

DanielJamesProposal

by Daniel James

Submission date: 04-May-2026 02:05PM (UTC+0100)

Submission ID: 282006992

File name: 40166_Daniel_James_DanielJamesProposal_726821_188596504.pdf (359.33K)

Word count: 4847

Character count: 31046



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

DESIGN AND VALIDATION OF A PHYSICAL SDN DDOS DATASET FOR REAL-TIME DETECTION RESEARCH

Daniel James

2218766@student.uwtsd.ac.uk

ACFA7004: Research Methods and Professional
Development

Abstract

Software-Defined Networking (SDN) has become increasingly important in modern enterprise and cloud-based environments due to its flexibility and centralised control architecture. However, this architecture introduces significant security challenges, particularly in relation to Distributed Denial of Service (DDoS) attacks, which can overwhelm the SDN controller and disrupt overall network performance. A key issue identified in current research is the reliance on simulated environments and legacy datasets for evaluating DDoS detection techniques. These datasets often fail to capture SDN-specific characteristics such as flow-based communications and controller interactions, resulting in limited realism and reduced comparability of results. This project aims to address this limitation by designing and validating a dataset generated within a physical SDN environment that better reflects real-world network behaviour. This study adopts a mono method experimental approach to generate both benign and malicious traffic. The dataset will be evaluated using established detection techniques, with performance measured through metrics such as accuracy, latency, and resource usage. This research aims to contribute a structured SDN dataset to support more reliable evaluation of DDoS detection techniques and improve the overall quality of SDN security research.

Table of Contents

Abstract	2
1.0 Introduction	4
1.1 Context and Background	4
1.2 Research Problem	5
1.3 Research Aim and Objectives	5
1.4 Significance of the Research	6
2.0 Literature Review	7
2.1 SDN DDoS Detection Techniques	7
2.2 Dataset Limitations in SDN Research	10
2.3 Research Gap	11
2.4 Relation to this Study	12
2.5 Conclusion	12
3.0 Research Design and Methodology	14
3.1 Research Design and Justification	14
3.2 Research Methods and Materials	15
3.2.1 Experimental Setup and System Design	15
3.2.2 Data Generation and Collection	16
3.2.3 Data Analysis and Evaluation Strategy	16
3.2.4 Materials and Tools	17
3.2.5 Reliability, Validity, and Generalisability	17
4.0 Expected Outcomes	18
5.0 Project Timeline and Milestones	18
6.0 References	19

1.0 Introduction

This proposal focuses on improving the reliability and realism of datasets used in Software-Defined Networking (SDN) security research, specifically focusing on Distributed Denial of Service (DDoS) detection. While SDN has become increasingly more important in modern enterprise and cloud-based networks, its centralised control architecture has introduced unique security challenges that are not fully addressed by traditional network architecture research [1].

A major limitation identified in existing literature is the reliance on simulated environments and legacy datasets which do not fully represent SDN behaviour [2]. As a result of this, evaluation of DDoS detection techniques may lack realism or consistency [2]. This project aims to address this by designing and validating an SDN dataset, which can support more reliable and comparable research in this area.

1.1 Context and Background

Software-Defined Networking has seen increased usage across enterprise and cloud environments due to its ability to separate the control plane from the data plane, allowing for centralised network management and programmability [3]. This shift away from traditional network architectures has enabled more flexible and scalable network configurations [3].

However, this centralised control introduces a critical vulnerability, where the SDN controller becomes a high-value target within the network due to it being responsible for managing all the network flows [4]. If the controller is overwhelmed or compromised, it can lead to widespread disruption across the entire network. One of the most significant threats in this context is DDoS attacks. These attacks generate a large amount of malicious traffic, forcing the controller to process excessive numbers of requests [5]. This can exhaust computational resources, increase latency, and ultimately lower or disable network performance [5].

To address this vulnerability, a wide range of DDoS detection techniques have been proposed, including machine learning-based approaches, statistical methods such as entropy analysis, and hybrid models [5], [6]. However, a common issue among these studies is the reliance on simulated environments and publicly available datasets such as KDD99 and CICIDS2017, which were not specifically designed for SDN environments

[7]. This focus on simulation has created a disconnect between research and real-world deployments, as the datasets may not accurately capture SDN-specific traffic behaviour, control plane interactions, or realistic attack patterns [7].

