International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 24s, 2025
https://theaspd.com/index.php

Exploring the Challenges and Vulnerabilities of Software-Defined Networking (SDN) In Campus Network Security

Armie C. Ibay[1]
[1]Western Philippunes University, armie.ibay@wpu.edu.ph

Abstract– *Today, Campus networks face unprecedented challenges in terms of scalability, security and performance wherein traditional network architecture is striving hard to achieve this goal. This systematic review evaluates Software-Defined Networking (SDN) as a transformative solution to centralized yet dynamic network control and management and increased operational efficiency for an academic institution. Software-defined networking (SDN) decouples the control and data plane, making it possible to make real-time changes and quick reconfigurations to optimize traffic flow and minimize problems such as latency and packet loss. This flexibility comes along with vulnerabilities notably in central control points susceptible to Distributed Denial of Service Attacks (DDoS) and the spreading of malware which requires robust security measures. With the integration of artificial intelligence (AI) into SDN, it can strengthens intrusion detection and it also opens the floodgates for vulnerabilities and heightens the risk of cyberattacks. Strategies to mitigate these problems include the use of multiple controller clusters, load-balancing architecture, and federated learning for privacy-preserving intrusion detection. This paper shows that the academic institution should adopt strict and proactive security measures and monitoring to protect against cyber threats through the implementation of SDN since it emphasizes scalability and resilience. SDN can also transform network administration efficiently.*

Keywords– *SDN Challenges in Campus Network, SDN Challenges, SDN Vulnerabilities in Campus Network, Software-Define Networking Vulnerabilities, Challenges in Software-Define Networking*

I. INTRODUCTION

Universities are swiftly embracing digital solutions in the era of digitization, making it essential to acquire knowledge on the subject as well. As the cloud and virtualization take over, the demand for smooth connectivity has risen to a stage which traditional networking systems are now proving insufficient in their operations. The growing new technology trends in Mobile Communication and Internet Technology cause a fleet growth of systems; smart solutions are obviously required or network complexity is preferred (I. A. Mahar et al., 2024).

Campus networks form the very core of university life and are coming under more intense pressure to maintain pace with burgeoning requirement. When it comes to the control planes managing these huge networks and increasing complexity, there is a clear challenge emerging with traditional static systems looming on high. In addition to the number of users that roam around on campus from students, admin etc., this leads more proper and dynamic as well as automated network management solutions (S. Karnani & H. K. Shakya, 2021). However, many learning institutions are still stuck with old ways of doing things by having to configure each piece of hardware such as firewalls and routers which becomes problematic at scale in terms scaling onboarding, traffic management as well as failover (T. Shanmugam & B. Malarkodi, 2019). Some common challenges such as packet loss, jitter and latency can also influence a bad network performance however upgrading bandwidth throughput and infrastructure might mitigate the challenge (Ojugo & Eboka, 2020).

Campus networks are also subject to a lot of data traffic that can either make performances slow, or more seriously makes them bypass the security measures leading to damage of institution (Deepak Nadig & Byrav Ramamurthy, 2019). Cyber threats are formidable within tertiary institutions, given the vast volumes of sensitive data processed by these entities which require heavy safeguarding (K. Rusere & E. K. Ngassam, 2020).

One feasible answer to these problems is Software-Defined Networking. Because of its flexibility and software-based nature, the technology is making major inroads into campus networks. The first is decentralized control, meaning that reconfiguration may require to manually access multiple network switches and this will makes harder or need more effort throughout the way of putting a security in place. SDN simplifies network complexity and helps improve operational management so SDN can help to make networks more agile in response to new threats as well (Guo et al., 2021). SDN differentiator: The control plane of the network is decoupled from its data planes, enabling an SDN to be managed

independently so that changes can appear programmatically in seconds or at wired speed – enhancing overall security (Guo et al., 2021).

SDN is associated with certain strengths, but there are issues that still resist its practical deployment. For example, the SDN controller can be a target for attackers using Distributed Denial of Service attacks or can bypass weak authentication standards to penetrate the system which leads to unauthorized access to sensitive information and disruption of services (Chatterjee & Rawat, 2024). Furthermore, the introduction of Artificial Intelligence (AI) to the SDN allows for more advanced features of the network but it also makes the network vulnerable to higher caliber cyber attacks (Yogita, Hande, Rupali, & Vairagade, 2024).

