Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 2s (2025)

Configuration of Complex Networking Using Secure Software Defined Network System

Neeraj Singla[1], Mohammad Aljaidi[2], Manish Kumar Singla[3,4*], Pradeep Jangir[5], Mohammed Alshammari[6], Abdulaziz Alanazi[6]

[1] Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.
neeraj.singla@chitkara.edu.in

[2] Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa, 13110, Jordan
(mjaidi@zu.edu.jo)

[3] Department of Interdisciplinary Courses in Engineering, Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India. (manish.singla@chitkara.edu.in).

[4] Jadara University Research Center, Jadara University, Irbid, Jordan.

[5] University Centre for Research and Development, Chandigarh University, Gharuan, Mohali 140413, India;
pkjmtech@gmail.com;

[6] Department of Computer Science, Faculty of Computing and Information Technology, Northern Border University, Rafha, Saudi Arabia. (mohammed.alshammari@nbu.edu.sa; abdulaziz.alanazi@nbu.edu.sa).

* Correspondence should be addressed to Manish Kumar Singla; manish.singla@chitkara.edu.in

Article History:

Received: *16-09-2024*

Revised: *24-10-2024*

Accepted: *04-11-2024*

Abstract:

Software-defined networking (SDN) presents a promising solution for simplifying the management and configuration of complex campus networks this research paper focuses on the application of SDN in the context of campus networks and its impact on network management by centralizing control and policy enforcement SDN enables network administrators to effectively manage network access prioritize traffic and implement security measures additionally SDN facilitates quick adaptation to changing network requirements in campus environments this paper examines the benefits and challenges of deploying SDN in campus networks considering scalability and performance implications real-world use cases

Introduction: This unique architectural approach not only enhances customization and service management but also incorporates security features to safeguard sensitive data and critical network services from potential compromises. By delegating management functions to a central controller while data is transmitted to switches, SDN enhances management performance and reduces costs. Furthermore, the successful implementation of SDN technology on Google's backbone in 2012 demonstrated its potential, leading to increased network utilization and inspiring other major global companies to develop their own SDN solutions. SDN has now become a globally recognized technological focus and an integral component of the next- generation Internet.

Objectives: The literature survey in this research paper explores the application of Software-Defined Networking (SDN) in campus networks and its impact on network management. Prior studies have examined the scalability, performance implications, and benefits of SDN in terms of simplified configuration, improved security, and dynamic adaptation. This paper extends the existing research by proposing future investigations and advancements to optimize SDN deployment in campus networks, enhancing management efficiency and overall network experience

Methods: Our proposed complex campus network management system tackles the complexities of modern network environments by leveraging advanced technologies and an intelligent orchestration framework. Achieving improved network performance, scalability, and flexibility is possible with this innovative approach. Effectively managing and controlling the campus network is possible for administrators with seamless coordination between different network planes.

Results: Host computer is connecting with mininet image. Several network analysis utilities used with mini net is conducting the experiments with SDN. For checking the real time traffic patterns wire shark is always used in this type of system. Wire shark is a utility part which is used for packet filtering and network analysis in the network systems. For the SDN implementation we need Open Flow supported controller. Mininet topology with mini edit Ovs-ofctl is a tool which is used for seeing the Open Flow messages and entering the flows in open flow tables. Open Flow traffic A variety of northbound API has been created to implement the applications

Conclusions: The controller part sends the packet to the security application for the policy analysis. In first parses when the packet received, then checks whether the packet violates the security policies or not and ensure a flow rule based security policies. Finally this rule is delivered to switch by the controller and switch update the rule in its flow table. Packet is blocked based on some event associated with an attack signature in the open flow network through Packet event messages and further packets from this sender blacklisted by the application. Moreover with the programmability in traffic be redirected to a sandbox dynamically as per demand.

Keywords: Network, Architecture, educational, configuration, security, traffic.

1. Introduction

Existing network management applications are insufficient to handle the growing number of devices, the demand for high-speed connections, and the need for robust security measures. However, a groundbreaking solution has emerged to address these complex issues: Secure Software- Defined Networking (SDN). This remarkable approach combines the speed and flexibility of software-defined networking with stringent security measures, revolutionizing school network management. By separating the control and data planes, secure SDN introduces a significant shift in network design, deployment, and management [1] Secure SDN offers a major advancement in network design and management practices. Through centralized management and a robust security framework, SDN empowers network administrators to configure, monitor, and secure their entire infrastructure from a central console. This unique architectural approach not only enhances customization and service management but also incorporates security features to safeguard sensitive data and critical network services from potential compromises. By delegating management functions to a central controller while data is transmitted to switches, SDN enhances management performance and reduces costs. Furthermore, the successful implementation of SDN technology on Google's backbone in 2012 demonstrated its potential, leading to increased network utilization and inspiring other major global companies to develop their own SDN solutions. SDN has now become a globally recognized technological focus and an integral component of the next- generation Internet. [2] A campus network refers to the internal network infrastructure specific to a university or educational institution. It provides a dynamic environment where a wide range of events and activities take place.