1.2 Research Problem

Despite the progress that has been made in SDN-based DDoS detection, a key limitation remains in the form of inadequate datasets used for evaluation [8]. Most existing research relies on either simulated environments or legacy datasets, which introduces several concerns.



Firstly, simulated environments often generate unrealistic traffic patterns that do not reflect real-world network conditions [8]. Secondly, many widely used datasets were originally designed for traditional networks rather than SDNs, meaning they do not capture SDN-specific characteristics such as flow-based communication or controller interactions [7], [8]. Additionally, some datasets are domain-specific, such as IoT-focused datasets, which limit their applicability [9].

1.3 Research Aim and Objectives

The aim of the project is to design and implement a physical SDN environment to generate a DDoS dataset, and to analyse and evaluate its effectiveness for real-time detection research through experimental testing.

- To conduct a systematic literature review on SDN, DDoS attacks, and the limitations of existing datasets used in SDN security research.
- To develop a suitable research methodology focused on dataset generation, including the selection of traffic parameters, data collection methods, and evaluation metrics, with justification from literature.
- To design and implement a physical SDN environment to generate structured network traffic, including both benign and DDoS attack scenarios.
- To validate the generated dataset by using multiple established DDoS detection methods to assess its suitability for detection research.
- To evaluate the dataset based on its ability to support real-time detection, using performance metrics such as accuracy, latency, and resource usage.

1.4 Significance of the Research

The research is significant because it addresses a key limitation in current SDN security research: the lack of realistic datasets for evaluating DDoS detection techniques. While many detection methods have been proposed, their effectiveness is often assessed using simulated environments or a legacy dataset [7]. This reduces the reliability of the experimental results and makes it difficult to compare different approaches.

By designing and implementing a physical SDN environment to generate a structured dataset, this study aims to provide a more realistic basis for evaluating DDoS detection techniques. The dataset will capture flow-based communication, controller interactions, and varying attack conditions, which are often missing from existing datasets. This improves the relevance of experimental results and allows for more meaningful analysis of detection performance.

In addition, this research contributes a practical artefact in the form of a generated SDN dataset, which can be used to support further research in this area. While the dataset is developed within a controlled environment, it provides an alternative to simulated data and can be extended into future work.

Overall, this project contributes to both academic research and practical network security by improving how DDoS detection techniques are evaluated in SDN environments, supporting the development of more effective and realistic security solutions.

2.0 Literature Review

This section critically reviews existing literature on DDoS detection in SDN environments, focusing on detection techniques proposed. In addition to detection techniques, attention is given to the datasets used for evaluation, as many studies rely on simulated data or legacy datasets that may not accurately reflect SDN-specific behaviour. This review is used to identify key limitations in current research and to justify the focus of this project on improving dataset realism and applicability.

2.1 SDN DDoS Detection Techniques

A wide range of DDOS detection techniques have been proposed for SDN environments, including statistical, machine learning, and hybrid approaches. These approaches vary in terms of their underlying detection strategies, complexity, and the type of data used for evaluation. As a result, comparing the effectiveness of different techniques requires careful consideration of both the detection techniques used and the datasets which they are evaluated with.

Table 1 provides an overview of selected studies on DDoS detection in SDN, highlighting key aspects such as the detection method, datasets used, experimental environments, evaluation metrics, and limitations. The table is used to illustrate the diversity of approaches in the literature and to support a structured comparison of how these techniques are evaluated.

Table 1: Summary of SDN-based DDoS detection techniques and datasets.