Sometimes the security challenges that come with SDN can outweigh the pros that come with it. The central controller which is an essential part of SDN is very susceptible to passive and active attacks such as DDoS attacks (Ali, et al., 2024). These risks imply that there is a need to use strong policy management together with intrusion detection systems and correct firewalls so as to make SDN networks secure (Ali et al., 2024). This is because as SDN technologies progress with OpenFlow, it is necessary to improve security guarantees to prevent the known vulnerabilities from being exploited (Gui, 2023).

Despite these problems, SDN is an attractive solution for enhancing security in campus network. By offering its adaptable, cost-efficient management through its centralized governance that suitably separate control and data planes for precise oversight and reduce for human error (Hill et al, 2024). However, it doesn't ensure the execution of the right solution, and such a risk should not be ignored. An anticipatory approach is critical in dealing with the complexities involved in SDN security.

This work proposes to explore and map out the challenges and vulnerabilities coupled with the implications SDN carries, without compromising the security in a campus network. Identify best practices and strategies deployed toward mitigating these challenges and vulnerabilities identified.

II. Related Works

2.1. Challenges of SDN in Campus Network Security

The research study mainly of M.A. Abir et al (2023) deals with the problems created regarding scalability and performance levels of the networks. The problem discussed in this article incorporates the problems that have cropped up as a result of scarce spectrum of RF and the rising necessity for data rates. With increasing demands for data, the radio frequency spectrum has become congested and ineffective, which makes it scarce and limited. The fast development in terms of the number of users and their requirement of data has made (M. A. Abir et al, 2023) postulate that the current demand in network communication has significantly forced the optimization of the finite radio frequency spectrum. Traditionally designed systems are non-changeable rigid hardware-based constructions and tend to introduce problem aspects connected to adjustment, extensibility and flexibility (D.A. Assreshey et al. 2022). This means that the integration of unstable loads is, indeed strongly correlated with elevated costs of operation and diminished performances even if the growth in network traffic is interacting with unstable loads.

The operating costs have increased and the demands for infrastructure in the last few years, making many complexities attached to traditional network management (O. David et al, 2023). Moreover, because it is hard for the conventional IP network management due to vendor-specific commands, it even decreases operational flexibility, increases the risk of mistakes and inefficiencies while enhancing the risk of inefficiency and thus decreases efficiency as well (S. Neelavathy Pari et al., 2023). According to Udo et al. (2020), the process of manual configuration of network devices is the most cumbersome, error-prone, and time-consuming process.

Even though centralized controllers make some of the administrative load easier, they also create single points of failure. In order to effectively administer big campus networks, it is required to implement high-level regulations that are flexible.

In the context of scalability and computational power, there are relevant issues that involve typical characteristics of classical networks along with novel security concepts like Intrusion Detection Systems. (M. Raza et al., 2024) proposed that IDS is strongly challenged by the need to balance contradictory requirements of data sovereignty and privacy. Although federated learning systems are proven to overcome the above-mentioned challenges, they are tied to the available resources and therefore come with high communication costs, which makes scalability a highly complex activity. In an exploratory study, M. Blose et al (2024) found out that the problems related to the issue of scalability can impact software-defined networking environments too. This comes in because most of the controllers do not have enough processing capabilities to handle efficiently the augmenting demand on the network infrastructure.

As the burden of big network complexity that SDN controllers have to deal, the utilization of multiple SDN controllers in a clustered architecture could possibly enhance scalability and accelerate network control plane processing (M.-H. Cheng et al., 2023). But since cost versus processing power are at odds with each other, it only serves to exacerbate the inequalities in the fundamental metrics that are load balancing, energy efficiency, and reliability (B. Isong et al, 2020). The reason is that the two elements are at such odds with each other that all it does is highlight the differences. Fault tolerance is a major issue in Software-Defined Networks (SDNs) as N. G. and A. M. (2023) state. A new design can only be considered acceptable if it can be proven to be fault tolerant.

As indicated in the study of S. Karnani and H. K. Shakya (2021), they explained that as the networks evolve the more it becomes ineffective with the current static load balancing methods. This is due to the inability of these approaches to cope to the ever evolving demands of an increasing number of network users and applications.

With the growth of mobile devices and Internet of Things (IoT) applications on campus networks, new wireless connectivity solutions that are more agile and scalable must be developed as W. Brockelsby and R. Dutta (2023) state. S. Karnani and H. K. Shakya (2023) write that the move from traditional learning to distance learning has been a difficult one for network administrators to manage, authenticate, and keep available. That is all made a lot harder due to the transition from the regular learning to learning through distant means.

