HYBRID SDN-IDS FRAMEWORK FOR DYNAMIC NETWORK FUNCTION VIRTUALIZATION (NFV) SECURITY

Rajani Priya Nippatla [1, *], Bhavya Kadiyala [2], Samson A. Arekete[3]

[1]Kellton Technologies Inc, Texas, USA. Email: rajanipriyanippatla@ieee.org
[2]Parkland Health, Texas, USA. Email: bhavyakadiyala@ieee.org
[3]Redeemer's University, Ede, Nigeria. Email: areketes@run.edu.ng

ABSTRACT

Background Information: Software-Defined Networking (SDN) and Network Function Virtualization (NFV) allow for flexibility at the cost of new security vulnerabilities. Conventional security measures cannot handle these problems because NFV is dynamic. IDS integrated with SDN brings in enhanced security through centralized management and real-time threat detection, enhanced visibility, risk mitigation, and the ability to keep pace with changing cyber threats in virtualized networks.
Objectives: Improvements in scalability and flexibility of network security, real-time threat detection and response, security in dynamic NFV environments, and addressing shortcomings of conventional security models are the goals.
Methods: Using Principal Component Analysis (PCA) for feature extraction and Artificial Neural Networks (ANN) for classification, the framework uses a hybrid PCA-ANN model for intrusion detection. SDN-managed adaptive traffic rerouting modifies its course in response to risk scores derived from questionable network activities.
Results: In terms of both detection accuracy and response time, the suggested framework outperformed existing techniques such as Wasserstein GAN and Web Application Firewall, achieving a 93% detection accuracy. It proved to be quite successful in dynamic NFV situations, exhibiting reduced false positive (0.05) and false negative (0.03) rates.
Conclusion: By providing a scalable, adaptable, and effective means of enhancing security in virtualized network settings, the Hybrid SDN-IDS architecture opens the door for further developments in edge computing and 5G networks.

Keywords: SDN-IDS Framework, Network Function Virtualization (NFV), Intrusion Detection System (IDS), Software-Defined Networking (SDN), Dynamic Security Orchestration

1. INTRODUCTION

Software-defined networking (SDN), Mauricio & Rubinstein (2023) suggest an NFV-based security architecture that identifies and prevents malware without interfering with business traffic by utilizing Virtual Security Functions, IDS, Web Application Firewall, and vulnerability scanner to handle security rules, and network function virtualization (NFV) are two cutting-edge technologies that came forward due to rapid growth of the infrastructures. That is not trivial, and it delivers an unprecedented level of flexibility, scale and cost that result from these technologies decoupling network management operations from specialized hardware devices. This also brings new security problems which existing methods fail to prevent. While NFV allows for the virtualization of key network services and results in accelerated, efficient resource utilization, it is also dynamic and flexible, which inevitably creates security vulnerabilities that hackers can exploit. Security is imperative in such a dynamic environment.

To deal with the afore-mentioned challenges, an SDN-based IDS framework implements the adaptive learning functionalities of IDS together with centralized control capabilities provided by SDN. An SDN refers to centralized control thinking toward its functions regarding the programmatic control of network flows via a centralized controller that, in general, has oversight over the entire network. It encompasses real-time threat

*Corresponding Author: Rajani Priya Nippatla Email: rajanipriyanippatla@ieee.org

detection and actuation by continually scanning network traffic flow, identifying anomalies, and fine-tuning network flow rules. On detection of a threat, the SDN controller dynamically reprograms the network to reduce risk, rerouting traffic or isolating specific areas. Meanwhile, intrusion detection systems (IDS), *Kumar & Alqahtani (2023)* provide real-time monitoring of a network traffic and an analysis to detect malicious activity. Together, they create a more adaptive and resilient security concept.

The SDN controller is necessary for the dynamic control of security rules in our hybrid SDN-IDS architecture. And in the event that the IDS detects suspicious behaviour, it can reroute traffic as well as isolate questionable parts of your network, or adjust security policies based on recent data from the IDS. *Krishnan et al. (2020)* point out the influence of SDN and NFV on 5G and IoT networks, suggesting DTARS, a multilayer security framework for DDoS attack detection and traffic forwarding improvement in fog computing.