Study	Year	Method	Dataset	Environment	Metrics	Limitations
Hassan et al. [10]	2023	ML + DL (CNN, LSTM, RF, KNN, etc.)	InSDN	Simulated SDN	Accuracy Precision Recall F1-Score	Single dataset No real-world deployment Limited real-time evaluation
Itagi et al. [11]	2021	DL (BRNN, FFNN)	Custom SDN dataset (generated)	Simulated (Mininet, Ryu controller)	Accuracy Error rate	Small dataset Simulated environment Limited evaluation metrics Simple topology
Yu et al. [12]	2018	ML (SVM)	Mixed (DARPA, CAIDA + simulated traffic)	Simulated (Mininet, Floodlight controller)	Detection rate False alarm rate	Vehicular SDN focus Simulated environment Reliance on legacy datasets No real-world deployment
Belachew et al. [9]	2025	ML (XGBoost, RF, K-NN, FFNN)	CICIDS2017 Edge-IIoTset	Simulated SDN-Edge-IoT (Mininet, edge deployment)	Accuracy Precision Recall F1-Score Testing time	Simulated environment IoT-specific architecture Reliance on benchmark datasets
Conti et al. [13]	2017	Statistical (CuSum)	CAIDA DARPA	Simulated (Mininet, controller)	Detection rate False alarm rate Accuracy Detection time	Relies on outdated datasets Higher false positive rates Lacks ability to detect complex attacks

							Evaluated only in simulated environment
Sumantra & Indira Gandhi [14]	2020	Statistical (Entropy-based)	Custom SDN dataset (generated)	Simulated (Mininet, controller)	SDN POX	Detection time Delay CPU utilisation	Synthetic traffic only Fixed threshold-based detection Limited evaluation metrics Simple topology
Asgari & Akbari [15]	2022	Statistical (Entropy + flow statistics)	Custom SDN dataset (generated)	Simulated (Mininet, controller)	SDN POX	Accuracy Precision Recall False positive rate	Relies on simulated traffic Increased controller overhead due to flow statistics Lacks real-world validation
Zhang et al. [16]	2024	ML (GBDT)	Custom SDN dataset (generated)	Simulated (Mininet, controller)	SDN Ryu	Accuracy Recall False positive rate Detection time	Relies on simulated traffic Limited topology No real-world validation

While Table 1 demonstrates the diversity of detection techniques proposed for SDN environments, it also highlights a fundamental limitation in how these approaches are evaluated. All reviewed studies rely on simulated environments, based on Mininet testbeds with no evidence of real-world deployments [11], [12], [16]. In addition, several approaches depend on either custom-generated traffic [11], [15] or legacy datasets such as DARPA and CAIDA [12], [13] which were not designed for SDN environments. More recent work incorporates domain-specific datasets, such as IoT based data [9], which may not accurately reflect SDN traffic behaviour. As a result, differences in dataset characteristics make it difficult to directly compare detection performance across studies and raise concerns about the realism of reported results. Furthermore, several studies are evaluated under simplified experimental conditions, including limited network topologies [11], [16] and the absence of real-world validation [10], [16], which may further restrict the generalisability of findings. This suggests that improvements in detection performance may be influenced as much by the evaluation data as the detection method itself, highlighting a key limitation in current SDN DDoS research.

2.2 Dataset Limitations in SDN Research

Building upon the issues identified in the detection techniques, this section specifically focuses on the datasets used within SDN DDoS detection research. While a range of datasets are commonly applied, they differ significantly in terms of their origin, structure, and suitability for SDN environments. Exploring these differences is essential for understanding the limitations behind how detection techniques are assessed.

Table 2 summarises selected datasets used in SDN DDoS detection research, outlining their evaluation environment, classification, and key limitations. The datasets included reflect those commonly applied across the literature and are presented to enable direct comparison of how they differ in structure and applicability. By organising these characteristics, the table provides a basis for identifying limitations in existing datasets and how these may affect their use in SDN-based evaluation.