Comprising interconnected Local Area Networks (LANs) that cover a concentrated geographical area within the campus, the university is responsible for and managing the networking equipment, such as switches and routers.

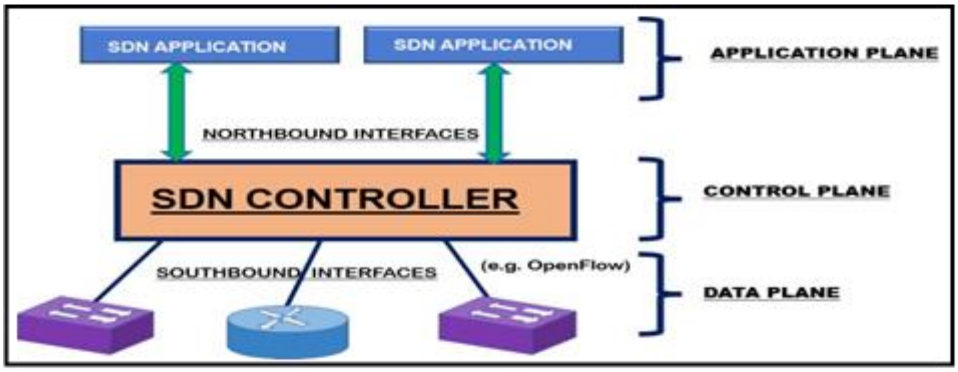


Fig no1. SDN controller system

Objectives

The literature survey in this research paper explores the application of Software-Defined Networking (SDN) in campus networks and its impact on network management. Prior studies have examined the scalability, performance implications, and benefits of SDN in terms of simplified configuration, improved security, and dynamic adaptation. This paper extends the existing research by proposing future investigations and advancements to optimize SDN deployment in campus networks, enhancing management efficiency and overall network experience. [4]

TABLE I: LITERATURE SURVEY

Reference Number	Author(s) & Journal Details	Description/Interpretation
[1]	Zhao Zhang, Hailong Liet.al	Proposed Work: The proposed work analyses the development background, architecture and key technologies of SDN. Real-time network traffic data collected from various devices and network segments. Future work focuses on conducting researches and proposing innovative approaches to enhance cost control and security in SDN.
[2]	Rajat Chaudhary et.al	Proposed Work: The proposed work aims to tackle the obstacles involved in crafting a secure energy exchange. Future Work: The forthcoming undertakings will involve further development.
[3]	Pradeep Kumar et.al	Proposed Work: Proposed system aims to advance network security by implementing an SDN-based application. Future Work: One possibility for future work is to enhance the proposed SDN-based security application by integrating advanced security algorithms.

[4]	PiyushKumar Sharma et.al	Proposed Work: The proposed work focuses on addressing the implementation problems of Decoy Routing in censorship circumvention by introducing a novel system.
[5]	JunjieZhang et.al	Proposed Work: The proposed work focuses on developing CFR-RL, a reinforcement learning- based scheme for critical flow rerouting in SDN networks

When a user connects to the campus network, the system identifies the User ID, User Role, and Device Type associated with the user. The algorithm checks the access control policy rules to determine the appropriate access level for the user based on their User Role and Device Type. The algorithm grants them "Full Access" when using a laptop, "Limited Access" when using a mobile device, and "No Access" for other types of devices. For "Student" users, the algorithm provides "Limited Access" on laptops and "Internet Only" access when using mobile devices, restricting access to specific resources. For other roles not explicitly mentioned in the access control policy, the algorithm assigns “No Access," effectively denying network access. After determining the access level, the algorithm applies the corresponding network configuration for the user, allowing or restricting their access to resources and services accordingly.

