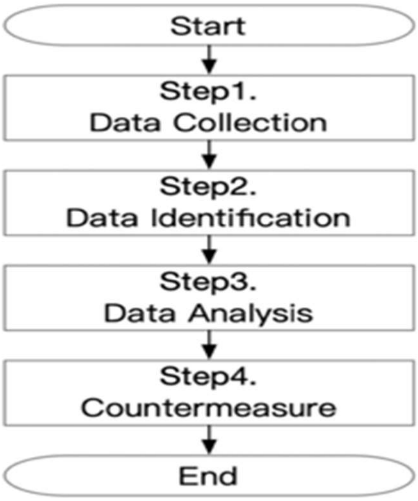

Figure 5. Flowchart of designing and deploying DDoS defense framework on SDN

Figure 6 likely illustrates the interaction between the data plane and control plane in an SDN architecture to detect and mitigate DDoS. The Data Plane Components in SDN involve traffic collection, where SDN switches gather incoming traffic from various sources like hosts and external networks, forwarding it to the control plane for analysis or processing it locally based on pre-installed flow rules. The data plane also enforces flow rules set by the control plane, such as forwarding, dropping, or rate-limiting packets. In Case 1, the data plane performs local analysis, identifying basic traffic patterns or anomalies without involving the control plane, enabling efficient handling of simpler tasks directly at the switch level.

The Control Plane Components in SDN involve centralized analysis, where the SDN controller receives traffic statistics and metadata from the data plane for in-depth analysis, utilizing algorithms like machine learning or statistical methods to detect DDoS attacks based on patterns such as traffic spikes or unusual packet sizes. Once an attack is detected, the control plane engages in decision making, determining countermeasures like blocking malicious IPs, rerouting traffic, or rate-limiting specific flows. It then sends flow rule updates to the data plane to enforce these countermeasures, ensuring the network responds dynamically to threats and maintains optimal performance.

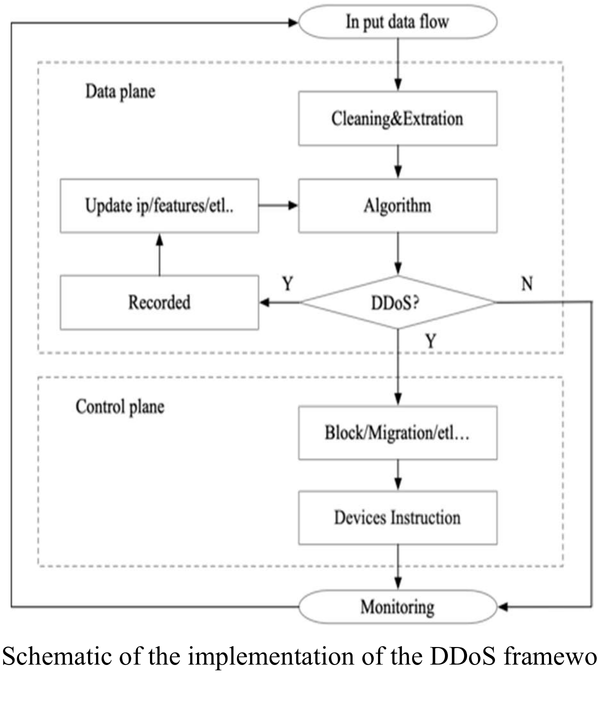

Figure 6. Schematic of the implementation of the DDoS framework on SDN

4. Result and Discussion

a. Defense Framework

The defense framework can be configured independently in a single plane, or it can cover the entire SDN. Some researchers focus on the data plane. By comparing different defense framework designs, the characteristics of different defense frameworks can be analyzed, which is helpful to choose the layout of defense frameworks reasonably. (Chauhan & Atulkar, 2023a) proposed framework uses a stack-based hybrid classifier in the data plane to detect DDoS attacks in a real-time environment. (Shirsath et al., 2024) introduces a framework using P4 language to analyze network traffic. The framework utilizes the data and control plane and uses data and statistical analysis techniques to identify and classify benign and malicious traffic to prevent interference from harmful packets.

Ali et al. (2020) proposed a hierarchical control plane SDN architecture for multi-domain communication. It used the statistical method called PCA to reduce the dimension of big data traffic and adopted a SVM classifier to detect DDoS attacks. (Sangodoyin et al., 2019)using a Mininet simulator, a floodlight controller, and a network performance testing tool, a mitigation mechanism was developed to counter these attacks by pushing the reaction flow from the controller to the attack switch port. The DDoS attack is mitigated with low performance overhead by pushing the flow through the controller and does not require changing the deployment operation mode of the controller.

Khedr et al. (2023a) proposed a DDoS attack detection and mitigation framework based on SDN with four main modules and five layers. The proposed framework can efficiently detect high-and low-rate DDoS attacks, is able to distinguish between attack traffic and burst traffic and protect local and remote IoT nodes by preventing the infection from spreading to the ISP level. The framework proposed in (Varghese & Muniyal, 2021a)solves the performance problem of IDS and the design problem of SDN against DDoS attacks by integrating intelligence in the data layer using Data Plane Development Kit (DPDK) in the SDN architecture. VNF (Virtual Network Function) statistical anomaly detection algorithm implemented by DPDK in the data plane can quickly detect DDoS attacks.

Other reseachers have proposed an intelligent data plane is deployed to detect DDoS attacks in the real environment, and a control plane is used to defend against them.However, most of the frameworks designed by researchers will apply the data plane and the control plane simultaneously. While the data plane completes the work of data cleaning and analysis, the control plane is used to complete the DDoS defense strategy (Chauhan & Atulkar, 2023b).

In (Riyad, 2021a), the DDoS defense phase of the data plane, it is mainly responsible for defending the attack packets through simple traffic analysis. In the control plane, it extracts features from the data packets, selects the important features based on rough set entropy, and uses the ensemble classifier to classify the flow into normal flow and attack flow. Update the flow rules based on the obtained results.