Table 2: Summary of datasets used in SDN DDoS detection research and their limitations

Dataset	Environment	Dataset Type	Limitation
InSDN [2]	Simulated SDN	SDN-specific	Simulated environment Lacks real-world deployment Limited network complexity
DARPA [17]	Simulated enterprise	Legacy	Outdated dataset Generated in a simulated environment Traffic patterns do not reflect modern network behaviour
CAIDA [18]	Internet backbone	Real-world	Limited attack diversity Short capture duration Lacks labelled benign traffic Not SDN specific
CICIDS2017 [19]	Simulated enterprise	Modern	Generated in a controlled environment Not SDN specific Limited representation of dynamic network behaviour
Edge-IIoTset [20]	IoT/Edge testbed	Domain-specific	Domain specific Not generalisable to SDN environments

As shown in Table 2, no single dataset fully satisfies the requirements for realistic SDN DDoS detection research. While InSDN [2] is specifically designed for SDN environments, it is generated with a simulated testbed and lacks real-world validation. On the other hand, datasets such as CAIDA [18] provide real-world traffic, but are not specific to SDNs and lack important characteristics such as labelled benign flows and controller-level interactions. Similarly, widely used datasets such as DARPA [17] and CICIDS2017 [19] are generated in controlled or simulated environments and do not reflect modern SDN architectures or dynamic network behaviours. Finally, domain-specific datasets, such as Edge-IIoTset [20], introduce additional limitations as their focus on IoT environments reduce their applicability to more generalised SDN scenarios.

2.3 Research Gap

The analysis of detection techniques and datasets highlights a fundamental limitation in current SDN DDoS research: a lack of datasets that are both realistic and representative of SDN environments. Existing approaches rely heavily on simulated testbeds or

datasets that were not designed for SDN architectures [11], [13], resulting in evaluation conditions that do not fully reflect real-world network behaviour. While some datasets provide realistic traffic, they lack SDN-specific characteristics such as flow-based communications and controller interactions [18], [19]. Conversely, datasets designed for SDN environments are typically generated within controlled simulations and do not capture the complexity of real network deployments.

This imbalance creates a clear disconnect between research and practical application, where the effectiveness of detection techniques is influenced by the dataset used rather than their ability to operate in realistic SDN conditions. Furthermore, the lack of a standardised dataset across studies limits the ability to directly compare results, making it difficult to decide which approach is most effective. This represents a significant limitation in the current body of SDN DDoS detection research.

2.4 Relation to this Study

This project aims to directly address the limitation identified in the existing literature by focusing on the design and validation of a dataset tailored specifically for SDN DDoS detection research. The proposed approach aims to incorporate SDN-specific characteristics, such as flow-based communication and controller interactions, while improving the realism of generated network traffic within a controlled physical experimental SDN environment.

By developing a dataset that better reflects both SDN architecture and realistic traffic behaviour, this project aims to provide a more suitable basis for evaluating detection techniques. From this, it aims to improve the reliability and comparability of experimental results, contributing to more meaningful assessment of DDoS detection methods in SDN environments.

2.5 Conclusion

This literature review has examined existing research on DDoS detection in SDN environments, highlighting both the range of detection techniques proposed and the datasets used for their evaluation. While significant progress has been made in developing statistical, machine learning, and hybrid detection methods, their evaluation is constrained by the environments and data on which they are tested.

The analysis of existing datasets demonstrates that no single dataset fully satisfies the requirements for realistic and representative SDN evaluation. Legacy datasets, simulated traffic, and domain-specific data each introduce limitations that affect the validity and comparability of the results. As a result, the effectiveness of detection techniques is often influenced by dataset characteristics rather than their ability to operate under realistic network conditions.

Overall, the literature indicates that improving the quality and relevance of datasets is essential for advancing SDN DDoS detection research. This provides a clear foundation for the focus of this study, which aims to address these limitations through the development of a more suitable dataset for evaluation.

3.0 Research Design and Methodology

This section outlines the overall research design and the methodology used to generate and evaluate the SDN DDoS dataset. The methodology is structured to align with the research aim and objectives, ensuring that a clear process for designing the SDN environment, generating network traffic, and assessing the suitability of the dataset for real-time detection research.

3.1 Research Design and Justification

The research design for this project is guided by the Research Onion [21] framework, which provides a structured approach to selecting research philosophy, approach, strategy, and method. This ensures that each methodological choice is aligned with the overall research aim and supports a systematic and justified design process. Figure 1 shows the chosen approaches as adapted from the Research Onion framework.