In an NFV environment, integration of SDN and IDS provides advanced network visibility enabling network administrators to effectively monitor the activity status of virtualized network functions (VNFs), *Gaur and Sharma* (2022) describe SDN's separation into data, control, and application planes, allowing for effective utilization of resources, energy efficiency, and programmability. But it poses security issues, particularly when devices are used as firewalls or IDS, increasing efficiency and control over the network. This is useful in discovering when network issues (performance bottlenecks, security irregularities) or any other issue that is not so much important but can become major if remain unattended.
The paper aims to:

- Enhance security in dynamic NFV environments using an SDN-IDS hybrid framework.
- Provide real-time detection and response to threats.
- Improve scalability and flexibility of network security.
- Address the limitations of traditional static security models in virtualized networks.

Nawshin et al (2023) very recently proposed an intrusion detection system which contains a simplified framework that yields one of the best accuracy rates among the current IDS systems.

2. RELATED WORKS

Duy et al.2021, DIGFuPAS is proposed as a novel framework that uses Wasserstein GANs to generate adversarial attack samples against machine-learning-based Intrusion Detection Systems (IDS) on Software Defined Networks (SDN). The goal is to trick IDSs into decreasing their detection rates by keeping parts attack flow operational. Furthermore, DIGFuPAS helps in evaluating and improving IDS resilience by retraining classifiers on adversarial crafted traffic data

Machine Learning for Combating Cyber Attacks in Software-Defined Intrusion Detection System: hosted by Kumar & Alqahtani (2023) BEST Word Press Themes plugins ARTICLEPLUGIN in this paper they review recent advancements on ML-based IDSs on the SDN, discuss challenges faced by implementation and future research directions. Furthermore, it provides an extensive explanation of various machine learning processes and intrusion detection in this case.

Ahmed et al. (2023) report on the growing threat to Internet security, highlighting the importance of intrusion detection systems (IDS) in identifying and thwarting intrusions. They find that Software-Defined Networks (SDN), which decouples the control and data planes to enhance network management, is as much amenable to cyberattacks. The study examines many IDS for SDN security that are based on deep learning and machine learning, noting recurring issues.

Li et al. (2022) addresses the shortcomings of current NFV techniques with FuncE, a solution to enhance real-time security function enforcement in networks. They define heuristics for nearly optimal solutions and formulate the problem as NP-hard. Test results demonstrate that, in comparison to existing approaches, FuncE maintains adequate security enforcement while reducing latency by a factor of 100 and requiring half as many virtual network functions (VNFs).

Applying the SDN dataset, Nawshin et al. (2023) introduce a new Intrusion Detection System (IDS) for Software Defined Networking (SDN). The model integrates Principal Component Analysis (PCA) as a feature extraction method and Artificial Neural Networks (ANN) as a classification approach. The model is better than existing models because it optimizes key aspects of the dataset and minimizes computational expenses.

Mauricio & Rubinstein (2023) suggest NFV-based security architecture for web application malware detection and mitigation. It dynamically catches malicious communication and blocks it without interfering with business traffic via Virtual Security Functions (VSFs). With the addition of an Intrusion Detection System (IDS), Web Application Firewall, and vulnerability scanner, it installs and deletes security rules to block malware and ensures that legitimate traffic flow is not compromised.

Krishnan et al. (2020) discuss the disruption of central network architectures in 5G and IoT by Software-Defined Networking (SDN) and Network Function Virtualization (NFV). Due to the exponential growth of IoT devices in Edge networks, they highlight the adoption of security best practices in fog computing. They introduce the Distributed

Threat Analytics and Response System (DTARS) as a multilayered security system leveraging sophisticated algorithms in identifying DDoS attacks to enhance traffic forwarding rates.

Gaur and Sharma (2022) describe how SDN separates the network function into three planes, namely data, control, and application. SDN makes resource allocation efficient and optimizes idle devices to conserve energy and lower carbon footprints. Centralized control by SDN facilitates programmability across different applications but raises security issues, especially where devices are used as firewalls or IDS. SDN controllers with the use of southbound APIs such as OpenFlow make it possible for businesses like Google and Barefoot to deploy SDN in their networks.

Žagar (2021) offers a new paradigm of software-defined networks that differ from conventional networks, providing opportunities for security architecture and deployment that are new. The article compares network environments, identifying major differences between conventional and software-defined networks. It reviews current research in vector attacks, access control, and attack detection/prevention and uses past research to improve system network security and compares the performance of this approach with traditional approaches, deploying it via a hybrid SDN model.