A five-stage defense framework was proposed in (Snehi et al., 2024) d, which adopted multi-level stack integration framework and supported by physical device behavior attributes to implement attack detection as a service, and realized a low-cost, reusable, and portable framework. The novel design of the proposed framework provides a lightweight mitigation solution for SDN controllers, ensuring negligible impact on controller performance. (Ali et al., 2023)proposed an optimized hierarchical control plane SDN architecture for multi-domain communication. Based on the original framework, the proposed architecture improves the classification performance and accuracy, and reduces the false positive rate.

According to Ezeh & de Oliveira (2023), Generative Adversarial Network (GAN) ensembles have been applied for anomaly detection in SDN environments. This approach combines a Global Network Innovation Environment (GENI) testbed to propose a controller-based framework that consists of multiple components across detection chains, generating a customized dataset to address three of the most prevalent contemporary cyber-attacks. In the defense framework outlined by Riyad (2021b), there are two main stages. The data plane's DDoS defense phase is primarily responsible for mitigating attack packets through basic traffic analysis. During the DDoS detection phase, the control plane extracts features from data packets using a rough set entropy method to identify the most significant characteristics. An ensemble classifier then categorizes the flows as either normal or malicious, and flow rules are updated based on these classifications. The proposed model achieved impressive accuracy rates of 96.3% for benign traffic and 96.12% for attack traffic.

Sahay et al. (2017) proposed an autonomous DDoS defense framework that effectively bridges the gap between various security functions, encompassing traffic monitoring, anomaly detection, and mitigation, while reducing the need for human intervention. By strategically distributing basic security functions, it processes DDoS traffic based on customer requests, thereby fostering collaboration between Internet Service Providers (ISPs) and customers to mitigate DDoS attacks.

Dai et al. (2024) introduced a framework known as DAmpADF, which employs bloom filters at the edge or core routers of ISPs or organizations to filter out malicious DNS responses. Additionally, some researchers have proposed an integrated framework for detecting DDoS attacks and ARP spoofing in IoT environments, utilizing machine learning and a stateful P4, SDN-based multi-controller architecture. Khedr et al. (2023) assert that P4-HLDMC addresses the limitations of standard SDN architectures, ensuring scalability, performance, and effective response to attacks. This framework demonstrates a high detection rate, low false alarm rate, low latency, and rapid detection times.

A similarity-based aggregation algorithm is proposed in(Wang et al., 2024) to correlate and aggregate alerts, a Transformer-based model is trained, and a threat estimation method is proposed to evaluate the prediction results. The framework can effectively aggregate alerts, predict different attack intelligence, and assess the level of threat faced. (Varghese & Muniyal, 2021)proposed a framework based on SD-IoT to provide security services for IoT networks. We developed a Counter-based DDoS Attack Detection (C-DAD) application based on counter values of different network parameters, which helps to successfully detect DDoS attacks. Deploying it on SDN can effectively detect attacks in the shortest time and consume less CPU and memory resources. Oyucu et al., 2024 proposed an ensemble learning technology based on decision tree, which used perform feature selection and hyperparameter tuning to enhance the performance of the decision tree ensembl model, and accurately distinguished normal and DDoS attack traffic to detect DDoS attacks in the system.

According to Revathi et al. (2022), a discrete, scalable memory-based SVM algorithm has been proposed to detect DDoS threats within an SDN mitigation framework. This process utilizes Spark for data preprocessing and employs semantic multilinear component analysis for feature extraction. Following the attack detection process, the mitigation server intelligently filters out malicious bot traffic while managing the remaining traffic, effectively reducing attack traffic and minimizing the drop of benign traffic. The evaluation was conducted using the KDD dataset, training the network model within an SDN environment for threat detection and mitigation.

Cherian and Varma (2023) introduced a framework that detects reflection and exploitation attacks across TCP, UDP, and ICMP protocols. This framework was tested under various network parameters, such as the number of attack nodes and IoT load, with performance metrics including SDN controller workload, CPU utilization, and attack detection time being measured to analyze the types of DDoS attacks. The effective utilization of CPU resources aids in the rapid identification of these attack types.

Zhang et al. (2021) proposed a security-oriented low-latency flow monitoring and sampling algorithm, alongside a service-oriented packet classification and identification framework. This framework integrates spectral clustering and a variational autoencoder to differentiate abnormal traffic from normal traffic, adapting seamlessly to hybrid DDoS attacks and providing predictive capabilities for unknown attacks not covered in the training dataset.

Y. Zhou et al. (2021) proposed a framework designed to actively adapt to the IoT attack surface, dynamically optimizing defense strategies and quickly deploying corresponding defense mechanisms. This hybrid active defense mechanism combines Moving Target Defense (MTD) and cyber deception to confuse attackers by dispersing misleading information. A defender-led signaling game model was introduced to formalize the defense scenario and describe the interaction between the defender and the attacker, along with an optimization algorithm to solve the decision problem for cost-effective defense implementation.

Anyanwu et al. (2023) presented an effective system for DDoS attack detection using a grid search cross-validation (GSCV) exhaustive parameter search technique and the Radial Basis Function Support Vector Machine (RBF-SVM) algorithm. In a follow-up study in 2024, Chee et al. introduced IoTSecSim, a novel simulation framework and software tool that aids in developing IoT networks by providing adaptable configurations for IoT devices and topology details. Notably, IoTSecSim can simulate attack behaviors and implement defenses at both the node and network levels, serving as a versatile and expandable platform for modeling evolving cyber-attacks on IoT networks and assessing the effectiveness of defense mechanisms. This enables users to design and evaluate new defense systems prior to actual implementation and deployment.

In the study by Doriguzzi and Siracusa (2024), the emphasis is on the convergence of the Federated Learning (FL) process within a dynamic network security context. In this framework, the trained model requires frequent updates to stay aligned with the latest attack profiles, ensuring that all members of the federation have access to up-to-date detection signatures. The paper presents FLAD, a FL solution for network security that incorporates an adaptive mechanism. This FL process is enhanced by dynamically allocating additional computational resources to members facing challenges in learning attack profiles, all while maintaining privacy by not sharing any test data and continuously monitoring the performance of the trained model.