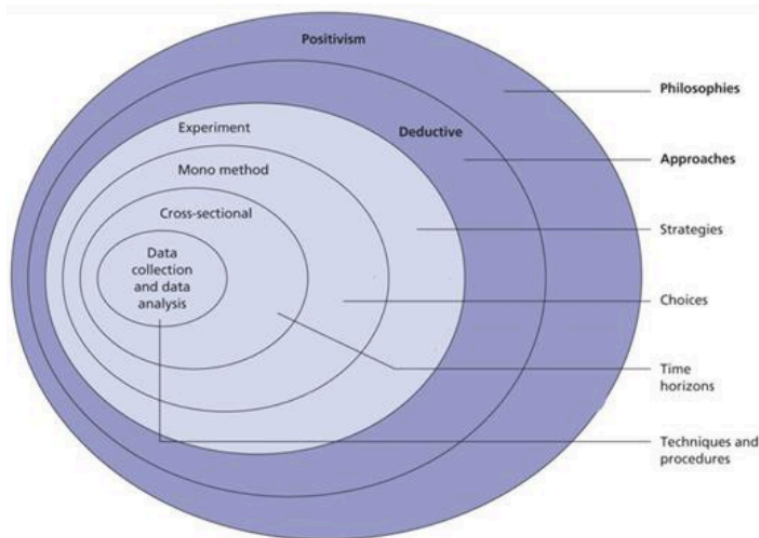


Figure 1: Chosen research methodology adapted from Saunders et al. [21]

This project will follow a positivist research philosophy, as the study focuses on measuring network behaviour and detection performance in an objective way. The dataset will consist of measurable data, such as traffic flows, latency, and resource usage.

A deductive approach is used for this project, as existing knowledge from SDN security and DDoS detection research is applied to a new experimental context. Rather than developing a new detection method, established techniques are used to validate the generated dataset, ensuring the focus remains on dataset quality. Furthermore, the research will use an experimental strategy, involving the creation of a controlled SDN environment where both normal and attack traffic can be generated. The experimental strategy was used as it is commonly applied in SDN research when controlled evaluations of network behaviour is necessary [1]. This allows key variables such as traffic intensity and attack type to be controlled and tested systematically. A quantitative mono-method is adopted, as the evaluation strategy relies on performance metrics. Finally, a cross-sectional time horizon is used, where data is collected within a defined experimental period rather than over a long period.

3.2 Research Methods and Materials

This section outlines the methods used to design the SDN environment, generate the dataset, and evaluate its suitability for DDoS detection research. It also describes the tools and materials used to support the implementation and analysis.

3.2.1 Experimental Setup and System Design

The experiment is designed to represent a simplified but realistic SDN environment. The system consists of an SDN controller, OpenFlow-enabled switches, legitimate client nodes, and attacker nodes. This reflects the core structure of SDN networks, where the controller manages network flows and communicates with switches. This setup reflects the standard SDN architecture as described in existing research [1].

Legitimate nodes generate normal network traffic, while attacker nodes simulate DDoS activity, which allows for both benign and malicious traffic to be captured within the same environment.

This design is chosen to provide a balance between realism and control. A fully real-world network would introduce too many uncontrollable variables, while purely simulated environments may lack realism. The controlled SDN setup allows structured data generation while still capturing key SDN characteristics such as flow-based communications and controller interactions. Furthermore, this design addresses

limitations identified in the literature, particularly the reliance on simulated environments and non-SDN-specific datasets [10], [11], [12].

3.2.2 Data Generation and Collection

Data is generated by producing both normal and attack traffic within the SDN environment. The normal traffic will simulate typical network activity, such as web requests and background communication, while attack traffic includes common DDoS attacks such as TCP SYN floods, UDP floods, and ICMP floods, as these are widely used in SDN research [9], [10].

To ensure the dataset reflects a range of realistic conditions, several parameters can vary, such as attack duration, packet rate, and number of attacking nodes. These parameters allow for different levels of attack intensity and distribution to be represented, improving the usefulness of the dataset for testing.