2.2 Vulnerabilities of SDN in Campus Network Security

Software defined networking (SDN) integration of data plane and control is flexible for network administration however the network becomes exposed to security flaws. A. H. Abdi et al. (2024) found that this convergence might leave weak parts of both domains open to hackers control.

This means that the security of the whole network is at stake. This means that if we're putting all the network control inside software defined networking (SDN), we increase the point of failure a thousand times, says W. P. Rey (2023), doubling the risk of security vulnerabilities. If the main controller is breached, most of the network could be affected; as such, various strong defensive mechanisms have to be adopted to protect the system.

In addition, B. Ahmed, et al. (2020) study consider that SDN is very susceptible to denial-of-service (DDoS) attacks and even more prone to attack if the attackers have access to the network rules. Therefore, this is another threat with SDN.M. W. Nadeem et al. (2023) extend their concern noting that the centralization nature of SDN also raises privacy and security concerns and raises concerns about distributed denial of service (DDoS) attacks. The problem with the SDN design is the possibility of having a single point of failure, and if the controller is compromised then the entire network is screwed.

SDN has modernized network management in a number of ways; however, it has also brought some security concerns to the fore. Denial of service attacks can be easily executed, especially in the context of SDN, which greatly deters the use of SDN based architectures. Accordingly, enhanced security controls are warranted.

2.3 Proposed Strategies to Mitigate Identified Challenges/Vulnerabilities

2.3.1 Performance and Scalability in SDN

The modern networking framework prioritizes both operational efficiency and scalability, utilizing diverse strategies to realize these aims. According to M. A. B. S. Abir et al. (2023), the implementation of multiple antenna systems is crucial for augmenting receiver signal strength, which in turn optimizes network performance in contexts where the radio frequency spectrum is restricted and applications necessitate elevated data transmission rates. This is the core network optimization component allowing data packets to be carried across SDN frameworks with almost zero latency.

Cheng et al. (2023) investigate the challenges associated with scaling in Software-Defined Networking (SDN) utilizing an open-source Management and Orchestration (MANO) framework that is integrated with OpenStack. This approach improves the adaptability and reliability of SDN controllers, facilitating a more efficient distribution of system workload across a cluster. What this research concludes is the requirement for adaptable systems within networked environments to maintain the dynamic demands across those systems. Blose et al. (2024) employs a hybrid architecture that includes switching which it utilizes for scalability enhancement with machine learning methodologies meant for achieving optimum network efficiency along with minimal response time. In this respect, it falls into the theme of "smart" technology, where the principle behind the network's improvement all the time ensures optimum, real-time responsiveness.

2.3.2 Security Enhancements through SDN

One of the very fast-emerging areas of research is applying SDN technology to network security. Actually, S. Neelavathy Pari et al. (2023) have proposed a framework using artificial intelligence technique in software-defined networking for assessment and detection of flooding attacks on the network. It also demonstrates the proactive security model where total network protection can be significantly enhanced through the real-time observation and analysis of data traffic. At the same time, this underlines the role of artificial intelligence in making customary security elements in the SDN paradigm stronger.

A. H. Abdi et al. (2024) has conducted a survey of vulnerabilities that exist both in the data and in the control planes of SDN, and after identifying the related security issues, has presented some future research directions. Being parallel to the findings of B. Ahmed et al. (2020), the current paper also shares the same similarities. Specifically, authors investigate how easily DDoS attacks may be launched on Software-Defined Networking exploiting existing policy configurations. Beyond that, adaptive policy parameterizations are furnished as one possible strengthening of such defenses against such attacks and thereby methodologies to find these properties are proposed. This paper focused on analyzing DDoS attacks on distributed systems and heavily underlined the use of a distributed controller coupled with verification mechanisms that ensure security in SDN architectures. This further strengthens the case for the implementation of strong and highly secure structures negating incoming intelligent threats (M. W. Nadeem et al., 2023).

In reference to A. H. Abdi et al. study in 2024 he pointed out a few important areas that should be targeted for more research in consideration of new security threats. Supported by the findings made by B. Ahmed, et al (2020) in which they explore the susceptibility of Software-Defined Networking (SDN) to Denial of Service attacks (DDos), amongst other things through those which exploit control policy configurations. For such, they propose fingerprinting techniques and continue by suggesting that one approach to making such systems more resistant to DoS attacks could be through the inspection of the dynamic settings of policies.

