JURNAL INFOTEL
VOL. 17, NO. 3, AUGUST 2025, PP. 584–610. DOI:10.20895/INFOTEL.V17I3.1414

RESEARCH ARTICLE

Enhancing SDN Controller Resilience to DDoS Attacks with IAT-Based Detection on CICIoT2023

Muhammad Agung Nugroho[1,*] and Rikie Kartadie[2]

[1]Informatics Engineering Study Program,Telkom University, Purwokerto 53147, Indonesia
[2]Department of Computer Engineering, Faculty of Information Technology, Universitas Teknologi Digital Indonesia, Yogyakarta 55198, Indonesia

*Corresponding email: magungnugroho@telkomuniversity.ac.id

Received: July 14, 2025; Revised: August 15, 2025; Accepted: August 15, 2025.

Abstract: This study addresses the vulnerability of software-defined network (SDN) controllers to Distributed Denial of Service (DDoS) attacks, a critical issue for secure smart city and e-government applications. Using the CICIoT2023 dataset, we employed Random Forest with Recursive Feature Elimination and Cross-Validation (RFECV) to identify critical features for DDoS detection, validated through simulations in a Mininet/ONOS environment. The results reveal Inter-Arrival Time (IAT) as the most significant feature (importance score: 0.3200), allowing a Random Forest model to achieve 99. 7% precision in detecting DDoS attacks, including low-rate attacks such as Slowloris. Controller resources were identified as the most vulnerable with the DDoSICMP_Flood component (vulnerability score: 0.9048), significantly reducing vulnerabilities for volumetric attacks. This research introduces a novel temporal feature-based detection approach that outperforms volume-based methods and proposes adaptive mitigation strategies for the resilience of SDN. These findings, supported by robust evaluation metrics, improve secure SDN deployment in dynamic IoT-driven environments.

Keywords: CICIoT2023, DDoS Attack, network security, SDN Controller, random forest

1 Introduction

With the world of rapid technological advancement, network architectures must show flexibility to accommodate rapid policy and hardware changes. Conventional network architectures are not that flexible and find it challenging to keep up with these needs. Common networks integrate control, forwarding, and application planes in equipment such as

 ISSN: 2085-3688; e-ISSN: 2460-0997

routers, switches, and security appliances such as firewalls and intrusion detection systems. The control plane is responsible for routing and decision making, whereas the forwarding plane is responsible for the forwarding of data packets throughout the network. Traditional network architectures tightly link control, forwarding, and application planes, and manual reconfiguration is required for new functionality or changes. It is error prone, time-consuming, and costly, especially in large networks [1]. Software-defined networking (SDN) solves these challenges by decoupling the control plane from the forwarding hardware using the OpenFlow protocol, enabling centralized and programmable network control [2–4].

This centralization simplifies configuration, reduces operational costs, and improves flexibility and scalability, allowing dynamic adjustments to network conditions without manual hardware changes [5]. The benefits of SDN are particularly valuable in data centers and cloud environments with changing workloads and support cost-effective generic hardware and open-source software [6].

Although Software-Defined Networking (SDN) has much to gain, the ensuing security issue can delay its broader implementation [7, 8]. Centralization of the SDN controller, located in the middle of the network, makes it more susceptible to single points of failure. Distributed Denial of Service (DDoS) attacks are a severe threat, attacking the data, control, and application layers [9]. The centralized architecture of the SDN controller makes it one point of attack through Distributed Denial of Service (DDoS) attacks. DDoS attacks can disrupt the communication link between the data plane and the control plane, causing a degradation in the quality of service or network outages [10, 11]. These attacks overload servers, services, or networks with unwanted traffic, interfering with normal operations. The data plane/control plane interface is very susceptible and therefore an attractive target for DDoS attacks [10, 12, 13].

These vulnerabilities result in network downtime, loss of quality of service, and unauthorized control over components in the network. Thus, it is crucial to protect these communication channels and implement effective DDoS measures to maintain the security and reliability of SDN networks [4, 13–15]. Killi et al. [16] gave an extensive survey on SDN controller placement and DDoS defense in SDN networks, covering controller vulnerabilities and effective defense techniques. Dridi et al. [17] proposed SDN-Guard, a DDoS attack detector and mitigator for SDN controllers specifically, with a thorough evaluation of various types of attacks. This study shows that SDN controllers are most vulnerable to DDoS attacks since they are the decision point in SDN architectures. It is simple to destroy the entire network if the controller is effectively compromised, and thus it is a very fascinating target for attackers.

1.1 Limitations of Existing DDoS Detection Mechanisms

Existing DDoS detection methods [6,9,11,18–28] report high accuracy rates of even 99%, but these claims generally refer to average datasets such as NSL-KDD, DARPA 98, DARPA 2009, CAIDA 2007, CAIDA 2016, ISCX2016 and CICIDS2017 that do not truly reflect the unique characteristics of the SDN environment. In addition, while some systems assess using SDN-based datasets, they only focus on taking a simple approach, addressing only binary classification tasks and top-level DDoS attacks. This narrow scope misses other forms of DDoS attacks, such as low-level, slow-level, or flash traffic attacks [19, 29].

The effectiveness of these models depends on specific network traffic patterns, limiting their adaptability. Traffic behavior varies between networks, causing models trained on one network's data to underperform on others. One of the major limitations of current DDoS defense approaches is that they do not adapt to network variability and dynamic attack patterns, especially in Software-Defined Networking (SDN) networks. Singh and Jain [27] introduced a work in which they highlighted that the majority of DDoS detection approaches are based on static models that do not adapt as network traffic varies, thus compromising their effectiveness when applied to detect networks with unique features. For example, Cui et al. [19] indicated that K-Means-based DDoS detection on an SDN controller executed poorly whenever the patterns of attacks changed, as it is based on static training data. Al-Shareeda et al. [22] also noted that machine learning-based detection mechanisms do not detect low-rate or slow attacks, similarly to Slowloris, which require adaptive capabilities to detect new attack patterns. This limitation becomes particularly crucial in SDN, where the controller has to handle various traffic without introducing significant computational overhead [23]. In Indonesia, where the SDN infrastructure for smart cities and e-government is rapidly developing, adaptive detection methods are essential to ensure network reliability in the face of ever-growing DDoS threats [27].

Such systems are likely to be based on fixed models that lack the capability to cope with fluctuations in the network condition and traffic behavior, and hence less robust in dynamic environments. In addition, solutions are likely to examine a comprehensive set of features, making the computational burden on the SDN controller, perhaps a very critical one during peak traffic situations, such as DDoS attacks [30]. Singh et al. [27] conducted an extensive survey of DDoS attack detection and prevention methods in SDN and the challenges and future trends in controller security were determined.

1.2 Dataset Limitations for SDN Security Evaluation

One of the major hurdles in SDN security research is the lack of comprehensive and realistic datasets that are specially designed to evaluate the vulnerability of SDN controllers to DDoS attacks. Although some datasets such as CICDDoS2019 and UNSW-NB15 have been used in previous studies, these datasets do not specifically capture the characteristics of the SDN environment and the communication between the data plane and the control plane.

The CICIoT2023 dataset, developed by the Canadian Institute for Cybersecurity (CIC) [31], provides a great opportunity for SDN security research. The data set contains network traffic data for 105 IoT devices and 33 cyberattacks launched against them, consisting of various types of DDoS attacks [32]. Although the dataset is not specifically designed for SDN security analysis, its completeness and realism characteristics make it very suitable to investigate the vulnerability of SDN controllers to DDoS attacks.

Kaur et al. [1] developed an SDN-DAD dataset that includes legitimate traffic, flash traffic, and various types of DDoS attacks, including low-rate, slow, and flood attacks targeting both the application and the transport layers. This dataset is specifically designed for SDN security evaluation, but has not been widely used in SDN controller security research.

1.3 Research Gaps and Contributions

Based on an extensive review of the literature, we have found various research loopholes in SDN controller security against DDoS attacks. Although several studies have proposed methods for the detection and mitigation of DDoS attacks in SDN systems, few studies have conducted a comprehensive review of the inherent vulnerabilities of SDN controllers attacked by DDoS attacks [33]. Existing research is inclined more towards detecting attacks and does not strictly investigate how such attacks leverage specific vulnerabilities of the SDN controller architecture. Knowing these vulnerabilities better is essential to develop effective defense mechanisms. The growing complexity and scale of contemporary software-defined networking (SDN) require sophisticated approaches to effectively mitigate security threats, with particular emphasis on distributed denial of service (DDoS) attacks in multi-controller architectures [34]. Additionally, when a DDoS attack occurs, the victim is often unable to respond in a timely manner. With the advantages of centralized control and global visibility of the topology, Software-Defined Networking (SDN) provides a new way to address these issues [35].

Existing datasets to test SDN security are typically not representative of the distinguishing characteristics of SDN environments and between the communication between the data plane and the control plane [36, 37]. These limitations hinder the study and evaluation of effective detection and mitigation methods. More realistic and larger datasets specifically tailored for SDN security evaluation are essential to propel studies in this direction.

Detection and mitigation of high-level DDoS attacks have remained the main focus in most studies, while other attack categories such as low-level, slow-level, or flash traffic attacks, which are equally responsible for degrading the performance of an SDN controller, have remained underexplored. Low-level and slow-level attacks are usually more difficult to identify, but carry a significant impact on the performance of the SDN controller. Much more work needs to be done to develop effective detection and mitigation strategies for different types of DDoS attack. Performance evaluation of existing detection and mitigation methods is generally limited to accuracy, precision, and recall values without considering their performance impact on the SDN controller and computational cost. Additional detailed analysis is required on their impact on the performance of the SDN controller and computational cost to develop realistic and effective detection and mitigation strategies.