Data is collected using PCAP tools and SDN flow statistics from the controller. Additional metrics such as controller resource usage and network latency are also recorded. This provides both traffic-level and system-level data, which is important for evaluating performance under different conditions. The dataset is stored in standard formats such as PCAP and CSV, allowing for consistent analysis and reuse.

In this experiment, the independent variables include traffic-related parameters such as attack type, packet rate, attack duration, and the number of attacking nodes. These variables are controlled and adjusted to generate different network conditions. The dependent variables are the resulting detection performance metrics, including accuracy, false positive rate, and detection latency, as well as system-level metrics such as controller resource usage. This allows the impact of varying traffic conditions on detection effectiveness to be studied.

3.2.3 Data Analysis and Evaluation Strategy

The dataset is evaluated by applying established DDoS detection techniques and measuring their performance. This includes both entropy-based methods and machine learning approaches, allowing for different detection styles to be tested. Entropy-based detection could be considered due to its efficiency and suitability for real-time environments, while machine learning techniques is an option due to its wide use in SDN security research and can capture more complex traffic patterns [10], [14].

Performance can be measured using metrics including accuracy, F1-score, false positive rate, and detection latency. These metrics are selected as they provide a balanced evaluation of detection performance and are commonly used in security research [22]. This evaluation approach allows the effectiveness of the dataset to be assessed based on how well it supports detection, rather than focusing on the performance of a single detection method.

3.2.4 Materials and Tools

The physical SDN environment for dataset creation will be implemented using a SDN controller such as Ryu, the simulated environment for evaluation will be implemented using tools such as Mininet. Python will be used for traffic generation, data processing, and analysis. Packet capture tools such as tcpdump or Wireshark are used to collect network traffic, while system monitoring tools record performance metrics. The simulated system will be deployed on hardware capable of supporting virtualised network environments.

Ethical considerations are minimal, as all traffic will be generated in a controlled lab environment and does not involve real users. This ensures that the research complies with ethical requirements while still producing relevant and realistic data.

3.2.5 Reliability, Validity, and Generalisability

Reliability is ensured by maintaining a controlled experimental environment, where network configurations and traffic generation parameters are consistent across tests. This allows experiments to be repeated under the same conditions, improving the consistency of results.

Validity is addressed by designing the SDN environment to reflect key characteristics of real networks, including flow-based communications and controller interactions. Additionally, the use of both benign and attack traffic ensures that the dataset represents realistic network behaviour, supporting accurate evaluation of detection techniques.

Generalisability is considered by varying traffic parameters such as attack intensity and duration, allowing the dataset to represent a range of network conditions. However, as the environment remains controlled, some limitations in generalisability to large-scale real-world deployments may still exist. This is acknowledged as a trade-off between experimental control and realism.

4.0 Expected Outcomes

This project is expected to produce a DDoS dataset generated within a physical SDN environment. The dataset will include both normal and attack traffic, capturing key SDN characteristics such as flow-based communications and controller behaviours while under different network conditions. It is expected that the dataset will support the application and research of existing DDoS detection techniques, allowing their performance to be evaluated in a more realistic environment compared to purely simulated datasets. Detection methods are expected to demonstrate measurable performance in terms of accuracy, latency, and resource usage.

The findings from the project are expected to highlight the importance of using a more representative dataset in SDN security research. Through providing a dataset generated in a controlled environment, this work may support more reliable evaluation of detection techniques and contribute to improved benchmarking in future research.

5.0 Project Timeline and Milestones

The project timeline shown in Figure 1 is structured across the main phases: initial planning and literature review, experimental implementation, and writing. Tasks are arranged to allow overlap between experimentation and writing, ensuring efficient use of time within the project period.