For emerging applications in IoT and 5G networks, Krishnan et al. (2020) proposed an autonomous multi-layer security framework that merges fog/edge computing with SDN architecture, termed the Distributed Threat Analytics and Response System (DTAR). The primary detection schemes are implemented in the data plane and include coarse-grained behavior analysis, anti-spoofing measures, flow monitoring, and fine-grained traffic detection algorithms based on multi-feature entropy. Table 1 below is the plane and implementation method of the above framework.

Table 1. Framework for DDoS analysis method deployed in SDN

Researcher	Data Plane	Control Plane	Method
(Chauhan & Atulkar, 2023a)	√		ML
(Shirsath et al., 2024)		√	ML
(Ali et al., 2020)			ML
(Sangodoyin et al., 2019)	√	√	Statistics
(Khedr et al., 2023a)	√		ML
(Varghese & Muniyal, 2021a)	√		Statistics
(Chauhan & Atulkar, 2023b)	√		Statistics
(Riyad, 2021a)	√	√	ML
(Snehi et al., 2024)		√	ML
(Ali et al., 2023)	√		ML
(Ezeh & de Oliveira, 2023)		√	ML
(Riyad, 2021b)	√	√	ML
(Sahay et al., 2017)	√		ML
(Dai et al., 2024)	√		Statistics
(Khedr et al., 2023b)	√	√	ML
(Wang et al., 2024)			DL
(Varghese & Muniyal, 2021b)	√		VNF
(Oyucu et al., 2024)	√		ML
(Revathi et al., 2022)	√		ML
(Cherian & Varma, 2023)	√	√	DL
(Zhang et al., 2021)	√		ML
(Y. Zhou et al., 2021)	√		ML
(Anyanwu et al., 2023)	√		ML
(Chee et al., 2024)	√	√	ML
(Doriguzzi-Corin & Siracusa, 2024)	√		DL
(Krishnan et al., 2020)	√		Statistics

Most of the current SDN-based DDoS defense frameworks use machine learning to analyze data sources, and the number of frameworks using deep learning methods is small, and most of the frameworks are arranged in the data plane.

b. Database for SDN Based DDoS Defense Framework

In addition to the above DDoS detection framework, for different application scenarios, this reflects the flexibility of SDN-based defense framework design. However, the defense design logic and database analysis used by different types of defense frameworks are different, so it is necessary to compare and analyze different frameworks to judge the frontier of defense frameworks. In recent years, machine learning can provide the necessary intelligence by using sophisticated algorithms and insights gained from collected data, and it is proven to provide accurate predictions for DDoS detection by identifying patterns, identifying anomalies, and predicting potential threats in real time (Alwahedi et al., 2024). In their 2022 work, (Mehra & Badotra t al., 2022) present an innovative framework leveraging machine learning models for the early detection of Distributed Denial of Service (DDoS) attacks. The framework not only identifies DDoS attacks at their nascent stages but also implements timely and targeted mitigation measures. Upon detecting malicious traffic through the proposed method, the framework promptly initiates actions to block the identified traffic from the targeted side.

Utilizing ML algorithms, and more recently DL algorithms have been used in various studies to detect, locate, and mitigate cyberattacks against SGCPS (Hasan et al., 2024). However, it is still challenging to improve the performance, accuracy, and real-time performance of these algorithms. The availability of high computational power and edge computing has led to the development of more sophisticated ML and DL algorithms, such as ensemble ML, CNN, LSTM, and RL. The potential of these advanced ML and DL algorithms to provide intelligent security countermeasures has attracted more research. (Ribeiro et al., 2023) proposed a DDoS detection and mitigation architecture based on SDN. The Moving Target Defense (MTD) approach is considered to redirect malicious flooding to consumable low-capacity servers to protect the primary server and deter attackers at the same time. The redirection decision is sensor-based, and a ML algorithm is used for flow classification. When a malicious flow is detected, the sensor informs the SDN controller to include it in the list of malicious hosts and implement redirection.

The framework presented by Mehra and Badotra (2022b) enables early detection of DDoS attacks using machine learning models, followed by the implementation of appropriate mitigation techniques. It generates TCP-SYN DDoS traffic directed at the ONOS SDN controller, utilizing the open-source access tool SNORT in conjunction with the hping3 tool. This approach allows for the early identification of DDoS attacks and the subsequent blocking of malicious traffic from the destination once detected.

Fadel et al. (2022) introduced a Hybrid Deep Learning Intrusion Detection and Prevention (HDLIDP) framework that enhances detection accuracy while addressing various challenges associated with DDoS traffic detection in SDN environments. Abdallah et al. (2022) proposed a dual-module method for detecting DDoS traffic, which utilizes information entropy alongside Deep Neural Networks (DNNs). The initial detection module computes the information entropy of source and destination IP addresses in packets to assess suspicious network traffic. Subsequently, the DNN-based module verifies potential DDoS attacks.

Experimental results show that this method achieves a recognition rate for DDoS activity exceeding 99% while significantly improving overall accuracy. Compared to detection methods based solely on information entropy, the proposed framework exhibits a much lower False Alarm Rate (FAR). Furthermore, it is designed to reduce detection time and enhance resource utilization efficiency.

Tan et al. (2020) developed a comprehensive DDoS attack detection and defense framework tailored for SDN environments. This framework begins with a detection trigger mechanism deployed in the data plane to filter through network traffic for anomalies. Following this, a hybrid machine learning algorithm combining K-Means and KNN is utilized to identify suspicious data flows flagged by the trigger mechanism, leveraging the rate characteristics and asymmetric features of the data flows. In response to detected DDoS attacks, the SDN controller implements appropriate defensive actions.

According to Salim et al. (2024), a novel cybersecurity framework for the industrial IoT environment has been proposed, based on federated learning and information fusion, termed FL-CTF. This framework employs an artificial neural network designed with federated learning principles, optimizing model training rounds based on user satisfaction. This optimization leads to improvements in the average accuracy of each attack vector. The evaluation demonstrates enhanced F1 scores, reduced training rounds, and minimized CPU consumption, outperforming existing studies. The federated learning model shows increased accuracy and decreased false positive rates, especially with the integration of a newly merged dataset.