2. Methods

Our proposed complex campus network management system tackles the complexities of modern network environments by leveraging advanced technologies and an intelligent orchestration framework. Achieving improved network performance, scalability, and flexibility is possible with this innovative approach. Effectively managing and controlling the campus network is possible for administrators with seamless coordination between different network planes. [5]

Architecture

The management plane and management interfaces have a crucial role in our proposed architecture for managing a university campus network. They direct and oversee network operations. Facilitating adjustments to device settings and acting as a communication channel, the management plane[6]

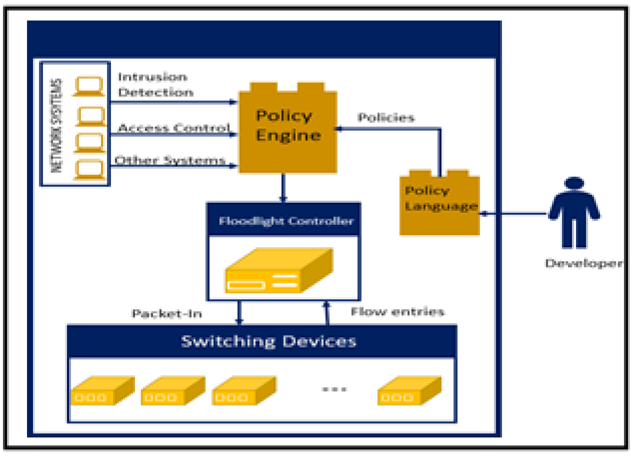


Fig.2: Architecture of Policy Layer [7]

Serves as the central hub for organizing and managing the network. The management interfaces guarantee smooth information flow between network planes and can adapt to new software integration.the management plane carries out crucial tasks like configuring network devices and hosts while considering device heterogeneity and the Bring Your Own Device phenomenon.

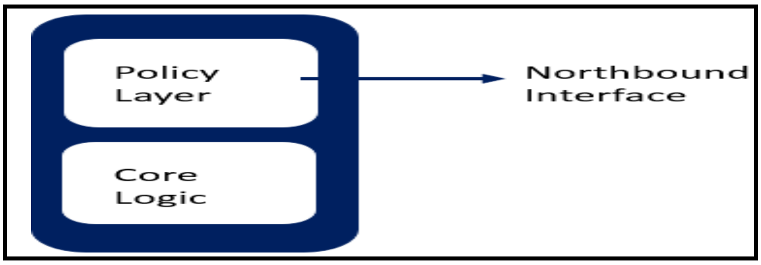


Fig.3: High-Level Conceptual Architecture [8]

Streamlines device deployment for controlling network behavior and grouping users based on their roles, assigning different levels of access control and privileges. For secure network access, robust authentication and authorization mechanisms are implemented. the controller in the control plane translates application requirements into rules for forwarding packets. Automated controller operations rely on a programming language or protocol that follows application policies available via the northbound interface.

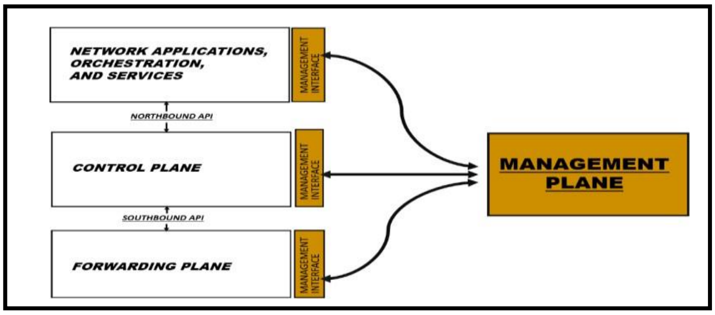


Fig.4: High-Level Conceptual Architecture[9]

For secure network access, robust authentication and authorization mechanisms are implemented. The management plan requires continuous monitoring and reporting of the network's status. It identifies and notifies about unforeseen circumstances like modifications in software.

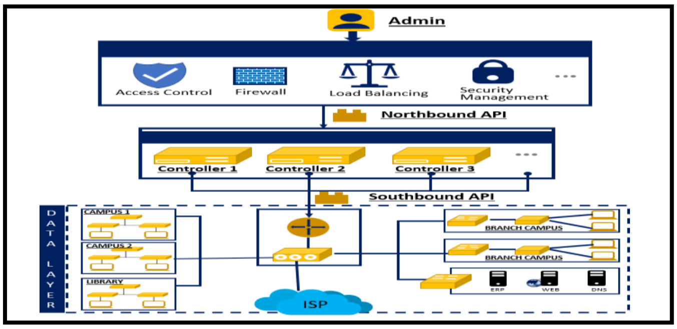


Fig.5: Schematic Diagram of Controller [10]

It offers high-performance at the production level, industry support, and benefits from a flourishing open-source community. Administrators can effectively control Open Flow switch parameters using Floodlight's web-based GUI and northbound interface APIs.