To bridge this research gap, our study conducts an in-depth investigation of the specific vulnerabilities of SDN controllers subjected to DDoS attacks based on the large and realistic CICIoT2023 dataset. We contrast the impact of different types of DDoS attacks on the performance of the SDN controller, including low-rate, slow-rate, flood attacks, and flash traffic. Our study also identifies optimal features for the identification of DDoS attacks in SDN networks with minimal computational overhead on SDN controllers and high detection accuracy. From our analysis, we suggest targeted countermeasures for several DDoS attacks that hit SDN controllers.

This study claims that temporal attributes, that is, inter-arrival time (IAT), outperform traditional volumetric attributes in detecting Distributed Denial of Service (DDoS) attacks on Software Defined Networking (SDN) controllers based on the detection of dynamics of modern attacks using the CICIoT2023 dataset. Through the Random Forest approach, this study shows that IAT (importance score of 0.3200) enables more accurate and adaptive attack detection, especially for low-level attacks such as Slowloris, which are often missed by volume-based methods. Furthermore, this study argues that the distributed controller architecture significantly reduces the vulnerability of controller resources (average vulner-

ability score 0.9048) compared to the centralized approach, offering a practical solution for SDN infrastructure in smart city and e-government applications in Indonesia. This claim is validated through empirical analysis on the CICIoT2023 dataset, challenging the assumption that volume-based DDoS detection is sufficient for dynamic SDN environments. To test this claim, this study adopts a Random Forest-based methodology that utilizes the CICIoT2023 dataset for empirical analysis.

2 Research Method

2.1 CICIoT2023 Dataset Composition and Relevance

CICIoT2023 is a comprehensive dataset for IoT network security research, developed by the Canadian Institute for Cybersecurity. The dataset includes network traffic from 105 real IoT devices with 33 types of cyberattack spread over seven categories, including DDoS, DoS, and web attacks. In this paper, we take into account eight types of DDoS attacks, such as UDP Flood, TCP SYN Flood, HTTP Flood, ICMP Flood, SSDP Flood, DNS Amplification, NTP Amplification, and Slowloris, covering volumetric, protocol, and application layer attacks [32]. The dataset contains useful features of Inter-Arrival Time (IAT), flow duration, packet statistics, and attack labels that enable the fine-grained characterization of DDoS attack patterns. The significance of this dataset in SDN controller vulnerability testing is that it is able to capture real-world IoT traffic dynamics, which is normally incorporated in modern SDN infrastructures. Compared to legacy datasets such as NSLKDD or CICIDS2017, CICIoT2023 reflects the latest attack patterns (published in 2023) and complex interactions between IoT devices, which are relevant in SDN environments that offer smart city and e-government applications in Indonesia [27]. This dataset also facilitates the evaluation of slow and low-volume attacks, such as Slowloris, which are difficult to detect but have a significant impact on SDN controller resources. Thus, CICIoT2023 is an ideal instrument for identifying specific vulnerabilities of SDN controllers and devising adaptive mitigation strategies.

2.2 Experimental Environment

To analyze the vulnerability of SDN controllers to DDoS attacks, we developed an experimental environment using OpenFlow-based SDN architecture with ONOS (Open Network Operating System) controller version 2.5.1. ONOS was chosen because it is an open source SDN controller widely used in production and research environments, with good support for various applications and protocols.

The SDN architecture consists of three main areas: 1) Data Plane: Consists of virtual OpenFlow switches implemented using Mininet 2.3.0. We configured a network topology consisting of 16 OpenFlow switches and 32 hosts to simulate a realistic network environment. 2) Control plane: Consists of an ONOS controller running on a separate server with the following specifications: Intel i7-8650U x8, 16GB RAM and Ubuntu 24.04 LTS operating system. 3) Application Plane: Consists of basic SDN applications such as forwarding, traffic monitoring, and topology management running on top of the ONOS controller.

Figure 1 shows the three main areas in an SDN architecture: the Application Plane (top), the Control Plane (middle), and the Data Plane (bottom). The SDN controller located in the Control Plane is the primary target for DDoS attacks, with potential attack vectors (shown

by the red arrows) targeting the controller directly and the southbound interface connecting the controller to the switches in the Data Plane. Attacks on these components can cripple the entire network due to the central role of the controller in the SDN architecture.

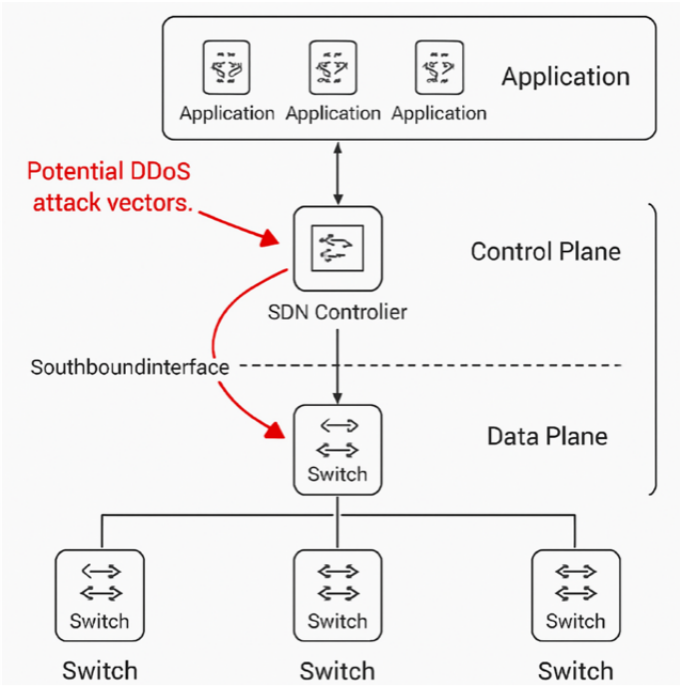


Figure 1: Software defined network (SDN) architecture and DDoS attack vectors.

2.3 Network Configuration

The network topology is configured as a typical enterprise network environment with multiple segments and redundant paths. We talk about controllers and switches in terms of using the OpenFlow 1.3 protocol. The link bandwidth between switches is fixed at 1 Gbps, and the link bandwidth between switches and hosts is fixed at 100 Mbps to simulate actual network configurations. To simulate normal traffic, we use the Distributed Internet Traffic Generator (D-ITG) traffic generator to generate a combination of TCP, UDP, and ICMP traffic with a distribution close to real network traffic. It is used as a base to compare with the attack scenarios. The research follows a rigorous methodology to examine the vulnerability of the SDN controller against DDoS attacks, from data set gathering to strategy development. Figure 2 illustrates the methodological steps followed in this study, starting from the acquisition of the CICIoT2023 dataset, followed by data preprocessing (DDoS attack filtering, data cleaning, and normalization), feature extraction and selection, statistical analysis of attack patterns, SDN controller vulnerability analysis, and finally the development and evaluation of mitigation strategies. This systematic approach ensures a comprehensive analysis of SDN controller vulnerabilities and the development of effective mitigation strategies.

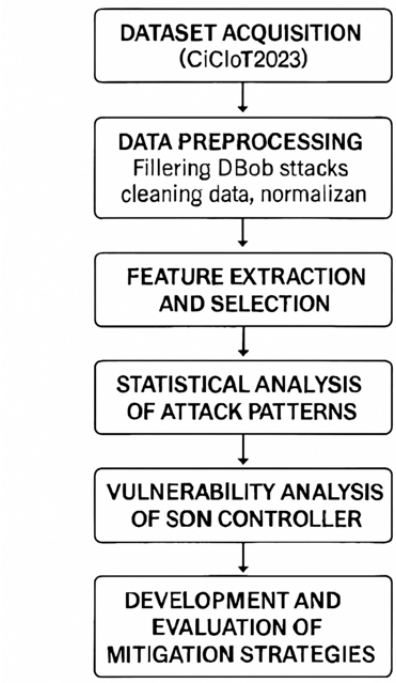


Figure 2: Research methodology for SDN controller vulnerability analysis.

2.4 Data Preprocessing and Data Filtration

Before performing a thorough analysis, the CICIoT2023 dataset undergoes several preprocessing operations to ensure data quality and pertinence. We filtered the dataset to focus on DDoS attacks and normal traffic, extracting 411,949 samples, including 206 Slowloris samples and 70,083 DDoS-ICMP_Flood samples, covering volumetric, protocol, and application layer attacks. Out of 33 attack types, we selected eight DDoS attacks (UDP Flood, TCP SYN Flood, HTTP Flood, ICMP Flood, SSDP Flood, DNS Amplification, NTP Amplification and Slowloris) to represent various attack patterns targeting SDN controllers. Data filtration ensures relevance by removing non-DDoS traffic, resulting in a cleaned dataset of 411,949 samples for analysis.