Macas et al. (2024) conducted a comprehensive survey that outlines recent research on adversarial example-based attacks against deep learning-based cybersecurity systems. This survey sheds light on the inherent risks posed by such attacks and presents effective countermeasures to mitigate these risks, aiming to equip the cybersecurity community with insights into the evolving landscape of adversarial attacks and fostering proactive defense strategies against potential vulnerabilities in deep learning-based security systems.

Mall et al. (2023) propose various deep learning models for the efficient detection of DDoS attacks within the SD-CPS framework, utilizing a scalable and adaptable SDN architecture. By analyzing multiple deep learning techniques, they aim to identify the most effective method under various attack scenarios. Additionally, Haider et al. (2020) proposed a Deep CNN ensemble framework that frames the DDoS detection challenge in SDN and is evaluated against the current state-of-the-art flow-based framework, leading to improved detection accuracy.

To address the detection challenges posed by low-rate DDoS attacks, a Low-Rate DDoS Attack Detection Framework (LRDADF) was proposed. This framework not only employs deep learning methods for detection but also introduces a mathematical model to implement mitigation strategies alongside a novel Hybrid Approach for Low-Rate DDoS Detection (HA-LRDD) algorithm (Pasha et al., 2023). Furthermore, Yungaicela-Naula et al. (2022) proposed a modular, flexible, and extensible SDN-based framework that integrates a deep learning-based intrusion detection system (IDS) with a deep reinforcement learning-based intrusion prevention system (IPS) to counter slow DDoS threats. This framework incorporates scalability features to design a lightweight DRL-based IPS, ensuring a rapid mitigation response. The proposed IDS achieves an average detection rate of 98% at a 30% traffic sampling rate, while the IPS records a 100% success rate in defending against slow DDoS attacks. Table 2 show the difference algorithm and datasets of the above framework.

Table 2. Comparison of algorithmic strategies and data sources for different defense frameworks

Researcher	ML	DL	DDoS Data
(Alwahedi et al., 2024)	√		Simulation datas
(Mehra & Badotra, 2022a)	√		CICDDoS 2019
(Hasan et al., 2024)		√	CICDDoS 2019
(Ribeiro et al., 2023)	√		Simulation datas
(Mehra & Badotra, 2022b)		√	CICDDoS 2019
(Fadel et al., 2022)		√	Simulation datas
(Abdallah et al., 2022)		√	Real datas
(Tan et al., 2020)	√		Simulation datas
(Salim et al., 2024)	√		ToN_IoT and CICDDoS 2019
(Macas et al., 2024)			A survey
(Mall et al., 2023)		√	CICDDoS 2019
(Haider et al., 2020)		√	CICDDoS 2017
(Pasha et al., 2023)		√	Simulation datas
(Yungaicela-Naula et al., 2022)		√	Simulation datas

Most of the mainstream SDN based DDoS defense frameworks for DDoS data source analysis are based on CICDDoS database, only a small number of frameworks will use simulation data, and a very small number of frameworks will use real life data for verification.

c. Scenarios of the SDN-based DDoS defense framework

The increase in DDoS attacks has made it crucial to address the challenges faced by the IoT industry. Bhayo et al. (2020) proposed an SD-IoT-based framework designed to provide robust security services for IoT networks by detecting DDoS attacks based on the counter values of various network parameters. Given the flexibility and scalability of SDN, it is anticipated that future integrations will support IoT devices and edge computing, helping edge computing servers respond quickly to client requests for delay-sensitive services (H. Zhou et al., 2023). The source-based DDoS defense mechanism can be effectively employed in both fog and cloud environments, deploying a DDoS defense module on the SDN controller to detect abnormal behavior linked to DDoS attacks at the network and transport layers (Priyadarshini & Barik, 2022).

Current innovations also include the use of hybrid cloud frameworks for DDoS mitigation. Jeba Praba and Sridaran (2023) introduced the Log-Cluster DDoS Tree mitigation (LCDT-M) framework aimed at detecting and defending against DDoS attacks in a hybrid cloud setting.

In another approach, Bhayo et al. (2023) proposed a machine learning-based method to detect DDoS attacks in SDN-WISE IoT controllers. This method integrates a machine learning detection module and utilizes a testbed environment to simulate DDoS traffic. By logging network data and preprocessing it into a dataset, algorithms such as Naive Bayes (NB), Decision Tree (DT), and Support Vector Machine (SVM) are employed for classification. Performance evaluations show that NB achieves 97.4% accuracy, SVM 96.1%, and DT 98.1%. The detection module effectively utilizes only 30% of memory and CPU resources, conserving 70% while processing an average of 48 packets per second, ultimately enhancing IoT network security.

Bawany and Shamsi (2019) introduced SEAL (Secure and Agile), an adaptive DDoS defense framework based on SDN specifically for smart city applications. The SEAL framework leverages the global visibility, centralized control, and programmability of SDN to improve security and resilience against DDoS attacks targeting both application servers and network resources. It consists of three modules: D-Defense, A-Defense, and C-Defense, and employs a custom estimated Weighted Moving Average (EWMA) filter to achieve adaptivity. The framework also introduces a novel source-based DDoS defense scheme applicable in fog and cloud computing scenarios.

Febro et al. (2022) presented ShieldSDN and ShieldCHAIN, inter-organizational collaborative defense frameworks using P4, SDN, and blockchain technology. These frameworks not only mitigate DDoS attacks but can also generate attack fingerprints, known as Indicators of Compromise (IOCs). These IOCs are shared with other organizations to enhance collective defense mechanisms against shared threats. In contrast, Murtuza and Asawa (2024) proposed a security framework to prevent and mitigate link flooding attacks in SDN, focusing on limiting attackers' reconnaissance probes to gather network topology information. By preventing accurate topology acquisition, the framework utilizes alternative paths and hop count operations to disrupt the reconnaissance process. Additionally, Houda et al. (2023) introduced the MiTFed framework, which enables multiple SDN domains to collaborate in building a global intrusion detection model without sharing sensitive datasets.