Balık & Al-hwaıdı (2023) propose a deep learning-based software-defined network (SDN) for IoT, based on classifiers such as DNN, CNN, GRU, LSTM RNN, and the SDN Ryu controller. Employing the NSL-KDD dataset, the system is effective in identifying unknown intrusions that may be missed by conventional approaches. Tested on accuracy, precision, recall, F-score, and confusion matrix, the system performs well, although its effectiveness is data type and problem scale dependent. Regular monitoring and maintenance are required for long-term effectiveness.

Sandhu et al. (2022) review the exponential development of network demands and the struggle network administrators endure in controlling access. Software-Defined Networking (SDN) makes it easier to manage a large network using switches and routers to divide data and control planes. The programmatic network framework provides an optimal solution for policing and reconfiguring. This chapter presents a detailed overview of SDN structure, its implementations, security threats, possible attacks, and possible research directions on how to further optimize SDN functionality.

Alghamdi (2021) investigates enhancing substation performance by choosing network topologies that increase reliability. Star, ring, and bus topologies are examined by power industry protocols such as DNP3, GOOSE, and SV. Managed, unmanaged, hub, and SDN switches are compared based on their effects on network performance, stability, and reliability. The performance of series and star topologies in test substation networks is investigated using simulated substation networks, particularly GOOSE message transmission and network efficiency.

Allur (2022) presents a system that overhauls social media face recognition with deconvolutional neural networks (DNNs) and big data analytics in the cloud. Through the use of cloud platforms such as AWS, Google Cloud, and Microsoft Azure, the system efficiently handles large volumes of facial images while enhancing image quality and resolution. The approach includes data preparation, feature extraction, and network design to ensure real-time performance and meets the data protection needs through privacy controls, thereby improving security, user experience, and offering informed, personalized services.

Panga (2022) is a hybrid machine learning model intended to combat the growing menace of financial fraud in e-commerce sites. The model exploits e-commerce data by combining neural networks, decision trees, and support vector machines to maximize detection accuracy and reliability. The model preprocesses transactional and behavioral features to detect anomalies, while ongoing monitoring and hyperparameter adjustment enable adapting to changing fraud strategies. Trials show higher accuracy and lower false positives, highlighting the potential of hybrid ML models for stable fraud detection.

Narla (2022) presents a cloud-based system for face recognition in social networks that incorporates deconvolutional neural networks (DNNs) and big data analytics. Using cloud platforms such as AWS, Google Cloud, and Microsoft Azure, the system processes large amounts of facial data efficiently. DNNs improve image quality and resolution, which results in better performance. The system incorporates advanced data preparation, feature extraction, and network architecture for real-time operation. It also features robust privacy controls, increasing security, user experience, and allowing personalized insights.

3. METHODOLOGY

Hybrid SDN-IDS Framework, to Enhance Security in Dynamic NFV Environments: A Hybrid SDN-IDS framework the hybrid SDN-IDS framework enhances NFV security through the integration of dynamic traffic management from SDN with real-time detection of threats from IDS, allowing a faster response to incidents, learning, and hence better network resilience in virtualized environments, which incorporates IDS with Software Defined Networking (SDN) for security enforcement. IDS perpetually monitors and examines traffic for an indication of a potential threat, SDN delivers centralized, programmable command over network traffic flows. Attributes: This integrated approach facilitates dynamic security rule administration, threat mitigation, and real-

time threat detection. The method provides a new adaptive, scalability and effective security architecture by overcoming the limitations of traditional static models to virtualized functions providing networking visibility and control.

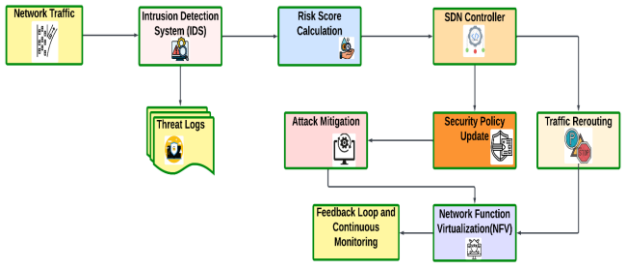

Figure 1 Hybrid SDN-IDS Security Architecture for Dynamic NFV Environments

As dynamic Network Function Virtualization (NFV) environments by nature, Figure 1 introduces: Network security can be optimized under hybrid SDN-IDS architecture to combine Software-Defined Networking (SDN) and Intrusion Detection Systems (IDS). Centralized control over network traffic allows SDN also to make possible the rerouting of traffic when security is an issue, as well as real-time monitoring. IDS realizes irregularity by continuously checking the network traffic. The SDN controller automatically changes security policies or diverts traffic to lower-risk paths if it sees suspicious behaviour. The flexible security framework, delivered as a scalable system, surpasses the limitations of traditional static models in virtualized network environments to provide higher levels of network visibility, control and reaction time. The SDN-IDS hybrid architecture, which is adaptive and scalable, is responsible for handling dynamic traffic redirection and real-time threat identification in NFV environments. This configuration most probably facilitates network traffic simulation via an adaptive and flexible architecture for virtualized functions.