2.3.3 Management and Flexibility

SDN or software-defined networking finds its reasons in making networks more efficient and secure. According to D. A. Assreshey et al. (2022), there is an urgent need for shift from conventional non-SDN frameworks into SDN-supportive frameworks. While flexibility along with governance is possible through SDN, it may not be necessary to do away with everything in totality. The organizations that have planned to upgrade their networking systems in an interrupted manner require such an extent of adaptability.

Apart from that, Udo, E. et al. (2020) concluded that traditional network management is a complex task loaded with several problems including human error during manual configurations and inherent vulnerabilities found within centralized systems. They recommend up gradation of management techniques to match the change in needs of the network through up-gradation of campus networks with software defined networking architectures to make them manageable.

S. Karnani and H. K. Shakya (2021) had proposed the usage of advanced load balancing and framework using software-defined networking for campus networks. Since the demand for users as well as application requirements is increasing, the network needs to be monitored in a dynamic, elastic, and flexible manner to meet user as well as application demands.

2.3.4 Fault Tolerance and Infrastructure Development

Network services reliability plays an important role in the discourse of fault tolerance in Software-Defined Networks (SDNs). N. G and A. M. (2023) delve these challenges and encourages improved techniques for the detection and correction of failure. This research only emphasizes the need for a robust infrastructure that can continue to perform if in case face potential adversities.

W. P. Rey, (2023) discusses the design and implementation of MidwestCloud, a centralized control plane using SDN to try to overcome the weaknesses of centralized control. This system attempts to provide a scalable, fault-tolerant, and adaptive networking fabric using SDN technologies to support automation and resource management.

Considering this, it remains imperative to develop resilient systems capable of enduring the demands of contemporary networking. As articulated by W. Brockelsby and R. Dutt (2021), enhancing the cybersecurity framework of university networks is essential. The strategic arrangement of hardware and software data planes augments overall functionality.

This study offers a solution for issues that are associated with managing networks at educational institutions. As becoming more capable to protect against an increased number of new discovered vulnerabilities with providing the faster speed and the overall higher throughput business will make it possible thanks to such modern designs like SDN and AI.

III. METHODOLOGY

This systematic literature review's (SLR) purpose is to summarize and present all the information from the literature in the field of study in a logical and coherent manner. Also, a systematic literature review would help to find the present gaps in research and therefore the possible directions that future research may take. This section delineates the methodology used to execute this systematic literature review (SLR). This included research questions (RQ), search strings, data sources, criteria for inclusion and exclusion, screening and selection processes, data extraction and analysis.

3.1. Research Question

This is to review the different academic literature from IEEE Xplore, ACM Digital Library, SpringerLink to analyze and synthesize insights on:

3.1.1 What are the main issues with implementing Software-Defined Networking (SDN) for campus networks.

3.1. 2 What are the vulnerabilities of SDN architectures and deployments in campus networks?

3. 1.3. How do these vulnerabilities and challenges affect the security of the campus networks?

3.2. Database Search and Search Strings

The search was conducted from 2020-2024 in different databases like IEEE Xplore, ACM, SpringerLink. Relevant keywords such as: “challenges in SDN campus network”, “SDN challenges in campus”, “Software Defined-Networking Challenges in University”. The researcher also applied search string via boolean operators “AND”: ("SDN vulnerabilities”) AND (“campus security"), ("Challenges”) AND ("Software Defined Networking”) AND ("Campus Security”), (“SDN”) AND (“Vulnerabilities”), AND (“Campus Security”).

3.3. Inclusion and Exclusion Criteria

This is to ensure that the only significant research are included in the literature review which are relevant to the study and excluded that are not focus or irrelevant to the study. Inclusion and exclusion are as follows:

Inclusion Criteria:

a. Papers published in peer-reviewed journals or conferences.

b. Studies focused on challenges and vulnerabilities of SDN for campus or university networks.

Exclusion Criteria:

a. Studies not focused on campus network security or irrelevant to SDN.

b. Non-peer-reviewed articles such as opinions, blogs

c. Papers not written in English or papers without full-text availability

3.4. Screening Process

Following the use of the search term on different databases of academics, duplicates were removed and remaining articles filtered for their relevance to the research question. In the first stage of filtering, papers found were ranked against the title of the papers, year of publication, and the nature of paper to filter out irrelevant ones based on the specific research theme.