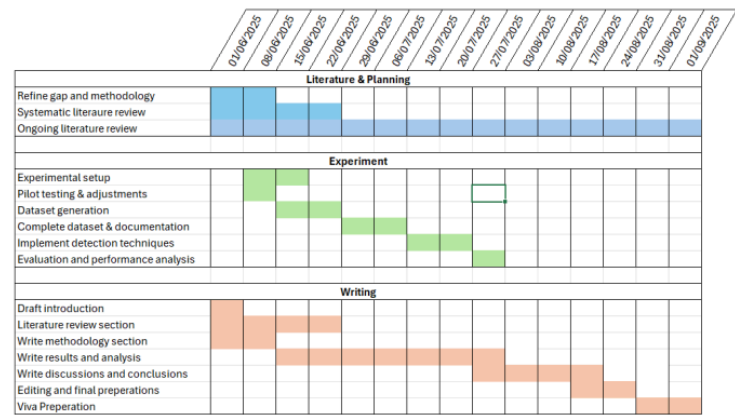


Figure 2 Project Timeline (Gantt Chart)

6.0 References

- [1] D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolkly, and S. Uhlig, 'Software-Defined Networking: A Comprehensive Survey', *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.
- [2] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, 'InSDN: A Novel SDN Intrusion Dataset', *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.
- [3] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y.-W. Chong, and Y. K. Sanjalawe, 'Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller—A Review', *IEEE Access*, vol. 8, pp. 143985–143995, 2020, doi: 10.1109/ACCESS.2020.3013998.
- [4] S. M. Mousavi and M. St-Hilaire, 'Early detection of DDoS attacks against SDN controllers', in *2015 International Conference on Computing, Networking and Communications (ICNC)*, Garden Grove, CA, USA: IEEE, Feb. 2015, pp. 77–81. doi: 10.1109/ICCNC.2015.7069319.
- [5] R. Fadaei Fouladi, O. Ermis, and E. Anarim, 'A Comparative Study on the Performance Evaluation of DDoS Attack Detection Methods', in *2022 30th Signal Processing and Communications Applications Conference (SIU)*, Safranbolu, Turkey: IEEE, May 2022, pp. 1–4. doi: 10.1109/SIU55565.2022.9864872.
- [6] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, 'Sdn Security: A Survey', in *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Trento, Italy: IEEE, Nov. 2013, pp. 1–7. doi: 10.1109/SDN4FNS.2013.6702553.
- [7] J. Hussain and V. Hnamte, 'A Novel Deep Learning Based Intrusion Detection System: Software Defined Network', in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2021, pp. 506–511. doi: 10.1109/3ICT53449.2021.9581404.
- [8] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, 'A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking', *Sensors*, vol. 23, no. 9, p. 4441, May 2023, doi: 10.3390/s23094441.
- [9] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa, and A. J. Muhammed, 'Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning', *IEEE Access*, vol. 13, pp. 10194–10214, 2025, doi: 10.1109/ACCESS.2025.3526692.
- [10] H. A. Hassan, E. El-Din Hemdan, M. Shokair, F. E. A. El-Samie, and W. El-Shafai, 'An Efficient Attack Detection Framework in Software-Defined Networking using Intelligent Techniques', in *2023 3rd International Conference on Electronic Engineering (ICEEM)*, 2023, pp. 1–6. doi: 10.1109/ICEEM58740.2023.10319575.
- [11] V. Itagi, M. Javali, H. Madhukeshwar, P. Shettar, P. Somashekar, and D. G. Narayan, 'DDoS Attack Detection in SDN Environment using Bi-directional Recurrent Neural Network', in *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Nite, India: IEEE, Nov. 2021, pp. 123–128. doi: 10.1109/DISCOVER52564.2021.9663667.