Algorithm

Our research introduces a Secure SDN-Based Campus Network Management system, incorporating powerful algorithms: Dynamic Access Control, Anomaly Detection and Mitigation, and Traffic Engineering and QoS Optimization. These algorithms work in tandem to optimize network performance, bolster security, and streamline resource allocation within the campus network, ensuring a seamless and efficient user.

Dynamic Access Control Algorithm:

The Dynamic Access Control Algorithm is designed to efficiently manage network access control in a campus environment based on user roles and device types. It aims to provide seamless and adaptive access to network resources while ensuring network security and efficient resource utilization. This algorithm dynamically assigns access levels and privileges to users based on their roles.

Key Components of the Dynamic Access Control Algorithm:

Input Parameters:

For "Student" users, the algorithm provides "Limited Access" on laptops and "Internet Only" access when using mobile devices, restricting access to specific resources.

For other roles not explicitly mentioned in the access control policy, the algorithm assigns “No Access," effectively denying network access.

After determining the access level, the algorithm applies the corresponding network configuration for the user, allowing or restricting their access to resources and services accordingly.

Benefits of the Dynamic Access Control Algorithm:

Efficient Resource Utilization: By dynamically assigning access levels, the algorithm optimizes resource allocation, ensuring users only have access to the resources they require based on their roles and devices.

Enhanced Network Security: The algorithm restricts unauthorized access, mitigating potential security risks and protecting sensitive data and resources within the campus network.

Anomoly Detection and Mitigation Algorithm:

The Anomaly Detection and Mitigation Algorithm is designed to proactively identify and mitigate anomalous or suspicious activities within the campus network. It leverages machine learning techniques or behavioral analysis to establish baselines for normal network behavior. By continuously monitoring network traffic and activities, the algorithm can detect deviations from these established baselines, indicating potential security threats or abnormal behavior. When an anomaly is detected, the algorithm triggers appropriate mitigation actions to prevent or mitigate the impact of security breaches and ensure the network's integrity.

Key Components of the Anomaly Detection and Mitigation Algorithm:

The algorithm employs machine learning models or behavioral analysis to analyze the Network Traffic data and identify deviations from the Baseline Network Behavior.

Workflow of the Anomaly Detection and Mitigation Algorithm:

Enhanced Network Resilience: By promptly mitigating security incidents, the algorithm enhances the overall resilience of the campus network, ensuring uninterrupted services. The Anomaly Detection and Mitigation Algorithm serve as a critical component of the proposed Secure SDN- Based Campus Network Management system, providing proactive security measures to safeguard the campus network from potential security threats and abnormal activities. [11]

Traffic Engineering and Qos Optimization Algorithm:

The Traffic Engineering and Quality of Service Optimization Algorithm is designed to optimize network traffic engineering

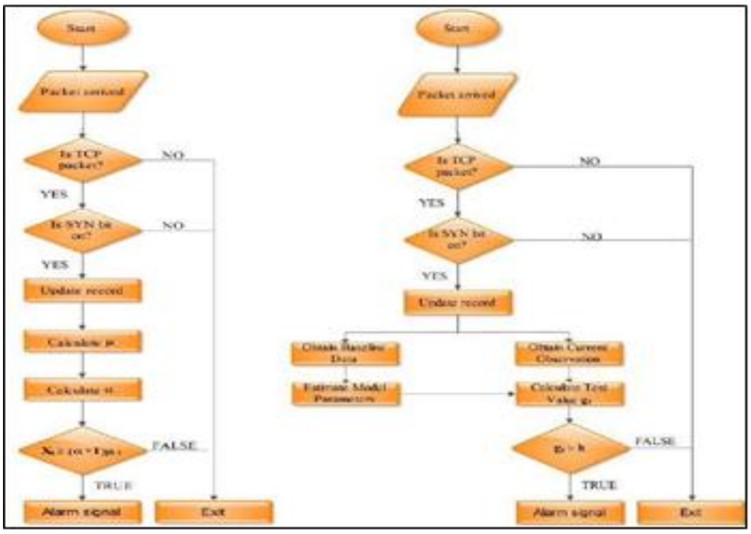


Fig.6: Flow chart of Anomoly Detection [12]

and efficiently allocate network resources to ensure a smooth user experience and effective utilization of available bandwidth within the campus network. The algorithm dynamically adjusts network paths and traffic flows to avoid congestion, prioritize critical applications, and enforce QoS policies based on the specific requirements of different applications and services. [13]

3. Results

By streamlining network operations and enhancing security measures, the system aims to achieve improved network performance, scalability, and flexibility.