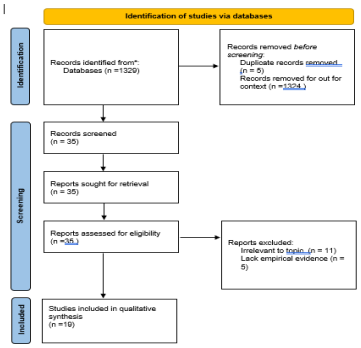

Figure 1 Article Selection Process (PRISMA) Flowchart

3.5 Data Extraction and Synthesis

The extraction and synthesis process entailed careful reading of each article wherein relevant items were noted using a Microsoft Excel spread sheet. The extracted items included article identification, author, year of publication, challenges, vulnerabilities, best practices or mitigation strategies, and additional contextual information. Data extraction involving the eighteen (20) articles are detailed on Table I.

Table I Data Extraction

Collected Data	Description
Article ID	Unique identity for the paper
References	Authors name, title, publication year and source
Challenges	List of the main challenges in SDN
Vulnerabilities	List of vulnerabilities of SDN in Campus Network Security
Mitigation Strategies	List of mitigation strategies/best practices of SDN in Campus Network Security
Other context	Definition of vulnerabilities and challenges, Insights, Results and Conclusions, Descriptions

III. RESULTS AND DISCUSSION

This section focuses on the result obtained after careful analysis of each article. The analysis focused on answering the research question published between 2020 to 2024. The researcher categorizes the result based on the challenges identified, a total of fourteen (14) challenges, five (5) vulnerabilities and nineteen (19) mitigations strategies for each challenge and vulnerabilities of SDN in Campus Network Security.

Table II. Challenges of SDN in Campus Network Security

Sources	Challenges	Description
M. A. B. S. Abir, S. H. Rian, S. R. Hasan and N. Arman (2023)	Network scalability and performance Limited radio frequency spectrum and increasing data rate demands	Enhanced receiver signal strength for better performance Optimizing limited RF spectrum for data rate demand
D. A. Assreshey et al (2022)	Limitations of conventional (non-SDN) network architectures	Cost and performance in traditional network management.
S. Neelavathy Pari et al. (2023)	Management of the classic IP networks	Managing classic IP networks has become challenging. Complexity arises from vendor-specific instructions for network policies.
M. -H. Cheng et al (2023)	Scalability challenges due to increasing network complexity, Single SDN controller cannot meet rising demand.	The deployment of multiple SDN controllers in a cluster can address the increasing demand and complexity of large-scale networks, ensuring high scalability and rapid deployment.

M. Raza et al (2024)	Scalability and computational demands of traditional IDS systems. Privacy concerns related to data sharing and sovereignty.	Resource constraints and communication overhead are significant challenges in FL systems.
M. Blose et al (2024)	Scalability issues	controller has limited computational resources
B. Isong et al (2020)	Performance metrics and cost constraint	Deploying the ideal quantity of controllers that are inherently conflicting in aspects such as dependability, load balancing, latency, energy efficiency, and computation time.
N. G & A. M (2023)	Fault-tolerance challenges	Fault-tolerance challenges unique to software-defined networks (SDNs)
O. David, P. Thornley and M. Bagheri (2023)	complex network environments	Complex management of traditional network devices. Increased operational costs due to infrastructure complexity.
S. Karnani & H. K. Shakya (2021)	Complex network with growing users and applications. A dynamic, flexible, and automated network behavior.	addressing the limitations of traditional static load balancing methods.
W. Brockelsby & R. Dutta (2023)	Flexibility, scalability, and management of campus networks	Increasing demand for robust wireless connectivity driven by the proliferation of mobile devices and IoT applications.
Karnani, S., Shakya, H.K (2023)	Increased network demand	Increased users and devices due to remote learning. Need for control and verification of network accessibility. rapid increase in the number of users and devices on campus networks due to the shift to remote learning.

Udo, et al (2020)	Manual configuration of devices is tedious and complex. Management errors arise from traditional network approaches. Single point of failure in centralized controller design. High-level decision policies needed for larger networks. Complexity of campus network policies complicates management.	Manually configuring network devices is time-consuming and prone to human error, traditional network management approaches often rely heavily on manual intervention and scripting, which can lead to management errors. Centralized network controllers create a single point of failure. Require high-level decision policies that can adapt to varying conditions and demands and diverse range of users and devices in a campus environment leads to complex network policies.
B. P., Agrawal, A., et. al (2024)	Security challenges in open technologies like SDN and Standardization Issues	Deployment presents challenges including security concerns and standardization issues.