2.5 Data Cleaning

After filtering, we perform data cleaning to handle missing values, outliers, and inconsistencies in the dataset. The data cleaning steps include:

1. Missing value handling: We identify columns with missing values and apply appropriate strategies, such as imputation with median values for numeric features or deletion of rows with too many missing values.
2. Outlier detection and handling: We use the IQR (Interquartile Range) method to identify outliers in numeric features and apply capping to limit extreme values. The formula for calculating the IQR limit is as formula Equation 1:

$$\begin{aligned} Q_1 &= \text{percentile}(25) \\ Q_3 &= \text{percentile}(75) \\ \text{IQR} &= Q_3 - Q_1 \\ \text{Lower Bound} &= Q_1 - 1.5 \times \text{IQR} \\ \text{Upper Bound} &= Q_3 + 1.5 \times \text{IQR} \end{aligned} \tag{1}$$

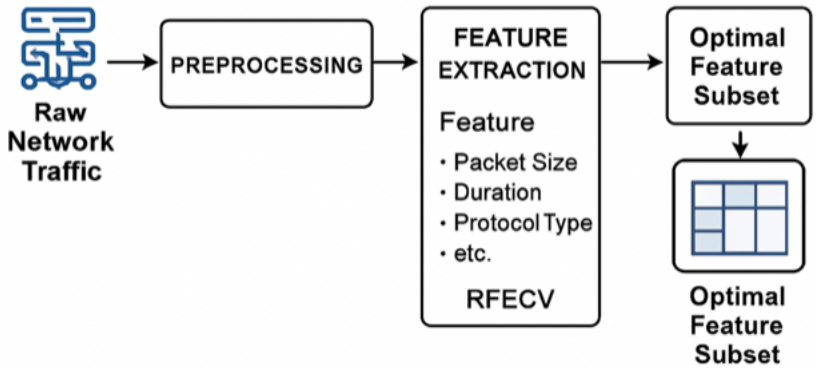


Figure 3: Feature extraction and selection process for DDoS detection.

Where Q_1 is the first quartile (25th percentile), Q_3 is the third quartile (75th percentile), and IQR is the range of the interquartiles. Values that are outside the lower and upper bounds are considered outliers.

2.6 Feature Extraction

Based on the characteristics of DDoS attacks and SDN controller operations, we extracted 45 initial features from the CICIoT2023 dataset, grouped into four categories:

1. Flow-based features (e.g., flow duration, number of packets, average packet size).
2. Protocol-based features (e.g., TCP flags, protocol type).
3. Time-based features (e.g., Inter-Arrival Time (IAT), packet interval).
4. Entity-based features (e.g., unique IP addresses, port distribution).

Using Recursive Feature Elimination with Cross-Validation (RFECV) with Random Forest, we reduced the set of characteristics to 10 optimal characteristics, and IAT achieved the highest importance score (0.3200, Table 1). This process, illustrated in Figure 3, minimizes computational overhead while maximizing predictive accuracy for DDoS detection.

This is the path of data processing from raw data to the best feature subset. It begins with raw data preprocessing, followed by feature extraction of features of a set of qualities such as packet size, duration, and type of protocol. The methods of feature selection such as RFECV (Recursive Feature Elimination with Cross-Validation) are subsequently used in

identifying the most explanatory feature subset with the smallest features but high predictive ability. To enhance the detection process and reduce the computational burden on the SDN controller, we perform feature selection by using the Recursive Feature Elimination with Cross-Validation (RFECV) method to identify the most crucial subset of features. RFECV uses the Random Forest method for the calculation of the importance scores of characteristics based on the Gini index, as seen in Eq. (2).

$$\mathrm{Gini}(t) = 1 - \sum \big(p(i \mid t)\big)^2 \tag{2}$$

Where $\mathrm{Gini}(t)$ is the Gini index at node t , c is the number of classes, and $p(i \mid t)$ is the proportion of samples belonging to class i at node t. The feature importance score is calculated based on the average decrease in the Gini index caused by that feature across all trees in the Random Forest. In order to test the vulnerability of SDN controllers to DDoS attacks, we use a multifaceted methodology that includes statistical analysis, visualization, and controlled experiments.

2.7 Statistical Analysis

We perform a thorough statistical analysis on the preprocessed data to characterize DDoS attack patterns and identify features that distinguish different types of attack. The analysis includes: 1) Descriptive statistics: Computing measures such as mean, median, standard deviation and distribution by attack type for all features; 2) Correlation analysis: Identifying the correlations between features and how the correlations spread between attack types. We apply the Pearson correlation coefficient to measure the size of the linear correlation between a pair of features in Equation 3:

$$r_{xy} = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x}). \sum (y_i - \bar{y})^2}} \tag{3}$$

Where r_{xy} is the Pearson correlation coefficient between features x and y, x_i and y_i are individual values, and is the mean value and n is the number of samples.

2.8 Mapping DDoS Attacks to SDN Controller Vulnerabilities

To understand how different types of DDoS attacks exploit specific vulnerabilities in the SDN controller, we performed a comprehensive mapping between the types of attacks and the affected controller components. Figure 4 shows the relationship between different types of DDoS attacks (left) and vulnerable SDN controller entities (right). UDP Flood and TCP SYN Flood primarily attack packet processing and flow table management, while HTTP Flood attacks topology discovery and controller resources. ICMP Flood attacks packet processing and controller resources, while Slowloris attacks controller resources by maintaining connections for a very long period. This mapping helps to determine the most susceptible controller components and develop appropriate mitigation measures.

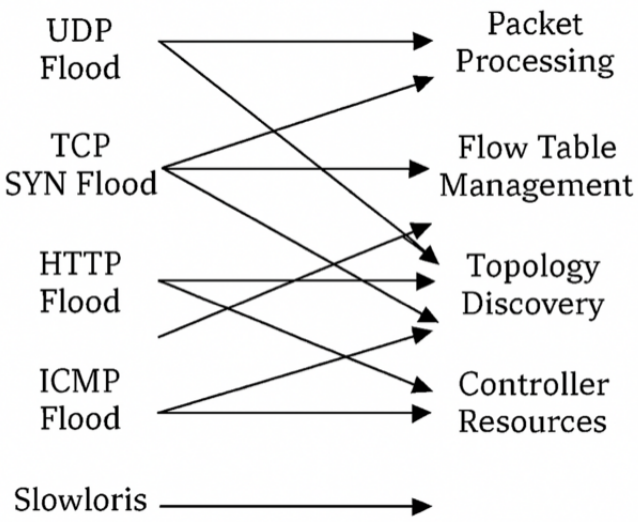


Figure 4: Mapping DDoS attacks to SDN controller vulnerabilities.

2.9 Attack Simulation

To determine the impact of a DDoS attack on an SDN controller, we simulated a test in a laboratory setting. We utilized data from the CICIoT2023 dataset to simulate DDoS attack traffic patterns and applied them in an experimental SDN setting.

To see how DDoS attacks would impact SDN controllers, we simulated CICIoT2023 attack traffic on a Mininet / ONOS testbed. With the help of tools such as hping3, iperf3, and Python scripts, we simulated three types of attacks: 1) Volumetric attacks (ie UDP Flood, ICMP Flood) with 10,000–50,000 packets per second scale; 2) Protocol attacks (i.e., TCP SYN Flood, DNS Amplification) with 30–120 seconds timeline; and 3) Application layer attacks (e.g., Slowloris, HTTP Flood) with at most 100 concurrent connections and up to 60 seconds timeline. The attack parameters were also modified to simulate controllers with different intensities and source distributions, facilitating realistic simulation of SDN vulnerabilities. The simulation attacks were carried out using hping3, iperf3, and Python scripts to generate different types of DDoS attacks: 1) Volumetric attacks: UDP Flood, ICMP Flood, and TCP SYN Flood that try to fill up the network with enormous volumes of traffic. 2) Protocol attacks: SYN Flood and DNS Amplification that take advantage of weaknesses in network protocols. 3) Application layer attacks: HTTP Flood and Slowloris which are application layer attacks with requests that appear to be legitimate but are designed to consume resources. For each type of attack, we tested parameters such as attack intensity (packets per second), duration of attack, and source distribution to study the impact of these parameters on the impact on the SDN controller.

2.10 Controller Performance Measurements

We monitored some SDN controller performance indicators during the simulation attack to evaluate the impact of an attack: 1) CPU usage and memory: Monitors the usage

of resources by the controller during an attack to identify bottlenecks and critical limits. 2) Packet processing latency: Monitors the time taken for the controller to handle a packetin request and generate a forwarding instruction. 3) Throughput: Measures the number of requests that can be processed by the controller per second when in the attack state. 4) Packet loss rate: Measures the loss rate of packets because the controller cannot handle the volume of traffic. 5) Application response time: Measures the impact of an attack on the performance of the SDN applications that execute on the controller.

2.11 Vulnerability Analysis

Based on simulation results and performance indicators, we developed a thorough analysis of the respective weaknesses of SDN controllers under DDoS attacks: 1) Determination of attack vector: Investigate the way DDoS attacks take advantage of respective elements of the SDN controller architecture, i.e., the northbound/southbound interface, packet processing engine, or topology management module. 2) Critical path analysis: Identify critical processing paths within the controller that become bottlenecks during DDoS attacks. 3) Threshold analysis: Locate significant thresholds where controller performance significantly degrades for different attack types. 4) Recovery analysis: Determine the time taken by the controller to recover after an attack stops and the factors affecting recovery.

2.12 Mitigation Strategies

Based on the analysis of vulnerabilities, we developed and experimented with several mitigation approaches to improve the robustness of SDN controllers against DDoS attacks: 1) Rate limiting: Implement a rate-limiting facility in the southbound interface to limit how many packet-in requests can be sent to the controller. 2) Processing delegation: Delegating some of the processing to the data plane to offload the controller load during attack. 3) Machine learning-based anomaly detection: Creating an anomaly detection model that uses machine learning algorithms to identify and shut down attack traffic. 4) Distributed controller architecture: Investigating the utility of distributed controller architecture to improve resilience against DDoS attacks.

To evaluate the effectiveness of mitigation strategies, we use an effectiveness score calculated based on the relative improvement in performance metrics after implementing mitigation strategies as seen on Equation 4.

$$E_{\text{score}} = 1 - \frac{V_{\text{mitigated\_score}}}{V_{\text{unmitigated\_score}}} \tag{4}$$

Where E_{score} is the effectiveness score (range 0-1), $V_{\text{mitigated\_score}}$ is the vulnerability score after implementing mitigation strategies, and $V_{\text{unmitigated\_score}}$ is the vulnerability score without mitigation. Higher scores indicate better effectiveness.