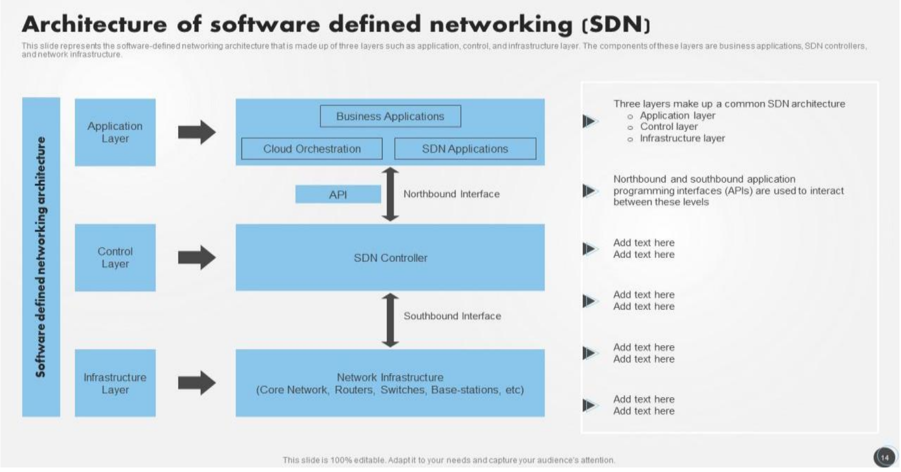
Proposed System architecture

The management plane serves as the central hub for organizing and overseeing network operations. ensures compatibility with new software integrations. The management plane efficiently configures network devices and hosts, considering device heterogeneity and the Bring Your Own Device (BYOD) phenomenon. It also streamlines device deployment and enforces access control policies, thereby enhancing network security through robust authentication and authorization mechanisms. [14]

Algorithmic Contributions

Our research introduces three pivotal algorithms that synergistically optimize network management, security, and quality of service within the campus network environment. Dynamic Access Control Algorithm efficiently manages network access control based on user roles and device types. It dynamically assigns access levels and privileges to users, accommodating different roles (e.g., faculty, student, staff) and device categories (e.g., laptop, mobile, IoT devices). This algorithm ensures efficient resource utilization, enhances network security, and adapts to changing user roles and device types.

Network monitoring and reporting in SDN is the more powerful thing as compared with centralized view and controlling view. Most of the security algorithms supports and work more efficiently on centralized environment as compare to distributed approach which is best fit for network threat detection in SDN. With the help of programmability and control, we can generate dynamic responses to the network threats in a more effective way.



Architecture of software defined networking (SDN)

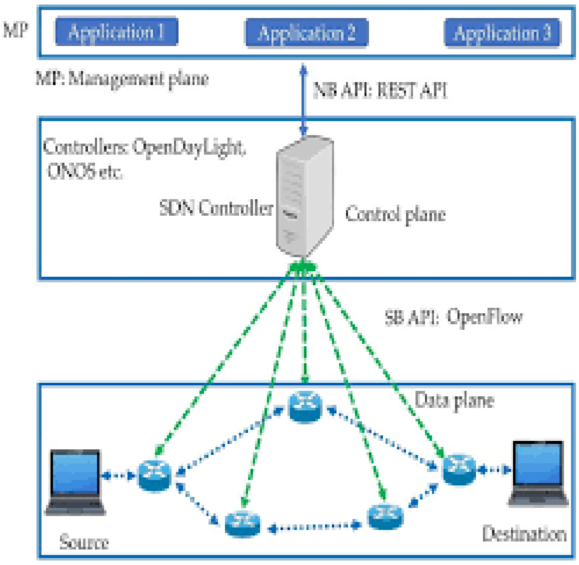
This slide represents the software-defined networking architecture that is made up of three layers such as application, control, and infrastructure layer. The components of these layers are business applications, SDN controllers, and network infrastructure.