As concluded in Table 2, fourteen (14) challenges have been identified. Networks that traditionally operate face tremendous obstacles concerning scalability and complexity due to their inflexibility as well as vendor specificity. SDN, however emerged to challenge these conventions, as it offers the flexibility of central control, dynamic management that is efficient. Centralized SDN controllers are effective in dynamic, efficient management, although there are problems related to fault tolerance, resource restrictions, and computational constraints, especially within large-scale settings. It is critical to install numerous SDN controllers to solve the bottleneck problems in task distribution, and thus, scalable challenges exist. SDN's capability to carry out the task in restrictive RF spectrum is a prominent improvement of wireless networks in restricted bandwidth and higher demand areas. Among these, few of the methods to accelerate the efficiency of SDNs are through suitable deployment of strategies, which balance the performance measure assessment of the correct number of controllers and restricted energy consumption. The traditional IDS and privacy-preserving approaches, like Federated Learning, provide a scalable advantage along with increased complexity in computing within SDN domains. Therefore, approaches for detailed planning are needed to highlight SDN limitations and implement an SDN infrastructure on a large scale in an efficient manner.

Table 3. Vulnerabilities in SDN in Campus Network Security

Sources	Vulnerabilities	Description
A. H. Abdi et al (2024)	Security threats and vulnerabilities in data and control planes.	SDN integrates data and control for flexible network management.

B. Ahmed et al (2020)	prone to many denial-of-service attacks, especially if the policy parameters of SDN are known to adversaries.	Security vulnerabilities in Software Defined Networks (SDN)
M. W. Nadeem et al (2023)	Distributed Denial of Service (DDoS) attack	Security and privacy challenges in Software-Defined Networking (SDN) Threats of a single point of failure in SDN
W. P. Rey (2023)	Vulnerabilities Associated with Centralized Network Management	Centralizing network management raises potential security vulnerabilities, necessitating robust measures to protect against threats.
W. Brockelsby and R. Dutt (2021)	Intrazone Communication Vulnerabilities	Traditional cybersecurity approaches fail to regulate intrazone communication

Table 3, enumerates the various key vulnerabilities of SDN in Campus Network Security. There are five (5) vulnerabilities identified: security threats and vulnerabilities in data and control planes, possible security vulnerabilities such as Denial of Service Attacks (DDOS) specially if the policy parameters of SDN are familiar to hackers and vulnerable if the network management is centralized. The study has outlined several relevant security weaknesses regarding SDN, specifically based on the data plane and the control plane; as SDN brings these two planes together to create an opportunity for dynamic management in the network, their integration exposes SDN to DDoS attacks in case a malicious party knows its parameters of the policy. One of the major components of SDN, centralized network management, poses severe security threats and vulnerabilities, including even the risk of DDoS attacks to a single point of failure. Thus, security measures must be applied rigorously to minimize such risks and reinforce the resilience of SDN infrastructure. These weaknesses and barriers in SDN deployment would result in a tremendous amount of network downtime and expanded attack surfaces, as well as potential data breaches. Even the dynamic nature of SDN makes it difficult to apply old security practices, and campus networks open up to more complex hacks. Horizontal malware propagation refers to malware that travels horizontally across devices within the same network segment or zone. Such infections abound because malware can spread quickly from an infected computer to many others, thereby causing significant operational problems, all without needing external transmission into these systems.

Table 4. Proposed Strategies to Mitigate Identified Challenges/Vulnerabilities

Sources	Identified Challenge/ Vulnerabilities	Proposed Mitigation Strategy
M. A. B. S. Abir, et al (2023)	Network scalability and performance Limited radio frequency spectrum and increasing data rate demands	Enhanced receiver signal strength for better performance Optimizing limited RF spectrum for data rate demand

D. A. Assreshey et al (2022)	limitations of conventional (non-SDN) network architectures	SDN adoption enabling enterprises to benefit from SDN's advantages without the need for a complete overhaul of existing infrastructure
S. Neelavathy Pari et al (2023)	management of the classic IP networks	Use of framework utilizing AI algorithms within an SDN environment to detect network flooding attacks, Enhancing security through real-time monitoring and analysis of traffic data.
M. -H. Cheng et al (2023)	Scalability challenges due to increasing network complexity, Single SDN controller cannot meet rising demand.	Utilizing Open-Source MANO and OpenStack to scale SDN controllers to enhance flexibility and reliability while managing system load effectively in SDN clusters.
M. Raza et al (2024)	Scalability and computational demands of traditional IDS systems. Privacy concerns related to data sharing and sovereignty.	Enabling decentralized model training, ensuring data sovereignty while collaboratively improving detection capabilities without sharing sensitive data.
M. Blose et al (2024)	scalability issues	Create a scalable hybrid switching solution using machine learning algorithms.