The FedAAA-SDN framework developed by Sousa and Gonçalves (2024) is designed to facilitate authentication, authorization, and accounting mechanisms in SDN controllers across diverse networks. This framework enables joint authentication and authorization processes for network functions while enforcing policies based on user context and access networks. Its proof of concept, implemented with OpenDaylight, OpenID Connect, and Keycloak, demonstrated its ability to reduce threats through trust levels and trust policies.

As we move toward Industry 5.0, advanced 6G technologies—including immersive cloud extended reality (XR), autonomous vehicles, holographic communication, and digital twins—are expected to significantly increase the number of connected devices, thereby expanding the attack surface. This reality raises concerns about data breaches, privacy violations, and system outages, underlining the need for innovative solutions to enhance the reliability and security of advanced 6G applications and their associated IoT devices. In this context, Abou El Houda et al. (2024) proposed the AdaptSDN framework, leveraging SDN technology to enhance the security of Industrial Internet of Things (IIoT) applications in 6G and beyond. This framework employs ensemble learning techniques to improve the accuracy of intrusion detection systems and minimizes the impact of attacks by segregating IIoT devices into network slices.

Furthermore, Chen et al. (2022) suggested the integration of Network Function Virtualization (NFV) technology to implement comprehensive defenses against potential DDoS attacks targeting the SDN control plane, highlighting a key future development direction for SDN. This is critical, as malicious entities can exploit weaknesses in the SDN. Table 3 shows the summarize of different IoT-DDoS defense frameworks above.

Table 3. Characteristics and usage scenarios of different IoT-DDoS defense frameworks

Researcher	Scenarios
(Bhayo et al., 2020)	Fog
(H. Zhou et al., 2023)	Edge network devices
(Priyadarshini & Barik, 2022)	Fog
(Jeba Praba & Sridaran, 2023)	Fog
(Bhayo et al., 2023)	IoT-controller
(Bawany & Shamsi, 2019)	Smart-City
(Priyadarshini et al., 2020)	Fog
(Febro et al., 2022)	Blockchain
(Murtuza & Asawa, 2024)	Blockchain
(Houda et al., 2023)	Between SDN controllers
(Sousa & Gonçalves, 2024)	Between SDN controllers
(Abou El Houda et al., 2024)	6G
(Chen et al., 2022)	Virtual network

5. Conslusion

Through comparative analysis, we observe a scarcity of frameworks specifically aimed at defending against DDoS attacks targeting IoT devices, especially in scenarios involving multiple IoT devices. Most of the current research predominantly focuses on data processing, and the data utilized rarely aligns with the specific requirements of IoT devices (Zhang, Liu, & Wang, 2022). The findings can be summarized as follows:

a. **Framework Deployment:** Most SDN-based DDoS defense frameworks are primarily deployed on the data plane for data collection and processing, with limited consideration given to responses from the control plane within the framework.
b. **Methodologies:** A majority of these frameworks employ machine learning techniques, while only a few utilize basic statistical data methods, indicating room for further optimization in data learning approaches.
c. **Data Sources:** Most frameworks rely on CICDDoS pair databases, which lack dedicated data collection efforts for IoT devices.

This research also highlights the need for suitable DDoS warning algorithms tailored for 5G smart home environments. These algorithms should incorporate deep learning techniques to analyze user habits and predict potential DDoS attacks (Chen, Zhang, & Li, 2021). Furthermore, given the inevitability of UDP/TCP flooding DDoS attacks, future work should focus on employing deep learning algorithms to ensure the basic security of smart home environments.

In the context of dynamic urban landscapes, the integration of technology and automation is crucial for sustainability. The synergy between human intelligence and technological advancements fosters a collaborative innovation ecosystem. Automation, a continuous evolution since the Industrial Revolution, significantly shapes urbanization (Huda et al., 2024). Smart homes, as a facet of IoT-based automation, aim to enhance comfort, convenience, and overall quality of life. Over the past decade, various automation techniques have been proposed and implemented, indicating a pressing need to understand existing methods to guide future research and refine technologies for human benefit.

This exploration emphasizes the potential of leveraging SDN technology to strengthen defense mechanisms for IoT systems, highlighting the crucial role of innovative technologies and intelligent approaches in maintaining the security of these systems. The survey provides an in-depth examination of SDN-based defenses against DDoS attacks. Through careful analysis and synthesis of contemporary technologies, it contributes significantly to the evolution of information security technology, enhancing the understanding of SDN technology's role and offering strategic guidance for implementing and innovating DDoS defenses while designing effective SDN-based defense frameworks.

In summary, this work systematically dissects the design process of SDN-based DDoS defense methods in network security. It consolidates common data analysis techniques, outlines defense framework layouts, and identifies prevalent data analysis sources and application scenarios, providing valuable insights and guidance for future research endeavors.

Acknowledgement

The authors gratefully acknowledge the research support provided by the College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia.

Funding

The author(s) received no specific funding for this work.

Author Contribution

Author 1 and Author 2 collaborated on crafting the literature review and supervising the article writing process. For the research methodology, Author 1, Author 2, Author 3, Author 4 and Author 5 collectively contributed. The analysis and interpretation of results were undertaken by Author 1 and Author 2.

Conflict of Interest

The authors have no conflicts of interest to declare.

References

Abdallah, A., Ishak, M. K., Sani, N. S., Khan, I., Albogamy, F. R., Amano, H., & Mostafa, S. M. (2022). An Optimal Framework for SDN Based on Deep Neural Network. Computers, Materials and Continua, 73(1), 1125–1140. https://doi.org/10.32604/cmc.2022.025810

Abou El Houda, Z., Brik, B., & Ksentini, A. (2024). Securing IIoT applications in 6G and beyond using adaptive ensemble learning and zero-touch multi-resource provisioning. Computer Communications, 216, 260–273. https://doi.org/10.1016/j.comcom.2024.01.018

Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. In Internet of Things and Cyber-Physical Systems (Vol. 4, pp. 110–128). KeAi Communications Co. https://doi.org/10.1016/j.iotcps.2023.09.003

Ali, J., Roh, B.-H., Lee, B., Oh, J., & Adil, M. (2020). A Machine Learning Framework for Prevention of Software-Defined Networking controller from DDoS Attacks and dimensionality reduction of big data. International Conference on ICT Convergence, 2020-Octob, 515–519. https://doi.org/10.1109/ICTC49870.2020.9289504