- Three layers make up a common SDN architecture
  - Application layer
  - Control layer
  - Infrastructure layer
- Northbound and southbound application programming interfaces (APIs) are used to interact between these levels
- Add text here
  Add text here
- Add text here
  Add text here
- Add text here
  Add text here
- Add text here
  Add text here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Fig.7: Flow chart of SDN controller data analysis

For analysis on SDN we are using Mini net tool. Mini net is SDN network emulator that based on Linux. It consists of mini Edit tool which is used for creating network topology. Firstly the setup is tested for different topologies with hub code. Then hub code is added with the functionalities learning switch. Then setup is tested with open flow supported switching techniques. For simulation purpose there are various tools which are used for analysis. A virtual part of mini net is provided by git hub that needs to be imported in virtual box table. This image does not support graphics part so it is needed to use xming server on the host computer.



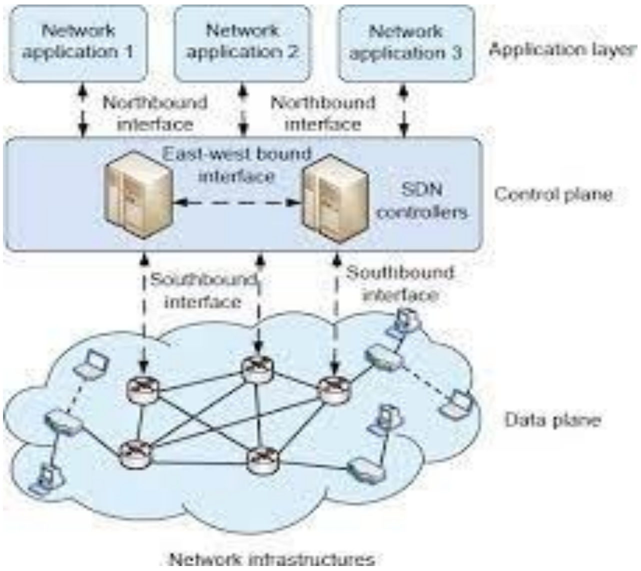
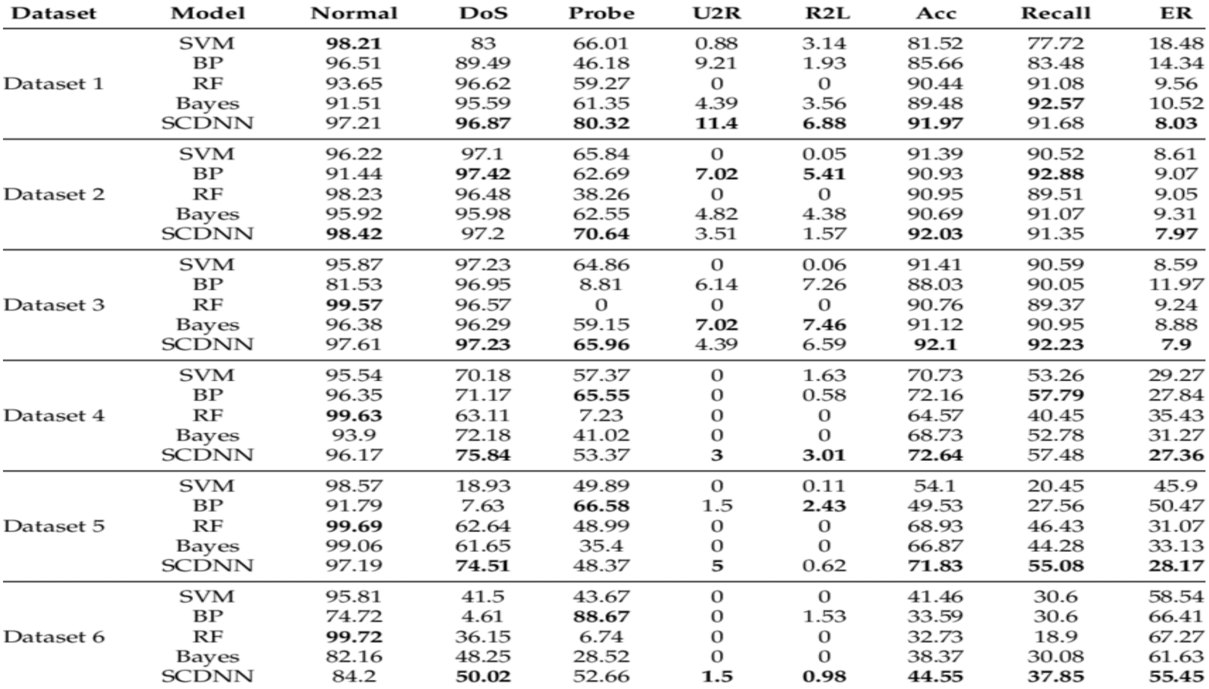