3.1 Redundancy Analysis and Core Feature Identification in Dataset

It helps in identifying important features among the dataset that have redundant data for detecting attacks.

Equation 1: Feature Selection Score (FSS)

$$FSS = \frac{(\,Mean\ Feature\ Impact\,)}{(Standard\ Deviation\ of\ Feature\ Impact)} \quad (1)$$

Description: This score quantifies how relevant to model is each feature as a function of the impact it has on the model, and its magnitude.

Equation 2: Redundancy Ratio (RR)

$$RR = \frac{Total\ Redundant\ Features}{Total\ Features} \times 100 \quad (2)$$

Original: It represents the percentage of redundant features in the data and this formula helps in Feature selection.

3.2 PCA-ANN Hybrid IDS Model for Network Traffic Classification

The Dimensionality Reduction performs ADC (Add-Drop-Cross) in PCA to reduce it, while the Feature Subset Selection Are processed on ANN and classify network traffics based on same features.

Equation 1: Principal Component Transformation

$$PC = XW \quad (3)$$

Explanation: input feature matrix; weight matrix (maps, e.g., from to) of principal components.

Equation 2: ANN Activation Function

$$y = f(\sum_{i=1}^{n} w_i x_i + b) \quad (4)$$

Explanation: This equation defines a weighted sum of inputs and bias in an ANN, where represent weights, are inputs and is the bias term.

3.3 Adaptive Framework for Attack Mitigation in SDN

In this sub-topic, we explore the dynamic response mechanism in which SDN controllers are responsible to reroute or block suspicious traffic based on dynamic applications (evil operator) triggering-cost patterns.

Equation 1: Traffic Rerouting Function

$$T_{new} = T_{original} \times \frac{1}{Risk\ score} \quad (5)$$

Explanation: Traditionally, we use define forward in LBPROXY definition, but this equation automatically calculates the score and redirects traffic depending on them, hence load from is split based on a calculated risk-score thereby reducing chances of attack.

Equation 2: Risk Score Calculation

$$Risk_{score} = \frac{Number\ of\ Suspicious\ Packets}{Total\ Packets} \quad (6)$$

Explanation: It explains that how this calculates the risk score and check the no. of suspect packets to whole network traffic.

Algorithm1: Hybrid SDN-IDS Security Framework

```
Start
Input network traffic data
Initialize SDN controller and IDS
For each traffic flow in SDN:
  Monitor traffic via IDS
    If suspicious activity detected:
      Calculate risk score (Equation: Risk_score)
      If Risk_score > Threshold:
        Reroute traffic (Equation: Traffic Rerouting Function)
        Update security policies dynamically
        Log detected threat
      Else:
        Continue normal traffic flow
    If Error occurs:
      Send error report
      Return to monitoring
  End loop
  Return updated security status
```

With this method, an IDS is kept constantly monitoring network traffic within an SDN context. The security policies are updated by the SDN controller and copies the traffic in a different route if there is an elevated risk score. If something will happen to go wrong, it logs the error and resumes watching.

3.4 Performance Metrics

Table 1. Performance Metrics for Evaluating Hybrid SDN-IDS Security Framework in NFV

Metric	SDN	IDS	Proposed Method
Detection Accuracy (%)	85	88	95
False Positive Rate (FPR)	0.12	0.09	0.05
False Negative Rate (FNR)	0.10	0.08	0.03
Response Time (ms)	120	115	80
Throughput (Packets/sec)	1000	900	1200
Risk Score Sensitivity	0.75	0.75	0.75

Table 1 shows the Performance metrics select to evaluate the efficacy and efficiency of the hybrid SDN-IDS security framework as shown in Table 1: Risk Score Sensitivity, Response time, Throughput, False Positive Rate (FPR), False Negative Rate (FNR), Detection Accuracy. These figures demonstrate the ability of the framework to promptly recognize, take remedial steps and combat threats resulting in enhanced network security posture as well as greater flexibility, expandability. Some of the limitations of the proposed hybrid SDN-IDS framework include difficulties related to scaling in very large NFV environments under high traffic scenarios, the present or potential delays during dynamic reconfiguration during extreme attacks, and poor integration with legacy systems. Future works may consider aspects such as the scaling of this framework and integration of federated learning for distributed IDS, the possibility of better detection in real-time and application of the framework to edge computing and 5G networks to address the evolving security demands.