Ali, J., Shan, G., Gul, N., & Roh, B.-H. (2023). An Intelligent Blockchain-based Secure Link Failure Recovery Framework for Software-defined Internet-of-Things. Journal of Grid Computing, 21(4). https://doi.org/10.1007/s10723-023-09693-8

Alshahrani, M. M. (2023). A Secure and Intelligent Software-Defined Networking Framework for Future Smart Cities to Prevent DDoS Attack. Applied Sciences (Switzerland), 13(17). https://doi.org/10.3390/app13179822

Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. In Internet of Things and Cyber-Physical Systems (Vol. 4, pp. 167–185). KeAi Communications Co. https://doi.org/10.1016/j.iotcps.2023.12.003

Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2023). RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network. Ad Hoc Networks, 140. https://doi.org/10.1016/j.adhoc.2022.103026

Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., & Kandeepan, S. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. In Engineering Science and Technology, an International Journal (Vol. 31). Elsevier B.V. https://doi.org/10.1016/j.jestch.2021.09.011

Bawany, N. Z., & Shamsi, J. A. (2019). SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. Journal of Network and Computer Applications, 145. https://doi.org/10.1016/j.jnca.2019.06.001

Bhayo, J., Hameed, S., & Shah, S. A. (2020). An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT). IEEE Access. https://doi.org/10.1109/ACCESS.2020.3043082

Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDoS attack detection in software-defined IoT (SD-IoT) networks. Engineering Applications of Artificial Intelligence, (Vol .123), Article 106432. https://doi.org/10.1016/j.engappai.2023.106432

Bukhari, S. M. S., Zafar, M. H., Houran, M. A., Moosavi, S. K. R., Mansoor, M., Muaaz, M., & Sanfilippo, F. (2024). Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, 155. https://doi.org/10.1016/j.adhoc.2024.103407

Chauhan, P., & Atulkar, M. (2023a). A Framework for DDoS Attack Detection in SDN-Based IoT Using Hybrid Classifier. In Lecture Notes in Electrical Engineering (Vol. 946). https://doi.org/10.1007/978-981-19-5868-7_67

Chauhan, P., & Atulkar, M. (2023b). A Framework for DDoS Attack Detection in SDN-Based IoT Using Hybrid Classifier. In Lecture Notes in Electrical Engineering (Vol. 946). https://doi.org/10.1007/978-981-19-5868-7_67

Chee, K. O., Ge, M., Bai, G., & Kim, D. D. (2024). IoTSecSim: A framework for modelling and simulation of security in Internet of things. Computers and Security, 136. https://doi.org/10.1016/j.cose.2023.103534

Chen, K.-Y., Liu, S., Xu, Y., Siddhrau, I. K., Zhou, S., Guo, Z., & Chao, H. J. (2022). SDNShield: NFV-Based Defense Framework Against DDoS Attacks on SDN Control Plane. IEEE/ACM Transactions on Networking, 30(1), 1–17. https://doi.org/10.1109/TNET.2021.3105187

Chen, S., Zhang, L., & Li, H. (2021). Deep learning for DDoS attack detection in 5G smart home environments. Journal of Information Security and Applications, 56, 102644. https://doi.org/10.1016/j.jisa.2021.102644

Cherian, M., & Varma, S. L. (2023). Secure SDN–IoT Framework for DDoS Attack Detection Using Deep Learning and Counter Based Approach. Journal of Network and Systems Management, 31(3). https://doi.org/10.1007/s10922-023-09749-w

Dai, Y., Huang, T., & Wang, S. (2024). DAmpADF: A framework for DNS amplification attack defense based on Bloom filters and NAmpKeeper. Computers and Security, 139. https://doi.org/10.1016/j.cose.2024.103718

Doriguzzi-Corin, R., & Siracusa, D. (2024). FLAD: Adaptive Federated Learning for DDoS attack detection. Computers and Security, 137. https://doi.org/10.1016/j.cose.2023.103597

El Kamel, A. (2024). Using FlowVisor and evolutionary algorithms to improve the switch migration in SDN. Journal of Network and Computer Applications, 222. https://doi.org/10.1016/j.jnca.2023.103807

El Kamel, A., Eltaief, H., & Youssef, H. (2022). On-the-fly (D)DoS attack mitigation in SDN using Deep Neural Network-based rate limiting. Computer Communications, 182, 153–169. https://doi.org/10.1016/j.comcom.2021.11.003

Ezeh, D., & de Oliveira, J. (2023). An SDN controller-based framework for anomaly detection using a GAN ensemble algorithm. Infocommunications Journal, 15(2), 29–36. https://doi.org/10.36244/ICJ.2023.2.5

Fadel, M. M., El-Ghamrawy, S. M., Ali-Eldin, A. M. T., Hassan, M. K., & El-Desoky, A. I. (2022). HDLIDP: A Hybrid Deep Learning Intrusion Detection and Prevention Framework. Computers, Materials and Continua, 73(2), 2293–2312. https://doi.org/10.32604/cmc.2022.028287

Febro, A., Xiao, H., Spring, J., & Christianson, B. (2022). Synchronizing DDoS defense at network edge with P4, SDN, and Blockchain. Computer Networks, 216. https://doi.org/10.1016/j.comnet.2022.109267

Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., Haunschild, D., Parlikad, A. K., Cetinkaya, O., Lutfiyya, H., Stankovski, V., Li, R., Ding, Y., Qadir, J., Abraham, A., Ghosh, S. K., Song, H. H., Sakellariou, R., Rana, O., … Buyya, R. (2024). Modern computing: Vision and challenges. Telematics and Informatics Reports, 13, 100116. https://doi.org/10.1016/j.teler.2024.100116

Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K.-K. R., & Iqbal, J. (2020). A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. IEEE Access, 8, 53972–53983. https://doi.org/10.1109/ACCESS.2020.2976908