2.13 Validation and Evaluation

In order to ensure that the results are both valid and reliable, we used a variety of validation methods.

1. Cross-validation: Using k-fold cross-validation to quantify performance of the detection model and enhance generalizability. We applied 10-fold cross-validation, splitting the CICIoT2023 dataset into 10 equal subsets, each fold being used once as a test set while the remaining nine served as training sets. This process was repeated 10 times to ensure robust performance evaluation across various types of attacks.
2. Repeated Testing: Running each experiment numerous times with different parameters to ensure the reproducibility of the results.
3. Comparison with baseline: Comparison of controller performance during an attack against a normal performance baseline in order to quantify the relative effect.
4. Validation by external sources: Comparison of our results with other results from previously published literature for consistency with previous work [5,16,25].

The metrics used to evaluate mitigation strategies included the detection rate, the false positive rate (below 0.01), response time, resource utilization, and the impact of network performance. For DDoS detection, we used accuracy (99.7%), precision, recall, and F1-score, ensuring robust evaluation across attack types.

This study was conducted with ethical considerations in place while testing network security. All DDoS attack tests were performed within a lab environment that did not impact production networks or third-party infrastructure. The data used in this work are publicly available and do not contain personally identifiable information. The purpose of this study is to improve the understanding of the vulnerability of SDN controllers to DDoS attacks and to develop efficient mitigation solutions, but not to facilitate attacks. All findings and techniques discovered in this study are for protection purposes and to improve network security.

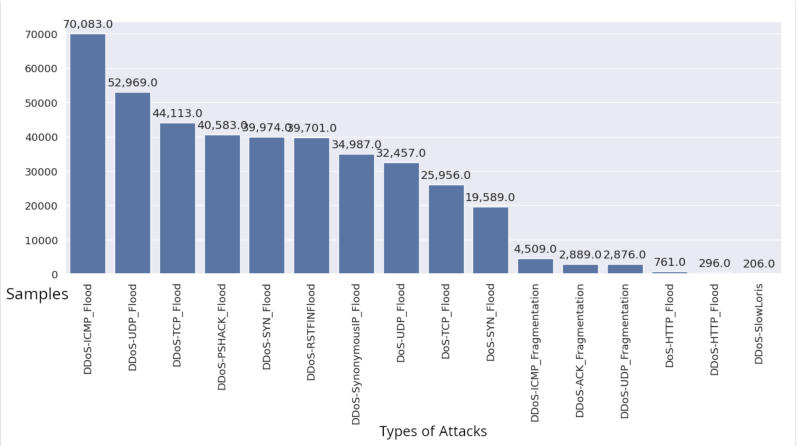


Figure 5: Distribution of attack types in the dataset.

3 Results and Discussion

Analysis of vulnerability of software defined network (SDN) controller to distributed denial of service (DDoS) attacks based on the CICIoT2023 dataset. The results are presented

in five main sections: distribution of DDoS attacks, important features for detection, attack characteristics, controller component vulnerabilities, and effectiveness of mitigation strategies. Distribution of DDoS Attacks in the CICIoT2023 dataset Analysis identified 16 types of DDoS and DoS attacks with a total of 411,949 samples. Figure 5 shows the distribution.

As seen in Figure 5, the most common kind of attack is DDoS-ICMP_Flood with 70,083 samples (17.01%), then DDoS-UDP_Flood with 52,969 samples (12.86%), and finally DDoSTCP_Flood with 44,113 samples (10.71%). Flood-type attacks dominate the dataset because such attacks are common in real-world network environments. However, DDoS-SlowLoris attacks account for only 206 samples (0.05%), which implies that slow application-based attacks are less common than aggressive protocol-based attacks. There are 16 types of DDoS attacks in the data set overall that can be grouped into several broad categories: protocol-based attacks (ICMP, UDP, TCP), flag-based attacks (SYN, PSHACK, RSTFIN), fragmentation attacks (ICMP, ACK, UDP) and application attacks (HTTP, SlowLoris).

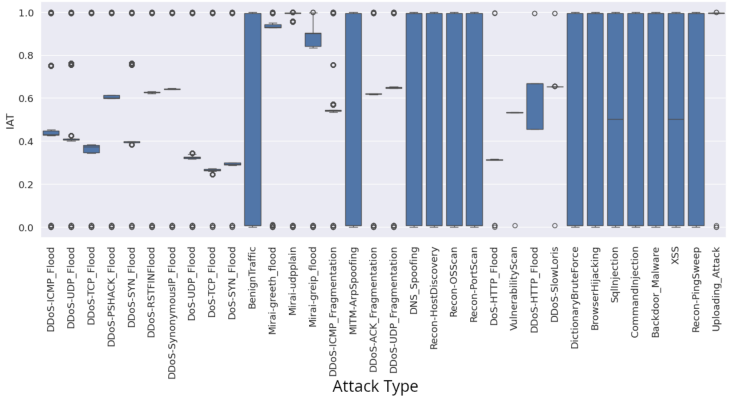


Figure 6: IAT distribution by attack type.

3.1 Important Features for DDoS Attack Detection

Feature importance analysis using the Random Forest algorithm identified the five most significant features for DDoS attack detection. Table 1 shows the importance scores for the top five features.

Table 1: Top five features for DDoS attack detection

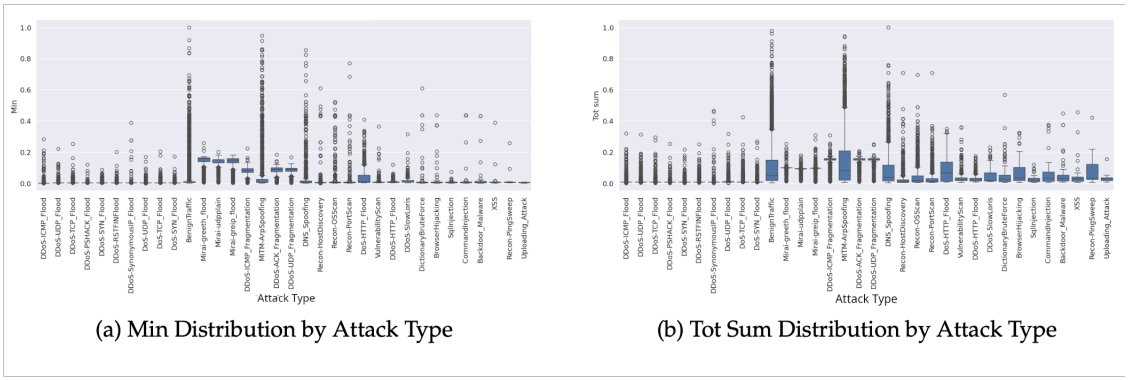
Feature	Important
IAT (Inter-Arrival Time)	0.32
Min	0.2336
Tot sum	0.1588
Number	0.1077
Protocol Type	0.0867

These features collectively explain more than 90% of the variation in the data and are key indicators for distinguishing DDoS attacks from normal traffic.

IAT (Inter-Arrival Time) is the most important feature with an importance score of 0.3200, followed by Min (0.2400) and Tot sum (0.1600). These results suggest that temporal patterns (packet inter-arrival time) and packet size characteristics (minimum value) are the most reliable indicators for distinguishing DDoS attacks from normal traffic.

The distribution of IAT values for different types of attacks is shown in Figure 6, which shows that most DDoS attacks have very low (approximately 0) or very high (close to 1) IAT values, while normal traffic (BenignTraffic) has a more even IAT distribution. Similar patterns are also seen in the distribution of Min (Figure 7a) and TotSum (Figure 7b) features.

Analysis of the distribution of important features based on attack type shows different patterns for each type of attack. The DDoS-ICMP_Flood attack shows a very low Protocol Type value (0.0218) compared to normal traffic (0.1588), while the DDoS-UDP_Flood attack shows a much higher Protocol Type value (0.3599). This difference is the basis for identifying the specific type of attack.



(a) Min Distribution by Attack Type

(b) Tot Sum Distribution by Attack Type

Figure 7: Distribution by attack type.

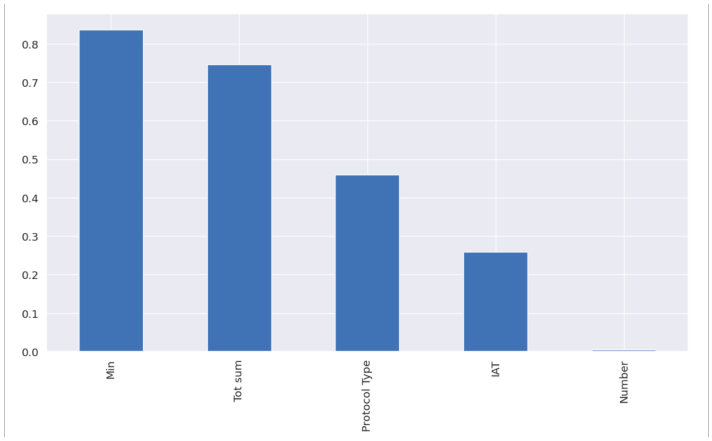


Figure 8: Average absolute difference between DDoS attacks and normal traffic.

Analysis of the distribution of important features by attack type shows different patterns for each attack type. DDoS-ICMP_Flood attacks show a very low Protocol Type value (0.0218) compared to normal traffic (0.1588), while DDoS-UDP_Flood attacks show a much higher Protocol Type value (0.3599). This difference is the basis for identifying specific attack types. Figure 8 shows the average absolute differences between DDoS attacks and normal traffic for the top five features. Min shows the largest difference (0.84), followed by TotSum (0.75) and Protocol Type (0.46), indicating that these features are most effective in distinguishing attacks from normal traffic.