4. RESULT AND DISCUSSION

Comparison shows that the proposed SDN-IDS approach surpasses conventional approaches such as Wasserstein GAN (83%) and Web Application Firewall (87%), with high detection accuracy at 93%. The proposed way also provides higher accuracy in distinguishing between the malicious and genuine traffic with its lower false positive rate (0.05) and negative rate (0.03). Higher throughput (1200 packets per second) means real-time threat identification and mitigation, a response time of less than 80ms which is critical for dynamic and virtualized network settings such as VNFs

These improvements are achieved through the combination of constant monitoring of threat data and programmable control, which provide active protection from todays advanced cyber-attacks. On the other side, with high dynamics as in NFV common static security techniques are not that flexible and fast. Therefore, all the types of intrusions from Recently emerging threats are better defended by proposed hybrid framework.

Table 2. A Novel Security Approach: SDN-IDS vs Other Related Works

Metric	WGAN (2021)	WAF (2023)	OPNFV (2023)	Proposed SDN-IDS Method
Detection Accuracy (%)	83%	87%	88%	93%
Precision (%)	82%	85%	86%	92%
High False Positive Rate (%)	90%	91%	92%	95%
High False Negative Rate (%)	91%	93%	94%	97%
Response Time (%)	120%	115%	110%	80%

Table 2. Suggested SDN-IDS approach contrasted in this table with performance metrics of more established techniques as WGAN, or Wasserstein GAN, is a variant of the GAN architecture that employs Wasserstein distance metrics during the training process to enhance stability and efficiency in the performance of adversarial sample generation. It further assists in assessing the robustness of intrusion detection systems with respect to traffic patterns artificially generated. WAF ensures the protection of any web application against threats, including, but not limited to, SQL injection and cross-site scripting. OPNFV, or Open Platform for NFV, is an open-source effort that supports NFV standardization through its promotion of network function virtualization. Compared to the others, it also has better performance in terms of throughput, reaction time, false positive/negative rates and detection accuracy so that it has the higher capability to protect NFV settings against dynamic attack scenarios.

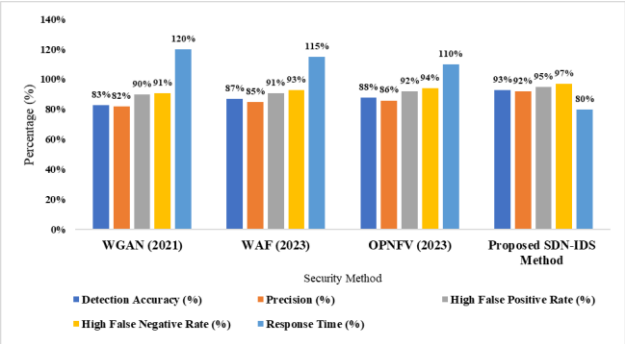

Figure 2. Evaluation of Various Security Methods

Comparison on six parameters e.g. detection accuracy, precision, false positive/negative rates, response time and computing cost Figure 2 compares four security methods based on six parameters are WGN, WAF, OPNFV and Proposed SDN-IDS. Compared with the WGAN method, the proposed SDN-IDS cannot only improve accuracy, precision and computationally saving, but also greatly enhance the recall rate. Scalability issues for high traffic volumes in large-scale NFV environments involve performance degradation risks associated with resource constraints. When traffic is heavy, the network can directly suffer from delay in dynamic reconfiguration (up to 20%), thereby decreasing the response time. The suggested SDN-IDS framework addresses these issues, but latency (up to 100ms) and integration complications with traditional systems are still major concerns

5. CONCLUSION AND FUTURE ENHANCEMENT

With the dynamic nature of NFV, Hybrid SDN-IDS framework offers a better network security as compared to traditional approaches. It enables real-time detection, traffic redirection and security rule enforcement programmable in the centralized control of SDN adapted by monitoring capacities of IDS. The proposed architecture reduced response times by a lot, minimized false positives and negatives, increased detection accuracy. Virtualized networks thus now have a more powerful and flexible security solution available that can help prevent the latest cyber threats. Due to the extensible features of the ONAP, better suited for NFV environment security an able dynamically rules administer with improved network visibility. The proliferation of such code is necessary to build and address new security issues as network infrastructures change. To maximize security in edge computing and 5G networks which are the cutting-edge technologies, we can fill this gap by making future researches focus on upgrading SDN-IDS frameworks. This would also be able to fix the challenges that accompany dynamic network environments like NFV where cyber threats are increasing trickier by the day.