- [12] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, 'An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks', *IEEE Access*, vol. 6, pp. 44570–44579, 2018, doi: 10.1109/ACCESS.2018.2854567.
- [13] M. Conti, A. Gangwal, and M. S. Gaur, 'A comprehensive and effective mechanism for DDoS detection in SDN', in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Rome: IEEE, Oct. 2017, pp. 1–8. doi: 10.1109/WiMOB.2017.8115796.
- [14] I. Sumantra and S. Indira Gandhi, 'DDoS attack Detection and Mitigation in Software Defined Networks', in *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India: IEEE, Jul. 2020, pp. 1–5. doi: 10.1109/ICSCAN49426.2020.9262408.
- [15] S. Asgari and B. Akbari, 'DDoS Attack Detection in OpenFlow Based Networks', in *2022 27th International Computer Conference, Computer Society of Iran (CSICC)*, Tehran, Iran, Islamic Republic of: IEEE, Feb. 2022, pp. 1–7. doi: 10.1109/CSICC55295.2022.9780508.
- [16] R. Zhang, G. Yang, and W. Zhang, 'DDoS Attack Detection System Based on GBDT Under SDN', in *2024 IEEE 7th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chongqing, China: IEEE, Sep. 2024, pp. 1415–1419. doi: 10.1109/ITNEC60942.2024.10733143.
- [17] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, 'The 1999 DARPA o-line intrusion detection evaluation'.
- [18] 'The CAIDA "DDoS Attack 2007" Dataset', CAIDA. Accessed: Oct. 14, 2025. [Online]. Available: https://www.caida.org/catalog/datasets/ddos-20070804_dataset/
- [19] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, 'Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization', in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. doi: 10.5220/0006639801080116.
- [20] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, 'Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning', *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.
- [21] M. Saunders, A. Thornhill, and P. Lewis, *Research methods for business students*, Eighth Edition. Harlow, United Kingdom: Pearson, 2019.
- [22] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, 'Network Anomaly Detection: Methods, Systems and Tools', *IEEE Commun. Surv. Tutor.*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.

DanielJamesProposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

80/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4



Comment 1

should not start with the literature.. here we are expecting the context of the study



Comment 2

citation ?



Comment 3

citation



Comment 4

are these hypbrid models ?

PAGE 5



Comment 5

which are those existing research ?

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

GRADING FORM: ACFA7004 PROPOSAL MAY 2026

DANIEL JAMES

80

ENGAGEMENT WITH LIT.SKILL [30]

Structure and Organization of the literature review [8 Marks] Critical Engagement with Literature [10 Marks] Relevance and Positioning of Your Study [7 Marks] Recent and Relevant in-text citations and reference list [5 Marks]



The review is logically structured and supported with tables; however, key ideas (especially dataset limitations) are repeated across sections without adding new insight, reducing clarity and conciseness.

The literature is well summarised and compared, but the analysis is mostly descriptive; there is limited critical discussion of how dataset design

26

affects detection validity.
The research gap is clearly identified and relevant.
Sources are appropriate and relevant,

KNOWLEDGE & UNDERSTANDING [20]

Brief overview and current developments in the proposed research area [10 Marks] Research problem statement [7 Marks] Significance of the study [3 Marks]



Demonstrates a good understanding of SDN, DDoS threats, and dataset challenges; however, some repetition is present and the discussion could explore the problem in slightly greater depth.
The problem is clearly stated and logically structured
The significance is clear and relevant, but some ideas are repeated across sections and could be presented more concisely.

16

COGNITIVE & INTELLECTUAL [10]

Clearly state the aim of the research based on the identified research problem [5] Break down the research aim into smaller, measurable, and achievable steps [5]



The aim is clear and relevant.
Some objectives are process-oriented (e.g., methodology development) rather than outcome-focused, and should be revised to reflect clear research outputs instead of general research activities.

7

PRACTICAL APPLICATION [25]

*Research Design (Explanation of the overall research approach) [7]
Research methods [10] - a detailed explanation about the research*

methods to achieve the research objectives Research materials [8] - in terms of Software and hardware



The design is appropriate and well-explained; The methodology is clearly described, but the justification of the evaluation strategy is limited; it is not clearly explained why specific detection approaches and evaluation metrics are appropriate for validating the dataset. Also, there is no clear methodology stated for the first objective (systematic literature review), and the process for conducting the review (e.g., selection criteria, databases, or analysis approach) should be explicitly defined. Tools and platforms are relevant and appropriate; however, the justification for their selection is limited

18

TRANSFERABLE SKILLS [15]

Project planning and resource management [5 Marks] Description of the project's potential impact and limitations [5 Marks] - Expected outcome Presentation style [5 Marks]



Project planning is well stated
Expected outcomes are clearly defined
The writing is generally clear and well presented; however, some repetition is evident.

13