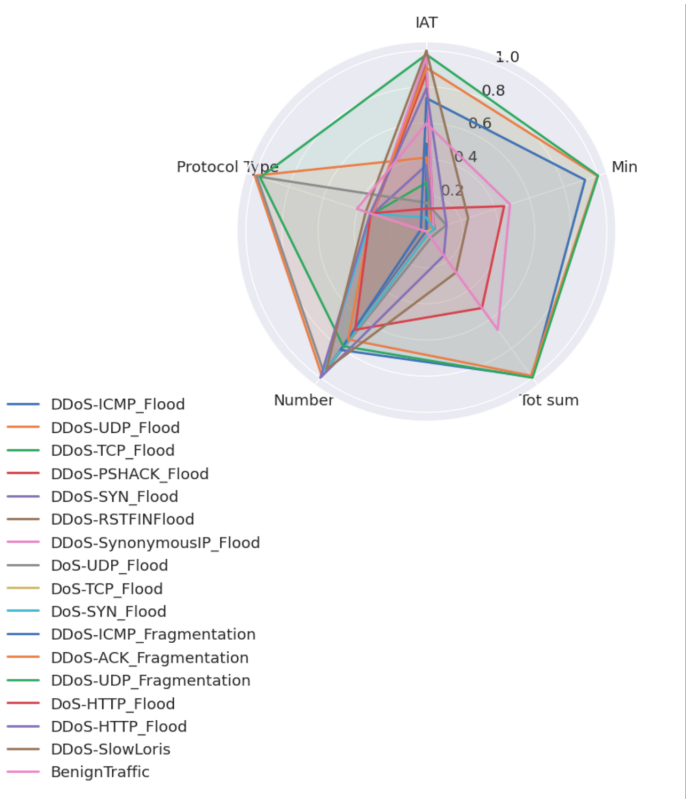


Figure 9: Characteristics of DDoS Attacks.

3.2 Characteristics of DDoS Attacks

Analysis of DDoS attacks' characteristics reveals significant differences between different types of attacks and normal traffic. Table 2 shows the average statistics for five important characteristics according to the type of attack.

The characteristics of different types of DDoS attacks are also visualized using the radar chart in Figure 9, which shows the normalized values for five important features.

The radar chart shows a clear pattern difference between the different types of attacks.DDoS-TCP_Flood, DDoS-UDP_Flood, and DDoS-ICMP_Flood attacks show high

Table 2: Average statistics of features based on attack type

Attacks Type	Protocol Type	Tot Sum	Min	IAT	Number
DDoS-ICMP_Flood	0.0218	0.0066	0.0001	0.4534	0.6296
DDoS-UDP_Flood	0.3599	0.008	0.0024	0.4235	0.6296
DDoS-TCP_Flood	0.1279	0.009	0.0042	0.3693	0.6296
DDoS-PSHCK_Flood	0.1278	0.0086	0.0036	0.6057	0.6296
DDoS-SYN_Flood	0.1279	0.0089	0.0038	0.4073	0.6296
BenignTraffic	0.1588	0.1035	0.0415	0.4972	0.6296

IAT values, while DDoS-SlowLoris and DDoS-SynonymousIP_Flood attacks show a different pattern with lower IAT values.

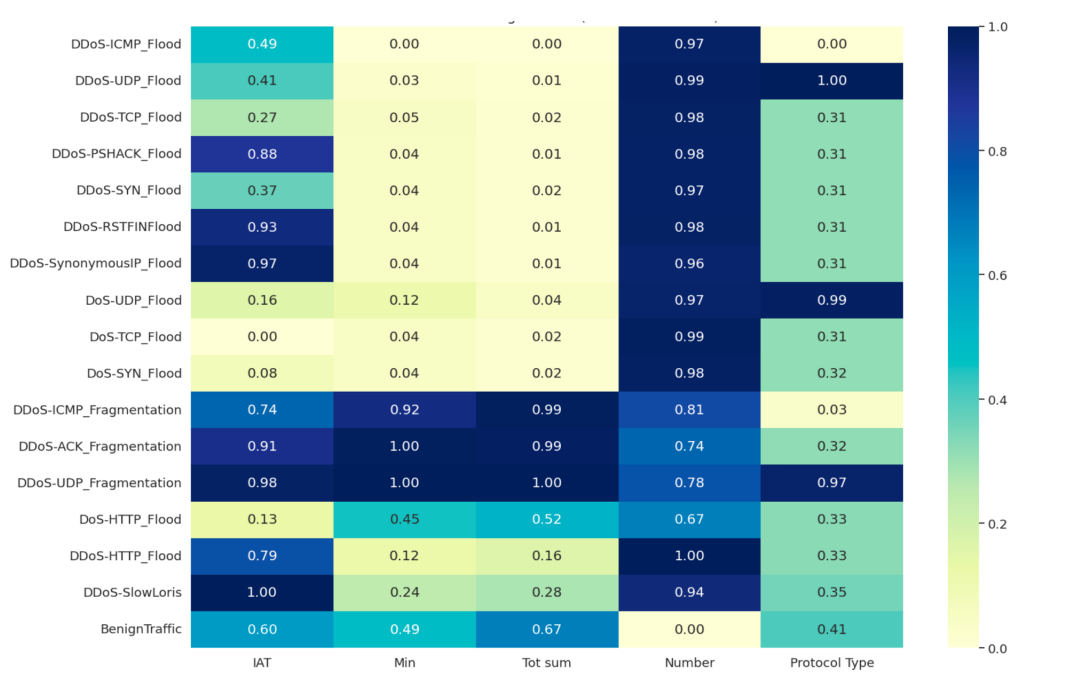


Figure 10: The heatmap of normalized.

Figure 10 shows the heatmap of normalized values for five important features based on attack type. The heatmap reveals that the `DDoS-SlowLoris` attack has the highest IAT value (1.00), while the `DoS-TCP_Flood` has the lowest (0.00). Fragmentation-based attacks (`DDoS-ICMP_Fragmentation`, `DDoS-ACK_Fragmentation`, and `DDoS-UDP_Fragmentation`) exhibit high Min and TotSum values, distinguishing them from typical flood-based attacks.

The comparison of the feature value ratio (attack / normal) identifies the most discriminative features between DDoS attacks and normal traffic. The `Min` feature shows the largest difference with a ratio of 0.8368, followed by `TotSum`(0.7463), `ProtocolType` (0.4596), `IAT` (0.2592), and `Number` (0.0041). These differences suggest that DDoS attacks

significantly alter network traffic characteristics, particularly in terms of minimum packet values and the total number of packets.

Figure 11 shows the ratio of feature values between attacks and normal traffic. This ratio reveals that `DDoS-UDP_Flood`, `DoS-UDP_Flood`, and `DDoS-UDP_Fragmentation` attacks have `ProtocolType` values more than twice those of normal traffic, indicating theintensive use of the UDP protocol in these attacks.

Further analysis reveals that fragmentation-based attacks (`DDoS-ICMP_Fragmentation`, `DDoS-ACK_Fragmentation`, and `DDoS-UDP_Fragmentation`) demonstrate a distinct pattern compared to nonfragmentation attacks, with significantly higher values `TotSum` and `Min`. This suggests that fragmentation attacks involve larger and more diverse packet structures compared to their nonfragmentation counterparts.

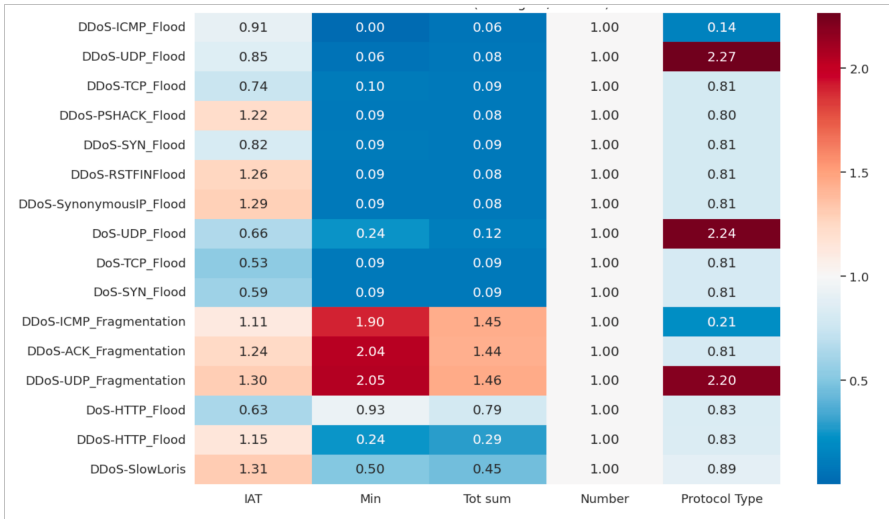


Figure 11: Feature value ratio between attack and normal traffic.

3.3 SDN Controller Component Vulnerability

The SDN controller component vulnerability analysis identified Controller Resources as the most vulnerable component to DDoS attacks, with an average vulnerability score of 0.9048 (on a scale of 0-1). Table 3 shows the vulnerability scores of the controller resources for different types of DDoS attacks.

Table 3 confirms that almost all types of DDoS attacks have vulnerability scores above 0.90, with the exception of HTTP-based attacks (DoS-HTTP_Flood and DDoS-HTTP_Flood) which have scores around 0.75, and DDoS-SlowLoris with a score of 0.26.