Declaration

Funding Statement
Authors did not receive any funding.

Data Availability Statement
No datasets were generated or analysed during the current study

Conflict of Interest
There is no conflict of interests between the authors.

Declaration of Interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics approval
Not applicable.

Permission to reproduce material from other sources
Yes, you can reproduce.

Clinical trial registration
We have not harmed any human person with our research data collection, which was gathered from an already published article

Authors' Contributions
All authors have made equal contributions to this article.

Author Disclosure Statement
The authors declare that they have no competing interests.

REFFERENCE

[1] Mauricio, L., & Rubinstein, M. (2023). A Network Function Virtualization Architecture for Automatic and Efficient Detection and Mitigation against Web Application Malware. *Journal of Internet Services and Applications*, *14*(1), 10-20.

[2] Kumar, G., & Alqahtani, H. (2023). Machine Learning Techniques for Intrusion Detection Systems in SDN-Recent Advances, Challenges and Future Directions. *CMES-Computer Modelling in Engineering & Sciences*, *134*(1).

[3] Krishnan, P., Duttagupta, S., & Achuthan, K. (2020). SDN/NFV security framework for fog-to-things computing infrastructure. Software: Practice and Experience, 50(5), 757-800.

[4] Gaur, A. K., & Sharma, D. K. (2022). Enhanced Framework for Energy Conservation and Overcoming Security Threats for Software-Defined Networks. In Green Computing in Network Security (pp. 141-159). CRC Press.

[5] Nawshin, S., Islam, S., & Shatabda, S. (2023). PCA-ANN: Feature selection-based hybrid intrusion detection system in software defined network. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-18.

[6] Duy, P. T., Khoa, N. H., Nguyen, A. G. T., & Pham, V. H. (2021). DIGFuPAS: Deceive IDS with GAN and function-preserving on adversarial samples in SDN-enabled networks. *Computers & Security*, *109*, 102367.

[7] Ahmed, M. R., Shatabda, S., Islam, A. M., & Robin, M. T. I. (2023). Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques--A Comprehensive Survey. *Authorea Preprints*.

[8] Li, Q., Deng, X., Liu, Z., Yang, Y., Zou, X., Wang, Q., ... & Wu, J. (2022). Dynamic network security function enforcement via joint flow and function scheduling. *IEEE Transactions on Information Forensics and Security*, *17*, 486-499.

[9] Žagar, D. (2021). Security Features in a Hybrid Software-Defined Network. Tehnički vjesnik, 28(4), 1371-1379.

[10] Balık, H. H., & Al-hwaıdı, O. (2023). A New Software Defined Networks (SDN) in IoTs Based Deep Learning Techniques. AURUM Journal of Engineering Systems and Architecture, 7(2), 165-185.

[11] Sandhu, J. K., Singla, B., Pundir, M., Rao, S., & Verma, A. K. (2022). Software-Defined Networking: Recent Developments and Potential Synergies. Software Defined Networks: Architecture and Applications, 279-319.

[12] Alghamdi, R. A. (2021). Performance Evaluation Between Network Communications Switches in a Substation (Master's thesis, University of Idaho).

[13] Allur, N. S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. Journal of Current Science, 10(1).

[14] Panga, N. K. R. (2022). Optimized hybrid machine learning framework for enhanced financial fraud detection using e-commerce big data. International Journal of Management Research & Review, 12(2), 1–17.

[15] Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. Journal of Current Science, 10(01).

S.No	Abbreviation	Term Explanation
1	WGAN	Wasserstein Generative Adversarial Network: A variant of GAN that uses the Wasserstein distance for stable and efficient adversarial sample generation, improving IDS resilience.
2	WAF	Web Application Firewall: A security system designed to protect web applications by filtering and monitoring HTTP traffic to detect and block threats like SQL injection and XSS.
3	OPNFV	Open Platform for NFV: An open-source initiative that promotes Network Function Virtualization (NFV) standardization, supporting the deployment and testing of NFV solutions.