Hasan, M. K., Abdulkadir, R. A., Islam, S., Gadekallu, T. R., & Safie, N. (2024). A review on machine learning techniques for secured cyber-physical systems in smart grid networks. Energy Reports, 11, 1268–1290. https://doi.org/10.1016/j.egyr.2023.12.040

Houda, Z. A. E., Hafid, A. S., & Khoukhi, L. (2023). MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain. IEEE Transactions on Network Science and Engineering, 10(4), 1985–2001. https://doi.org/10.1109/TNSE.2023.3237367

Huda, N. U., Ahmed, I., Adnan, M., Ali, M., & Naeem, F. (2024). Experts and intelligent systems for smart homes' Transformation to Sustainable Smart Cities: A comprehensive review. In Expert Systems with Applications (Vol. 238). Elsevier Ltd. https://doi.org/10.1016/j.eswa.2023.122380

Indrason, N., & Saha, G. (2024). Exploring Blockchain-driven security in SDN-based IoT networks. Journal of Network and Computer Applications, (Vol. 224), 103838. https://doi.org/10.1016/j.jnca.2024.103838

Iranmanesh, A., & Reza Naji, H. (2021). A protocol for cluster confirmations of SDN controllers against DDoS attacks. Computers and Electrical Engineering, 93. https://doi.org/10.1016/j.compeleceng.2021.107265

Jeba Praba, J., & Sridaran, R. (2023). LCDT-M: Log-Cluster DDoS Tree Mitigation Framework Using SDN in the Cloud Environment. International Journal of Computer Network and Information Security, 15(2), 62–72. https://doi.org/10.5815/ijcnis.2023.02.05

Kadri, M. R., Abdelli, A., Ben Othman, J., & Mokdad, L. (2024). Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments. In Internet of Things (Netherlands) (Vol. 25). Elsevier B.V. https://doi.org/10.1016/j.iot.2023.101021

Kaur, S., Kumar, K., Aggarwal, N., & Singh, G. (2021). A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions. In Computers and Security (Vol. 110). Elsevier Ltd. https://doi.org/10.1016/j.cose.2021.102423

Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023a). FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks. IEEE Access, 11, 28934–28954. https://doi.org/10.1109/ACCESS.2023.3260256

Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023b). P4-HLDMC: A Novel Framework for DDoS and ARP Attack Detection and Mitigation in SD-IoT Networks Using Machine Learning, Stateful P4, and Distributed Multi-Controller Architecture. Mathematics, 11(16), 3552. https://doi.org/10.3390/math11163552

Kim, J., Seo, M., Lee, S., Nam, J., Yegneswaran, V., Porras, P., Gu, G., & Shin, S. (2024). Enhancing security in SDN: Systematizing attacks and defenses from a penetration perspective. In Computer Networks (Vol. 241). Elsevier B.V. https://doi.org/10.1016/j.comnet.2024.110203

Krishnan, P., Duttagupta, S., & Achuthan, K. (2020). SDN/NFV security framework for fog-to-things computing infrastructure. Software - Practice and Experience, 50(5), 757–800. https://doi.org/10.1002/spe.2761

Lee, A. Y. P., Wang, M. I. C., Hung, C. H., & Wen, C. H. P. (2024). PS-IPS: Deploying Intrusion Prevention System with machine learning on programmable switch. Future Generation Computer Systems, 152, 333–342. https://doi.org/10.1016/j.future.2023.11.011

Liu, Y., Zhi, T., Shen, M., Wang, L., Li, Y., & Wan, M. (2022). Software-defined DDoS detection with information entropy analysis and optimized deep learning. Future Generation Computer Systems, 129, 99–114. https://doi.org/10.1016/j.future.2021.11.009

Macas, M., Wu, C., & Fuertes, W. (2024). Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. In Expert Systems with Applications (Vol. 238). Elsevier Ltd. https://doi.org/10.1016/j.eswa.2023.122223

Mall, R., Abhishek, K., Manimurugan, S., Shankar, A., & Kumar, A. (2023). Stacking ensemble approach for DDoS attack detection in software-defined cyber–physical systems. Computers and Electrical Engineering, 107. https://doi.org/10.1016/j.compeleceng.2023.108635

Mehra, A., & Badotra, S. (2022). A Novel Framework for Prevention against DDoS Attacks using Software Defined-machine Learning Model. International Journal of Performability Engineering, 18(8), 580–588. https://doi.org/10.23940/ijpe.22.08.p6.580588

Murtuza, S., & Asawa, K. (2024). Early prevention and mitigation of link flooding attacks in software defined networks. Journal of Network and Computer Applications, 103832. https://doi.org/10.1016/j.jnca.2024.103832

Neto, E. C. P., Dadkhah, S., Sadeghi, S., Molyneaux, H., & Ghorbani, A. A. (2024). A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective. In Computer Communications (Vol. 213, pp. 61–77). Elsevier B.V. https://doi.org/10.1016/j.comcom.2023.11.002

Nurwarsito, H., & Nadhif, M. F. (2021). DDoS Attack Early Detection and Mitigation System on SDN using Random Forest Algorithm and Ryu Framework. Proceedings of the 8th International Conference on Computer and Communication Engineering, ICCCE 2021, 178–183. https://doi.org/10.1109/ICCCE50029.2021.9467167

Oyucu, S., Polat, O., Türkoğlu, M., Polat, H., Aksöz, A., & Ağdaş, M. T. (2024). Ensemble Learning Framework for DDoS Detection in SDN-Based SCADA Systems. Sensors, 24(1). https://doi.org/10.3390/s24010155

Pascoal, T. A., Fonseca, I. E., & Nigam, V. (2020). Slow denial-of-service attacks on software defined networks. Computer Networks, 173. https://doi.org/10.1016/j.comnet.2020.107223

Pasha, M. J., Rao, K. P., MallaReddy, A., & Bande, V. (2023). LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments. Measurement: Sensors, 28. https://doi.org/10.1016/j.measen.2023.100828

Priyadarshini, R., & Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University - Computer and Information Sciences, 34(3), 825–831. https://doi.org/10.1016/j.jksuci.2019.04.010

Priyadarshini, R., Kumar Barik, R., & Dubey, H. (2020). Fog-SDN: A light mitigation scheme for DDoS attack in fog computing framework. International Journal of Communication Systems, 33(9). https://doi.org/10.1002/dac.4389

Pisal, N., Abdul-Rahman, S., Hanafiah, M., & Kamarudin, S. (2022). Prediction Of Life Expectancy For Asian Population Using Machine Learning Algorithms. *Malaysian Journal Of Computing, 7*(2), 1150-1161. doi:10.24191/mjoc.v7i2.18218.