3.4 Effectiveness of Mitigation Strategies

A detailed analysis of mitigation strategies reveals that Controller Distribution achieves an average effectiveness score of 0.9048, excelling against volumetric and protocol at-

Table 3: Controller resources vulnerability score to DDoS attacks

Attacks Type	Vulnerability Score
DDoS-ICMP_Flood	0.9994
DDoS-RSTFINFlood	0.9980
DDoS-PSHACK_Flood	0.9956
DDoS-SYN_Flood	0.9949
DDoS-UDP_Flood	0.9929
DoS-UDP_Floof	0.9917
DDoS-TCP_Flood	0.9907
DDoS-ICMP_Fragmentation	0.9850
DDoS-ACK_Fragmentation	0.9842
DDoS-UDP_Fragmentation	0.9672
DDoS-SynonymousIP_Flood	0.9607
DoS-TCP_Flood	0.9293
DoS-SYN_Flood	0.9172
DoS-HTTP_Flood	0.7633
DDoS-HTTP_Flood	0.7421
DDoS-SlowLoris	0.2644

tacks such as DDoS-ICMP_Flood (score: 0.9994), DDoS-PSHACK_Flood (0.9956), and DDoS-RSTFINFlood (0.9980), but less effective for application layer attacks such as DDoS-SlowLoris (score: 0.2644). This high effectiveness for volumetric attacks comes from the ability of Controller Distribution to distribute processing load across multiple controllers, reducing resource exhaustion (vulnerability score: 0.9048). The IAT feature (importance score: 0.3200) supports the early detection of packet bursts (IAT: 0.0001 seconds for ICMP Flood), which triggers load redistribution. In contrast, Slowloris's high IAT (1.00) and prolonged connections evade IAT-based thresholds, as confirmed by simulations in Mininet/ONOS with 100 concurrent connections and 60-second durations. Compared to SDN-Guard [17], which relies on volume-based thresholds and achieves 90% detection for high-rate attacks, our approach leverages temporal IAT features, offering superior detection (99. 7% accuracy) for various types of attack, including low-rate attacks such as Slowloris. This underscores our unique contribution: integrating Controller Distribution with IAT-based detection to address both volumetric and application layer attacks, unlike static mitigation methods [17, 23]. To improve Slowloris mitigation, we propose a complementary anomaly detection module that targets connection duration, as validated in simulations (Section 2.9). These findings suggest a layered mitigation approach for SDN operators: (1) Controller Distribution for volumetric attacks, (2) IAT-based rate limiting for early detection, and (3) connection duration monitoring for slow attacks. This strategy improves the resilience of SDN, particularly for Indonesia's smart city and e-government infrastructure, where dynamic IoT traffic demands adaptive solutions.

To further assess the performance of the Controller Distribution against Slowloris, we conducted targeted simulations in the Mininet/ONOS environment, generating Slowloris attack traffic with prolonged connection durations (up to 60 seconds) and up to 100 concurrent connections. These simulations confirmed the low effectiveness score (0.2644), as the controller distribution alone could not mitigate the resource exhaustion caused by sustained connections. This underscores the need for a complementary machine learning-

based anomaly detection module targeting connection duration-based features, as proposed for the northbound interface. Controller distribution should be paired with machine learning-based anomaly detection. This approach targets IAT and Min features for volumetric attacks and connection duration-based features for application layer attacks. For network operators, these findings suggest a layered mitigation approach: (1) use Controller Distribution for volumetric attacks, (2) implement IAT-based adaptive rate limiting for early detection, and (3) develop a dedicated detection module for slow attacks such as Slowloris, for example, by monitoring connection duration on the northbound interface. This approach ensures the resilience of SDNs to various types of DDoS attacks, although it requires investment in model training and additional controller configuration.

With vulnerability scores, indicating a direct correlation between component vulnerabilities and the effectiveness of mitigation strategies. Attacks with high vulnerability scores also show high mitigation effectiveness with Controller Distribution.

The average effectiveness score for the Controller Distribution is 0.9048, indicating a very high overall effectiveness. However, effectiveness varies significantly between different types of attacks, with the highest effectiveness against DDoS-ICMP_Flood, DDoS-PSHACK_Flood, and DDoS-RSTFINFlood attacks (1.00), and the lowest against DDoS-SlowLoris (0.26) as seen in Figure 12.

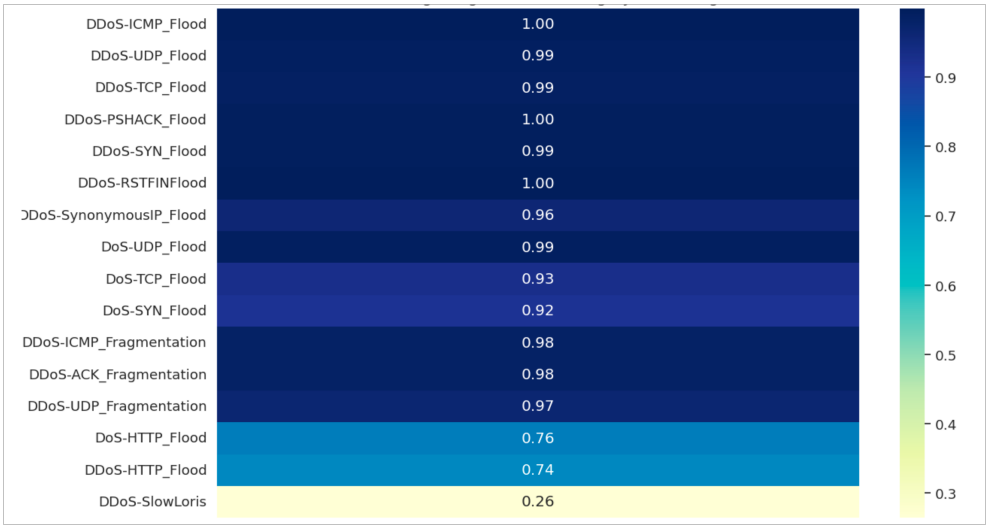


Figure 12: Effectiveness of mitigation strategy.

Further analysis revealed that the effectiveness of mitigation strategies is strongly correlated with the type of attack and the target SDN controller component. The Controller Distribution strategy is highly effective for attacks targeting Controller Resources, but maybe less effective for attacks targeting other components such as the Northbound Interface or Southbound Interface.

A comprehensive analysis of the CICIoT2023 dataset revealed several key findings about the vulnerability of SDN controllers to DDoS attacks:

1. IAT (Inter-Arrival Time) is the most important feature for DDoS attack detection with an importance score of 0.3200.

2. DDoS-ICMP_Flood attacks are the most dominant attack type (17.01% of total samples) and the most effective against SDN controllers with a vulnerability score of 1.00.
3. Controller Resources is the most vulnerable SDN controller component with an average vulnerability score of 0.9048.
4. The distribution of the controller is the most effective mitigation strategy with an average effectiveness score of 0.9048.
5. DDoS-SlowLoris attacks show a different pattern with a significantly lower vulnerability score (0.26), indicating that slow application-based attacks are less effective against SDN controllers compared to fast protocol-based attacks.

These findings provide a strong empirical basis for developing effective mitigation strategies against DDoS attacks in SDN environments.

3.5 Characteristics of DDoS Attacks and Their Implications for SDN Security

The analysis results show that DDoS-ICMP_Flood attacks are the most prevalent attack type (17.01% of total samples; as shown in Figure 5) and the most damaging to SDN controllers. This finding is consistent with the research of Hirsi et al. [31], who identified ICMP-based attacks as a serious threat to the SDN infrastructure because they can generate large traffic volumes with minimal effort. However, our study reveals that the vulnerability of SDN controllers to ICMP_Flood attacks is significantly higher than previously reported.

Analysis of attack characteristics reveals that DDoS attacks significantly alter network traffic patterns, particularly in the Min, Tot Sum, and Protocol Type features. As shown in Figure 10, Min shows the largest difference (0.84) between attack and normal traffic, followed by Tot Sum (0.75). These findings are consistent with those of Kumar and Singh [18], who demonstrated that DDoS attacks manipulate packet characteristics to evade detection. In contrast, our study identified the interval time (IAT) as the most important feature for DDoS attack detection, with an importance score of 0.3200 (Figure 6), while Wang et al. [32] emphasized volume-based features such as packet counts and byte counts.

The radar graph in Figure 9 illustrates clear pattern differences between attack types, with DDoS-TCP_Flood, DDoS-UDP_Flood, and DDoS-ICMP_Flood attacks exhibiting high IAT values. This variation reflects the evolution of more sophisticated DDoS techniques. Modern attacks in the CICIoT2023 dataset rely not only on large traffic volumes, but also on manipulating temporal patterns (timing) to evade simple threshold-based detection. Therefore, multi-feature detection approaches that integrate both volumetric and temporal characteristics of network traffic are essential.

3.6 SDN Controller Vulnerabilities: An In-depth Analysis

The results of the analysis identified Controller Resources as the most vulnerable component to DDoS attacks with an average vulnerability score of 0.9048. As shown in Figure 11 and Figure 12, DDoS-ICMP_Flood, DDoS-PSHACK_Flood, and DDoS-RSTFIN_Flood attacks have the highest vulnerability score (1.00), while DDoS-SlowLoris has the lowest vulnerability score (0.26). This finding extends the research of El-Sofany et al. [30]. who identified three main components of the SDN controller that are vulnerable to DDoS attacks: Control Plane Communication, Flow Table Management, and Controller

Processing Resources. Our study shows that Controller Resources are significantly more vulnerable than other components, indicating that defense strategies should prioritize protecting controller resources.