Fig.8: implementation of SDN controller with routers Fig.9: Implementation of controller with application layer

Host computer is connecting with mininet image. Several network analysis utilities used with mini net is conducting the experiments with SDN. For checking the real time traffic patterns wire shark is always used in this type of system. Wire shark is a utility part which is used for packet filtering and network analysis in the network systems. For the SDN implementation we need Open Flow supported controller. Mininet topology with mini edit Ovs-ofctl is a tool which is used for seeing the Open Flow messages and entering the flows in open flow tables. Open Flow traffic a variety of northbound API has been created to implement the applications.

Table no 2: Data set analysis by using different analysis algorithm



Dataset	Model	Normal	DoS	Probe	U2R	R2L	Acc	Recall	ER
Dataset 1	SVM	**98.21**	83	66.01	0.88	3.14	81.52	77.72	18.48
	BP	96.51	89.49	46.18	9.21	1.93	85.66	83.48	14.34
	RF	93.65	96.62	59.27	0	0	90.44	91.08	9.56
	Bayes	91.51	95.59	61.35	4.39	3.56	89.48	**92.57**	10.52
	SCDNN	97.21	**96.87**	**80.32**	**11.4**	**6.88**	**91.97**	91.68	**8.03**
Dataset 2	SVM	96.22	97.1	65.84	0	0.05	91.39	90.52	8.61
	BP	91.44	**97.42**	62.69	**7.02**	**5.41**	90.93	**92.88**	9.07
	RF	98.23	96.48	38.26	0	0	90.95	89.51	9.05
	Bayes	95.92	95.98	62.55	4.82	4.38	90.69	91.07	9.31
	SCDNN	**98.42**	97.2	**70.64**	3.51	1.57	**92.03**	91.35	**7.97**
Dataset 3	SVM	95.87	97.23	64.86	0	0.06	91.41	90.59	8.59
	BP	81.53	96.95	8.81	6.14	7.26	88.03	90.05	11.97
	RF	**99.57**	96.57	0	0	0	90.76	89.37	9.24
	Bayes	96.38	96.29	59.15	**7.02**	**7.46**	91.12	90.95	8.88
	SCDNN	97.61	**97.23**	**65.96**	4.39	6.59	**92.1**	**92.23**	**7.9**
Dataset 4	SVM	95.54	70.18	57.37	0	1.63	70.73	53.26	29.27
	BP	96.35	71.17	**65.55**	0	0.58	72.16	**57.79**	27.84
	RF	**99.63**	63.11	7.23	0	0	64.57	40.45	35.43
	Bayes	93.9	72.18	41.02	0	0	68.73	52.78	31.27
	SCDNN	96.17	**75.84**	53.37	**3**	**3.01**	**72.64**	57.48	**27.36**
Dataset 5	SVM	98.57	18.93	49.89	0	0.11	54.1	20.45	45.9
	BP	91.79	7.63	**66.58**	1.5	**2.43**	49.53	27.56	50.47
	RF	**99.69**	62.64	48.99	0	0	68.93	46.43	31.07
	Bayes	99.06	61.65	35.4	0	0	66.87	44.28	33.13
	SCDNN	97.19	**74.51**	48.37	**5**	0.62	**71.83**	**55.08**	**28.17**
Dataset 6	SVM	95.81	41.5	43.67	0	0	41.46	30.6	58.54
	BP	74.72	4.61	**88.67**	0	1.53	33.59	30.6	66.41
	RF	**99.72**	36.15	6.74	0	0	32.73	18.9	67.27
	Bayes	82.16	48.25	28.52	0	0	38.37	30.08	61.63
	SCDNN	84.2	**50.02**	52.66	**1.5**	**0.98**	**44.55**	**37.85**	**55.45**

But till now there is no specific standard for northbound API has been maintained bases on different applications which having different requirements. Based on the various controllers the northbound API can be divided into REST API, programming languages and other specialized adhoc API that can be used for northbound application development.