Revathi, M., Ramalingam, V. V., & Amutha, B. (2022). A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework. Wireless Personal Communications, 127(3), 2417–2441. https://doi.org/10.1007/s11277-021-09071-1

Ribeiro, M. A., Pereira Fonseca, M. S., & de Santi, J. (2023). Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks. Computers and Security, 134. https://doi.org/10.1016/j.cose.2023.103462

Riyad, A. M. (2021a). A ddos defence framework in software defined network using ensemble classifier with rough set theory based feature selection. International Journal of Advanced Technology and Engineering Exploration, 8(82), 1120–1135. https://doi.org/10.19101/IJATEE.2021.874477

Riyad, A. M. (2021b). A ddos defence framework in software defined network using ensemble classifier with rough set theory based feature selection. International Journal of Advanced Technology and Engineering Exploration, 8(82), 1120–1135. https://doi.org/10.19101/IJATEE.2021.874477

Sahay, R., Blanc, G., Zhang, Z., & Debar, H. (2017). ArOMA: An SDN based autonomic DDoS mitigation framework. Computers and Security, 70, 482–499. https://doi.org/10.1016/j.cose.2017.07.008

Saied, M., Guirguis, S., & Madbouly, M. (2024). Review of artificial intelligence for enhancing intrusion detection in the internet of things. In Engineering Applications of Artificial Intelligence (Vol. 127). Elsevier Ltd. https://doi.org/10.1016/j.engappai.2023.107231

Salim, M. M., Azzaoui, A. El, Deng, X., & Park, J. H. (2024). FL-CTIF: A federated learning based CTI framework based on information fusion for secure IIoT. Information Fusion, 102. https://doi.org/10.1016/j.inffus.2023.102074

Sangodoyin, A., Mohammed, B., Sibusiso, M., Awan, I., & Disso, J. P. (2019). A framework for distributed denial of service attack detection and reactive countermeasure in software defined network. Proceedings - 2019 International Conference on Future Internet of Things and Cloud, FiCloud 2019, 80–87. https://doi.org/10.1109/FiCloud.2019.00019

Shirsath, V. A., Chandane, M. M., Lal, C., & Conti, M. (2024). SPARQ: SYN Protection using Acyclic Redundancy check and Quartile range on P4 switches. Computer Communications, 216, 283–294. https://doi.org/10.1016/j.comcom.2023.12.027

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

Singh, M. P., & Bhandari, A. (2020). New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. In Computer Communications (Vol. 154, pp. 509–527). Elsevier B.V. https://doi.org/10.1016/j.comcom.2020.02.085

Snehi, M., Bhandari, A., & Verma, J. (2024). Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems. Computers and Security, 139. https://doi.org/10.1016/j.cose.2024.103702

Sousa, B., & Gonçalves, C. (2024). FedAAA-SDN: Federated Authentication, Authorization and Accounting in SDN controllers. Computer Networks, 239. https://doi.org/10.1016/j.comnet.2023.110130

Tan, L., Pan, Y., Wu, J., Zhou, J., Jiang, H., & Deng, Y. (2020). A New Framework for DDoS Attack Detection and Defense in SDN Environment. IEEE Access, 8, 161908–161919. https://doi.org/10.1109/ACCESS.2020.3021435

Uddin, R., Kumar, S. A. P., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. In Ad Hoc Networks (Vol. 152). Elsevier B.V. https://doi.org/10.1016/j.adhoc.2023.103322

Varghese, J. E., & Muniyal, B. (2021a). An Efficient IDS Framework for DDoS Attacks in SDN Environment. IEEE Access, 9, 69680–69699. https://doi.org/10.1109/ACCESS.2021.3078065

Varghese, J. E., & Muniyal, B. (2021b). An Efficient IDS Framework for DDoS Attacks in SDN Environment. IEEE Access, 9, 69680–69699. https://doi.org/10.1109/ACCESS.2021.3078065

Wabi, A. A., Idris, I., Olaniyi, O. M., & Ojeniyi, J. A. (2023). DDOS ATTACK DETECTION IN SDN: Method of attacks, Detection techniques, Challenges and Research Gaps. Computers & Security, 103652. https://doi.org/10.1016/j.cose.2023.103652

Wang, W., Yi, P., Jiang, J., Zhang, P., & Chen, X. (2024). Transformer-based framework for alert aggregation and attack prediction in a multi-stage attack. Computers and Security, 136. https://doi.org/10.1016/j.cose.2023.103533

Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Carrera, D. F. (2022). A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning. Journal of Network and Computer Applications, 205. https://doi.org/10.1016/j.jnca.2022.103444

Zhang, X., Zhang, C., Zhong, Z., & Ye, P. (2021). An Intelligent SDN DDoS Detection Framework. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST: Vol. 406 LNICST. https://doi.org/10.1007/978-3-030-92635-9_20

Zhang, Y., Liu, T., & Wang, H. (2022). DDoS defense mechanisms in IoT: A survey. Computer Networks, 199, 108408. https://doi.org/10.1016/j.comnet.2022.108408

Zhou, H., Zheng, Y., Jia, X., & Shu, J. (2023). Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN. Computer Networks, 225. https://doi.org/10.1016/j.comnet.2023.109642

Zhou, Y., Cheng, G., & Yu, S. (2021). An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks. IEEE Transactions on Information Forensics and Security, 16, 5366–5380. https://doi.org/10.1109/TIFS.2021.3127009

Zormati, M. A., Lakhlef, H., & Ouni, S. (2024). Review and analysis of recent advances in intelligent network softwarization for the Internet of Things. Computer Networks, 110215. https://doi.org/10.1016/j.comnet.2024.110215