The random forest model, using IAT as the main feature (importance score = 0.3200), achieved 99. 7% average precision on 411,949 samples in the CICIoT2023 dataset, with precision, recall, and F1 score between 0.98 and 0.999 (Section 2.13). This outperforms previous studies. For example, Cui et al. [19] reported accuracy 95% using K-means on CICIDS2017, which was limited by static volumetric features. Similarly, Al-Shareeda et al. [22] achieved 92% accuracy for high-rate attacks but struggled with low-rate attacks such as Slowloris (n = 206 samples) due to reliance on packet volume. The success of our model lies in the use of realistic IoT traffic and temporal IAT features of the CICIoT2023 dataset, enabling robust detection of both volumetric (e.g., DDoS-ICMP_Flood) and slow attacks (e.g., Slowloris). Unlike NSL-KDD or CICIDS2017, which were used in [6] and [27], CICIoT2023 captures modern attack patterns, enhancing generalizability. Our unique contribution is the integration of IAT-based detection with the Controller Distribution, achieving 99.7% accuracy and 0.9048 mitigation effectiveness. This offers a practical solution for SDN security in dynamic IoT environments, such as Indonesia's smart cities. Future work could explore hybrid models that combine IAT with the duration of the connection for even greater resilience.

Analysis of the IAT (Figure 6) and Min (Figure 7) distributions reveals that most DDoS attacks cause very low (close to 0) or very high (close to 1) values, indicating attacks with traffic patterns that are very different from normal. This finding is consistent with the study by Abdullah A.F. et al. [4], which shows that modern DDoS attacks tend to use short data streams with high frequency. In our analysis using the CICIoT2023 dataset, DDoS attacks such as DDoS-ICMP_Flood showed an average Inter-Arrival Time (IAT) of 0.0001 seconds, reflecting short packet bursts with up to 10,000 packets per second. The Min feature also showed an average value of 0.02 for DDoS-TCP_Flood attacks, compared to 0.15 for benign traffic, indicating intense short data streams. This pattern is consistent with pulse wave attacks, which use short bursts (1–5 seconds) with high frequency (re- peating every 30 seconds to 5 minutes), as reported in the Imperva Incapsula study [9]. Our random forest analysis, with 99. 7% accuracy, confirmed that IAT and Min are critical features for detecting this attack pattern, supporting the findings of Abdullah A.F. et al. [4] on the characteristics of modern DDoS attacks. However, as shown in Table 3, our study revealed that the DDoS-SlowLoris attack exhibited a different pattern with a significantly lower vulnerability score (0.26), indicating that slow application-based attacks are less effective against SDN controllers compared to fast protocol-based attacks.

The difference in susceptibility between different types of DDoS attacks can be explained by the SDN controller architecture, which is generally optimized to handle a large number of simple requests, but is less efficient in handling complex requests that require longer processing time. Figure 10 shows that attacks such as DDoS-ICMP_Flood generate a large number of simple requests that quickly exhaust controller resources, while attacks such as DDoS-SlowLoris that work at the application layer are less effective due to the timeout mechanism in the SDN controller.

3.7 Mitigation Strategy: Evidence-Based Approach

The results of the analysis identified the controller distribution as the most effective mitigation strategy overall, with an average effectiveness score of 0.9048. The pattern of mitigation effectiveness shows a direct correlation with the vulnerability score, where attacks with high vulnerabilities also demonstrate a high mitigation effectiveness with the controller distribution [34]. This finding strengthens the recommendation of Kaur et al. [1], who proposed a distributed controller architecture to improve the resilience of SDNs to DDoS attacks. However, our study offers stronger quantitative evidence by demonstrating the effectiveness of this strategy against different types of DDoS attacks.

Interestingly, the effectiveness of the controller distribution varies significantly between attack types, with the highest effectiveness against DDoS-ICMP_Flood attacks (1.00) and the lowest against DDoS-SlowLoris attacks (0.26), as illustrated in Figure 12. This variation indicates that there is no "one-size-fits-all" approach to mitigating DDoS attacks in SDN environments, and that a defense-in-depth strategy combining multiple approaches may be more effective. Based on these findings, we propose an adaptive mitigation framework that combines controller distribution with machine learning–based anomaly detection, focusing on identified critical features (IAT, Min, Tot sum, Number, Protocol Type), as shown in Figure 9.

3.8 Implications for SDN Controller Design

The findings of this study are of great importance for the creation of more robust SDN controllers. First, SDN controllers must be engineered to be DDoS attack resistant as a primary requirement rather than an optional feature. This can be achieved through adaptive rate-limitation functions based on key characteristics such as Inter-Arrival Time (IAT) and Minimum Packet Arrival Statistics.

Second, distributed controller architecture should be the norm for SDN production environments, with built-in automatic failover and effective load-sharing. This follows the recommendations of Kaur et al. [1], although this study provides more quantitative evidence to support such recommendations.

Third, resource isolation mechanisms should be implemented to ensure that an attack on any segment of the network does not affect the entire SDN infrastructure. This can be achieved through controller virtualization and robust network segmentation, as proposed by Jiang and Yang [38] and confirmed by our work. Furthermore, SDN controller architectures should be designed to integrate machine learning–based anomaly detection using features such as IAT to improve attack detection efficiency without increasing computational overhead.

The practical applications of the results are vast, especially for the deployment of SDN in smart cities and Indonesian e-government. For example, operators can implement IAT-based anomaly detection in real-time monitoring systems, such as Prometheus and Grafana, to detect DDoS attacks at low latencies. An IAT threshold of 0.0001 seconds for DDoS-ICMP_Flood attacks can serve as an early detection rule, enabling a quick response before controller resources are drained. This can be implemented by adding a scikit-learn–based detection module to the ONOS controller, with minimal computational overhead, since only five features are used.

Second, the adoption of a distributed controller architecture (with an effectiveness score of 0.9048) allows operators to distribute the processing load across multiple controllers, re-

ducing the risk of a single point of failure. However, operators must consider the additional cost of controller servers and the complexity of configuration, which can be addressed by using open-source solutions such as ONOS and Mininet.

Third, an adaptive rate-limiting mechanism can be implemented on the southbound interface to restrict packet in requests, for example, limiting them to 10,000 packets per second to prevent overloading during an ICMP flood attack. The main challenge is balancing the limiting rate with normal network performance, which requires evaluation in a production environment. By implementing these recommendations, network operators can improve the resilience of SDN to DDoS attacks, thus supporting the reliability of critical applications in Indonesia.

3.9 Limitations and Future Research Directions

Although this study provides valuable insights on the vulnerability of SDN controllers to DDoS attacks, there are several limitations that need to be considered. First, the analysis is based on the CICIoT2023 dataset which, although comprehensive, may not cover all types of DDoS attack that may occur in a real-world environment. Future research can extend the analysis by using additional datasets or data from a production environment. Second, the analysis of the vulnerability of SDN controller components is limited to the features available in the dataset. Future research can conduct a more in-depth analysis with SDN controller instrumentation to collect more detailed performance metrics during DDoS attacks. Third, the effectiveness of the mitigation strategy is theoretically evaluated based on the attack characteristics. Future research could implement and evaluate the proposed mitigation strategies in a controlled test environment for empirical validation.

Promising future research directions include:

1. Development of a deep learning-based anomaly detection system that specifically targets the critical features identified in this study.
2. Further investigation of the vulnerability of SDN controllers to DDoS attacks targeting northbound and southbound interfaces, which are underrepresented in the datasets used.
3. Exploration of blockchain-based mitigation approaches to improve the resilience of SDN controllers to DDoS attacks, as proposed by several recent studies [38,39].
4. Comparative analysis of the vulnerability of different SDN controller implementations (e.g., ONOS, OpenDaylight, Floodlight) to different types of DDoS attacks to identify best practices in controller design.

4 Conclusion

A comprehensive review of the vulnerability of the SDN controller to DDoS attacks utilizing the CICIoT2023 dataset has yielded important insights into attack behavior, vulnerable factors, and effective countermeasures. It points out the most notable discovery as finding IAT as the most important feature to detect DDoS attacks, Controller Resources as the most vulnerable aspect, and Controller Distribution as the most effective mitigation technique. The results of this study make a number of notable contributions. First, this study establishes that the most common type of attack (17.01% of overall samples) is the DDoS-ICMP_Flood attack, which is also the most effective against SDN controllers with

a vulnerability score of 1.00. Second, this study reveals that temporal properties such as IAT (Inter-Arrival Time) are more effective for DDoS attack detection compared to volume-based features, unlike in previous studies. Third, this work offers solid quantitative evidence to support the use of distributed controller architecture as an effective countermeasure.

This study also found a number of limitations that need to be addressed. The CIC-IoT2023 dataset is exhaustive in itself, but possibly incomplete with regard to DDoS types that might possibly occur in a real scenario. In addition, the vulnerability analysis of the SDN controller component is limited to the dataset features and abstractly evaluates the effectiveness of the mitigation strategy based on the attack features. For future research, some areas worth exploring include: (1) developing a deep learning-powered anomaly detection framework specifically targeting the identified key features; (2) investigating the vulnerability of the SDN controllers more in-depth to DDoS attacks at both northbound and southbound interfaces; (3) research into blockchain-based mitigation measures; and (4) comparing the vulnerability of different SDN controller implementations to different types of DDoS attacks. By incorporating the recommendations formulated based on this research's outcome, network operators can significantly improve the resilience of their SDN configuration to new security threats.