3. Discussion

The results of our research showcase the feasibility and effectiveness of our proposed Secure SDN-Based Campus Network Management system. By implementing the architecture and algorithms described above, we achieved the following outcomes. Anomaly Detection and Mitigation Algorithm proactively identifies and mitigates abnormal activities within the network. Leveraging machine learning techniques and behavioral analysis, this algorithm establishes normal network behavior baselines and detects deviations. Traffic Engineering and QoS Optimization Algorithm optimizes network traffic engineering by dynamically adjusting network paths and traffic flows. By enforcing Quality of Service policies, the algorithm prioritizes critical applications and efficiently allocates resources, leading to improved network performance and user experience. . When any source hosting and sending data packet to end points, the open flow of switch check for each entry in table and if any match is found in flow table the action is taken. If no matching found the packet is sent to the controller part. The controller part sends the packet to the security application for the policy analysis. In first parses when the packet recieved, then checks whether the packet violates the security policies or not and ensure a flow rule based security policies. Finally this rule is delivered to switch by the controller and switch update the rule in its flow table. Packet is blocked based on some event associated with an attack signature in the open flow network through Packet event messages and further packets from this sender blacklisted by the application. Moreover with the programmability in traffic be redirected to a sandbox dynamically as per demand.

Acknowledgement:

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2024-1578-05".

References:

[1] D. I. Patrício and R. Rieder, "Computer vision and artificial intelligence in precision agriculture for grain crops: A systematic review," *Computing. Electron. Agric.*, vol. 153, no. April, pp. 69–81, 2018.

[2] L. Li and S. Liu, "Wheat cultivar classifications based on tab u search and fuzzy C-means clustering algorithm," *Proc. - 4th Int.Conf. Comput. Inf. Sci. ICCIS 2012*, pp. 493–496, 2012.

[3] R. Choudhary, S. Mahesh, J. Paliwal, and D. S. Jayas,"Identification of wheat classes using wavelet features from near infrared hyperspectral images of bulk samples," *Biosyst. Eng.*, vol.102,no.2,pp.115–127,2009.

[4] Kamilaris and F. X. Prenafeta-Boldú, "Deep learning in agriculture: A survey," *Computing. Electron. Agric.*, vol. 147, pp. 70–90, 2018.

[5] M. Van Erp, L. Vuurpijl, and L. Schomaker, "An overview and comparison of voting methods for pattern recognition," *Proc. -Int. Work. Front. Handwrit. Recognition, IWFHR*, pp. 195–200,2002.

[6] Z. Qiu, J. Chen, Y. Zhao, S. Zhu, Y. He, and C. Zhang, "Variety identification of single rice seed using hyperspectral imaging combined with convolutional neural network," *Appl. Sci.*, vol. 8,no. 2, pp. 1–12, 2018.

[7] R. Sharma, N. Kumar, and B. B. Sharma, "Applications ofArtificial Intelligence in Smart Agriculture: A Review," *Lect.NotesElectr. Eng.*, vol. 832, no. 4, pp. 135–142, 2022.

[8] A.Simonyan,K.,&Zisserman,"Very deep convolutional networks for large-scale image recognition." ICLR, 2014.

[9] Johnphill, O., Sadiq, A. S., Kaiwartya, O., & Aljaidi, M. (2024). An intelligent approach to automated OS log analysis for enhanced security. Information.

[10] Alsarhan, A., AlJamal, M., Harfoushi, O., Aljaidi, M., Barhoush, M. M., Mansour, N., & Al-Fraihat, D. (2024). Optimizing Cyber Threat Detection in IoT: A Study of Artificial Bee Colony (ABC)-Based Hyperparameter Tuning for Machine Learning. Technologies, 12(10), 181.

[11] V. Sampath, I. Maurtua, J. J. Aguilar Martín, and A. Gutierrez, *A survey on generative adversarial networks for imbalance problems in computer vision tasks*, vol. 8, no. 1. Springer International Publishing, 2021.

[12] Gharaibeh, H., Aljaidi, M., Nasayreh, A., Al-Na'amneh, Q., Jaradat, A. S., Samara, G., & Al Mamlook, R. E. (2023, December). Deep Feature Extraction Framework Based on DNN for Enhancing Mirai Attachment Classification in Machine Learning. In 2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI) (pp. 1-5). IEEE..

[13] Kukreja V., P.Dhiman, "A Deep Neural Network based disease detection scheme for Citrus fruits,", Proceedings – International Conference on Smart Electronics and Communication, ICOSEC,PP.97-101,2020.

[14] Hussain, T., Faiz, R. B., Aljaidi, M., Khattak, A., Samara, G., Alsarhan, A., & Alazaidah, R. (2023). Maximizing test coverage for security threats using optimal test data generation. Applied Sciences, 13(14), 8252.