B. Isong, et al (2020)	Performance Metrics, Cost Constraint	Suggesting future research directions for optimizing controller deployment in large-scale networks.
N. G & A. M (2023)	Fault-tolerance challenges	Use of improved fault-tolerance solutions, focusing on failure detection and recovery
O. David, et al (2023)	complex network environments	Adoption of SDN to enhance network effectiveness and security
S. Karnani & H. K. Shakya (2021)	Complex network with growing users and applications. Need for dynamic, flexible, and automated network behavior.	Proposes SDN-based load balancing for campus networks. Introduces bi-fold module for traffic management efficiency
W. Brockelsby & R. Dutta (2023)	Flexibility, scalability, and management of campus networks	enhancing traditional campus wireless networks through a hybrid Software-Defined Networking architecture, enabling policy-driven networking and improved traffic analysis in the context of contemporary wireless traffic patterns.
Karnani, S., Shakya, H.K (2023)	Increased network demand	Integrating SDP with SDCN enhances authentication and access control, minimizing unauthorized access and

		improving network security and scalability in campus environments.
Udo, Edward et al (2020)	Manual configuration of devices is tedious and complex. Management errors arise from traditional network approaches. Single point of failure in centralized controller design. High-level decision policies needed for larger networks. Complexity of campus network policies complicates management.	The proposed SDN framework enhances campus network management efficiency.
A. H. Abdi et al (2024)	Security threats and vulnerabilities in data and control planes.	Comprehensive study on SDN security solutions conducted. Future research directions for emerging threats.
B. Ahmed et al (2020)	Vulnerable to many kinds of denial-of-service attacks especially if the policy parameters of SDN are known to adversaries.	Use of techniques to fingerprint SDN policy parameters presented. Dynamic policy parameters to further research for resilience
M. W. Nadeem et al (2023)	Distributed Denial of Service (DDoS) attack	Distributed controller, verification policies
W. P. Rey (2023)	Vulnerabilities Associated with Centralized Network Management	The design and deployment of MidwestCloud, a centralized SDN-based network management system to create a scalable, fault-

		tolerant, and flexible network infrastructure. This involves leveraging SDN technology to enhance network management, automation, and resource allocation.
W. Brockelsby and R. Dutt (2021)	Intrazone Communication Vulnerabilities	Enhancing cybersecurity in campus networks is crucial. Strategic placement of hardware/software data planes improves effectiveness
Baniya, P. et al. (2024).	Security challenges in open technologies like SDN and Standardization Issues	Practical solutions for integrating OpenFlow with legacy system SDN-based Mobile Networks can greatly enhance network adaptability, streamline management processes, and improve overall security.

Table 4 presents the proposed mitigation strategies based on the identified challenges and vulnerabilities. It points out many problems and weaknesses with current network architectures, and it suggests that SDN is the answer to the scalability and performance, and security problems. Manual scalability, manual configuration, manual performance, growing user requirements, network complexity have been the major limitations of traditional networks. With adoption of SDN, enterprises can integrate more sophisticated technologies such as AI algorithms which can detect network flooding attacks and allow better monitoring and analyzing real time traffic in the network, making the network more secure. One of the biggest problems with SDN is the fact that a single controller can't handle increased load. This is somewhat remedied by the use of frameworks like Open Source MANO and OpenStack, which provide scalability, flexibility, and reliability in the administration of SDN clusters. With the growing demands for radio frequency spectrum and data rate, SDN manages these limited resources and enables effective communication among the expanding number of users. Also, it deals with the issue of fault-tolerance by improving failure detection and recovery at various strata of the network and finally it also suggests some future work around dynamic load balancing and resilient policy parameter management. SDN in campus networks allows for automated, policy-driven, and hybrid architectures that provide for better traffic analysis and increased scalability, as well as a significant reduction in management complexity and improved security. Lastly, the combination of SDN and decentralized privacy-preserving techniques such as federated learning is discussed, allowing for data sovereignty and improved detection without a need to reveal personal information. Horizontal malware propagation requires a shift in cybersecurity strategies.

Campus networks must have strong cyber security, and this can be achieved by placing hardware and software data planes in strategic locations. This approach, apart from improved traffic management and monitoring, also allows for effective policy implementation and scalability. Should the educational institutions be able to identify these vulnerabilities beforehand, they will have an opportunity to implement measures to safeguard their networks, prevent personal information compromise, and provide a secure environment for the users.