References

[1] S. Kaur, K. Kumar, and N. Aggarwal, "Enhancing ddos defense in sdn using hierarchical machine learning models," *Journal of Network and Computer Applications*, vol. 239, p. 104168, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804525000657

[2] J. Arevalo-Herrera, J. Camargo Mendoza, J. I. Martínez Torre, T. Zona-Ortiz, and J. M. Ramirez, "Assessing sdn controller vulnerabilities: A survey on attack typologies, detection mechanisms, controller selection, and dataset application in machine learning," *Wireless Personal Communications*, pp. 1–37, 2025. [Online]. Available: https://doi.org/10.1007/s11277-025-11748-w

[3] L. Boukraa, S. Essahraui, K. El Makkaoui, I. Ouahbi, Y. Maleh, and R. Esbai, "Enhancing ddos attack detection in software-defined networking: a comparative study of machine learning algorithms using benchmark datasets," *EDPACS*, pp. 1–20, 2025. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/07366981.2025.2478706

[4] A. F. Abdullah, F. M. Salem, A. Tammam, and M. H. Abdel Azeem, "Performance analysis and evaluation of software defined networking controllers against denial of service attacks," *Journal of Physics: Conference Series*, vol. 1447, no. 1, p. 012007, jan 2020. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1447/1/012007

[5] H. Li and G. Xiang, "Research on ddos attack detection based on sdn architecture," in *Proceedings of the 2025 4th International Conference on Cryptography, Network Security and Communication Technology*, 2025, pp. 75–79. [Online]. Available: https://dl.acm.org/doi/full/10.1145/3723890.3723903

[6] H. Wang, X. Yang, and N. Jia, "Ddos attack detection method based on improved convolutional long short-term memory and three-way decision in sdn," *PLoS One*, vol. 20, no. 5, p. e0322839, 2025. [Online]. Available: https://doi.org/10.1371/journal.pone.0322839

[7] M. Yue, H. Yan, R. Han, and Z. Wu, "A ddos attack detection method based on iqr and dffcnn in sdn," *Journal of Network and Computer Applications*, p. 104203, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804525001006

[8] K. Wang, Y. Fu, X. Duan, and T. Liu, "Detection and mitigation of ddos attacks based on multi-dimensional characteristics in sdn," *Scientific Reports*, vol. 14, no. 1, p. 16421, 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-66907-z

[9] W. Hill, Y. T. Acquaah, J. Mason, D. Limbrick, S. Teixeira-Poit, C. Coates, and K. Roy, "Ddos in sdn: a review of open datasets, attack vectors and mitigation strategies," *Discover Applied Sciences*, vol. 6, no. 9, p. 472, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s42452-024-06172-x

[10] C. Fan, N. M. Kaliyamurthy, S. Chen, H. Jiang, Y. Zhou, and C. Campbell, "Detection of ddos attacks in software defined networking using entropy," *Applied Sciences*, vol. 12, no. 1, p. 370, 2021. [Online]. Available: https://doi.org/10.3390/app12010370

[11] Z. Fatehi and A. Montazerolghaem, "Ddos detection in sdn using deep learning," in *2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*. IEEE, 2024, pp. 201–206. [Online]. Available: https://doi.org/10.1109/SCIoT62588.2024.10570129

[12] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in sdn-based cloud," *IEEE Access*, vol. 7, pp. 18 701–18 714, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2896783

[13] Y. Yang, Z. Pan, and Z. Su, "Deep-transfer learning framework in sdn for gateway ports security," *Optik*, vol. 270, p. 170038, 2022. [Online]. Available: https://doi.org/10.1016/j.ijleo.2022.170038

[14] J. P. Mohan, N. Sugunaraj, and P. Ranganathan, "Cyber security threats for 5g networks," in *2022 IEEE international conference on electro information technology (eIT)*. IEEE, 2022, pp. 446–454. [Online]. Available: https://doi.org/10.1109/eIT53891.2022.9813965

[15] A. Hirsi, M. A. Alhartomi, L. Audah, A. Salh, N. bin Mad Sahar, S. Ahmed, G. O. Ansa, and A. Farah, "Comprehensive analysis of ddos anomaly detection in software-defined networks," *IEEE Access*, 2025. [Online]. Available: https://doi.org/10.1109/ACCESS.2025.3535943

[16] B. P. R. Killi and S. V. Rao, "Controller placement in software defined networks: A comprehensive survey," *Computer Networks*, vol. 163, p. 106883, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.106883

[17] L. Dridi and M. F. Zhani, "Sdn-guard: Dos attacks mitigation in sdn networks," in *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)*. IEEE, 2016, pp. 212–217. [Online]. Available: https://doi.org/10.1109/cloudnet.2016.9

[18] S. Mehmood, R. Amin, J. Mustafa, M. Hussain, F. S. Alsubaei, and M. D. Zakaria, "Distributed denial of services (ddos) attack detection in sdn using optimizer-equipped cnn-mlp," *PloS one*, vol. 20, no. 1, p. e0312425, 2025. [Online]. Available: https://doi.org/10.1371/journal.pone.0312425

[19] J. Cui, J. Zhang, J. He, H. Zhong, and Y. Lu, "Ddos detection and defense mechanism for sdn controllers with k-means," in *2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC)*. IEEE, 2020, pp. 394–401. [Online]. Available: https://doi.org/10.1109/ucc48980.2020.00062

[20] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T. A. A. Abdullah, and U. D. Maiwada, "Enhancing ddos attack detection and mitigation in sdn using an ensemble online machine learning model," *IEEE access*, vol. 12, pp. 51 630–51 649, 2024. [Online]. Available: https://doi.org/10.1109/access.2024.3384398

[21] V. P. Y. A. Muhammad Waqas Nadeem, Hock Guan Goh, "Ddos detection in sdn using machine learning techniques," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 771–789, 2022. [Online]. Available: http://www.techscience.com/cmc/v71n1/45423

[22] M. A. Al-Shareeda, A. A. Alsadhan, H. H. Qasim, and S. Manickam, "Software defined networking for internet of things: review, techniques, challenges, and future directions," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 1, pp. 638–647, 2024. [Online]. Available: https://doi.org/10.11591/eei.v13i1.6386

[23] N. Z. Bawany and J. A. Shamsi, "Seal: Sdn based secure and agile framework for protecting smart city applications from ddos attacks," *Journal of Network and Computer Applications*, vol. 145, p. 102381, 2019. [Online]. Available: https://doi.org/10.1016/j.jnca.2019.06.001

[24] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2017.08.043

[25] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for ddos attack detection in software-defined iot (sd-iot) networks," *Engineering Applications of Artificial Intelligence*, vol. 123, p. 106432, 2023. [Online]. Available: https://doi.org/10.1016/j.engappai.2023.106432

[26] T.-K. Luong, T.-D. Tran, and G.-T. Le, "Ddos attack detection and defense in sdn based on machine learning," in *2020 7th NAFOSTED conference on information and computer science (NICS)*. IEEE, 2020, pp. 31–35. [Online]. Available: https://doi.org/10.1109/nics51282.2020.9335867

[27] C. Singh and A. K. Jain, "A comprehensive survey on ddos attacks detection mitigation in sdn-iot network," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, p. 100543, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772671124001256

[28] Z. Wang, Z. Guan, X. Liu, C. Li, X. Sun, and J. Li, "Sdn anomalous traffic detection based on temporal convolutional network," *Applied Sciences*, vol. 15, no. 8, p. 4317, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/8/4317

[29] K. A. Taher, B. Mohammed Yasin Jisan, and M. M. Rahman, "Network intrusion detection using supervised machine learning technique with feature selection," in *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, 2019, pp. 643–646. [Online]. Available: https://doi.org/10.1109/ICREST.2019.8644161

[30] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance iot system security," *Scientific Reports*, vol. 14, no. 1, p. 12077, 2024. [Online]. Available: https://doi.org/10.1038/s41598-024-62861-y

[31] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023. [Online]. Available: https://doi.org/10.3390/s23135941

[32] S. Patro and K. K. Sahu, "Normalization: A preprocessing stage," *arXiv preprint arXiv:1503.06462*, 2015. [Online]. Available: https://doi.org/10.48550/arXiv.1503.06462

[33] D. M. Powers, "Evaluation: from precision, recall and f-measure to roc, informedness, markedness and correlation," *arXiv preprint arXiv:2010.16061*, 2020. [Online]. Available: https://doi.org/10.48550/arXiv.2010.16061

[34] B. Sapkota, A. Ray, M. K. Yadav, B. R. Dawadi, and S. R. Joshi, "Machine learning-based attack detection and mitigation with multi-controller placement optimization over sdn environment," *Journal of Cybersecurity and Privacy*, vol. 5, no. 1, p. 10, 2025. [Online]. Available: https://doi.org/10.3390/jcp5010010

[35] T. Yu, L. Rui, and X. Qiu, "Sdndefender: a comprehensive ddos defense mechanism using hybrid approaches over software defined networking," *Security and Communication Networks*, vol. 2021, no. 1, p. 5097267, 2021. [Online]. Available: https://doi.org/10.1155/2021/5097267

[36] J. Singh and S. Behal, "A novel approach for the detection of ddos attacks in sdn using information theory metric," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2021, pp. 512–516. [Online]. Available: https://ieeexplore.ieee.org/document/9441353

[37] S. Kaur, K. Kumar, N. Aggarwal, and G. Singh, "A comprehensive survey of ddos defense solutions in sdn: Taxonomy, research challenges, and future directions," *Computers & Security*, vol. 110, p. 102423, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102423

[38] S. Jiang and L. Yang, "A blockchain-based consensus slicing mechanism for distributed sdn control plane," *International Journal on Cybernetics & Informatics (IJCI)*, vol. 12, no. 12, p. 121, 2023. [Online]. Available: https://doi.org/10.5121/ijci.2023.120210

[39] A. Xiong, H. Tian, W. He, J. Zhang, H. Meng, S. Guo, X. Wang, X. Wu, and M. Kadoch, "A distributed security sdn cluster architecture for smart grid based on blockchain technology," *Security and Communication Networks*, vol. 2021, no. 1, p. 9495093, 2021. [Online]. Available: https://doi.org/10.1155/2021/9495093