IV. CONCLUSION

The PRISMA systematic review has identified key challenges and vulnerabilities of SDN in campus networks. These include scalability issues, and security vulnerabilities in centralized control. These are critical issues that must be addressed to enhance the security and efficiency of campus networks that use SDN architectures.

According to the study, with Software-Defined Networking (SDN) in place, institutions would have better scalability, stronger security, and less complicated management.

This transition not only improves our capability to manage resources with growing demands from users but also paves the way for deployment of privacy-preserving techniques in detecting users' activities based on their personal data, such as federated learning, typically carried out on the users' devices independently of the servers.

In summary, even though SDN provides a revolutionary solution to the problems of traditional networks, its drawbacks cannot be overlooked. Universities can create a secure, stable, and efficient network atmosphere by simply consulting, and being proactive by finding weaknesses and implementing strong security measures to protect their networks. This study suggests further research to improve the abilities of Software-Defined Networking (SN) so that the campus networks will continue to be secure and versatile enough to defend against the constantly changing face of cyber warfare and prevalent cyberattacks.

ACKNOWLEDGEMENT

The researcher wishes to show her deepest appreciation to those who have contributed to the fulfillment of this study especially to God Almighty and to her family. The researcher would like to convey her heartfelt gratitude to Western Philippines University and National University for their support and assistance.

REFERENCES

[1]A. Mahar et al. 2024. An analysis of software-defined networking and its related security implications. 2024 IEEE Khwarizmi Humanitarian Technology Conference (KHI-HTC)*. IEEE, pages 1-5. DOI: https://doi.org/10.1109/khi-htc60760.2024.10482096.

[2]T. Shanmugam and B. Malarkodi, 2019. Mitigating challenges in campus network administration: Proposed solutions. IEEE International Conference on Innovative Computing and Communication Workshops (IMICPW)*. IEEE, pp. 312–316. DOI: https://doi.org/10.1109/imicpw.2019.8933236.

[3]A. A. Ojugo and A. O. Eboka. 2020. Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view. *International Journal of Modern Education and Computer Science* 12, 6 (2020), 24-30. DOI:https://doi.org/10.5815/IJMECS.2020.06.03

[4]D. Nadig and B. Ramamurthy. 2019. Securing large-scale data transfers in campus networks. In *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (SDN-NFV '19). ACM, New York, NY, 29–32. DOI:https://doi.org/10.1145/3309194.3309444.

[5] K. Rusere and E. K. Ngassam. 2020. Emerging network security issues in modern tertiary institutions. *International Journal of Modern Education and Computer Science* 12, 1 (2020), 1–9.

[6]Guo, G., Zhang, J., & Ma, Z. (2021). Implementation of intrusion prevention and attack traceback protocols in campus networks. *Computer Science and Information Systems* 18, no. 2 (2021), pp. 49–68.

[7]Chatterjee, S. P., & Rawat, D. B. (2024). An innovative framework for enhancing access control in software-defined networking.International Conference on Communications Workshops (ICC Workshops '24)*. IEEE, pp. 1816–1821.

[8][8] R. H. Vairagade. 2024. A Comprehensive Examination of SDN Architecture and Its Practical Implementations. *International Journal of Science and Research* 13, no. 2 (2024), pp. 836–846.

[9]A. Ali, M. Yousaf, and M. Bashir. 2024. Assessing security in software-defined networks: Identifying vulnerabilities and addressing challenges.Lahore Garrison University Research Journal of Computer Science and Information Technology, vol. 8, no. 2 (July 2024).

[10] X. Gui. 2023. Creating software-defined network controllers for campus settings. 35th Chinese Control and Decision Conference (CCDC '23)*. IEEE, pp. 3712–3715.

[11] W. Hill, et al. 2024. An extensive examination of DDoS attacks inside software-defined networking: Assessing datasets, attack strategies, and mitigation approaches. Applied Sciences 6, no. 9 (2024).

[12] Abir, M. A. B. S., et al. (2023). Improving signal transmission in campus networks with software-defined networking. 2023 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), Dhaka, Bangladesh, pp. 417–420.

[13] D. A. Assreshey et al., 2022. Employing radial architecture for hybrid software-defined networking inside companies. 14th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, pp. 145–151.
[14] S. Neelavathy Pari et al. 2023. Detecting flooding hazards in software-defined networks with artificial intelligence and various learning methods. 12th International Conference on Advanced Computing (ICoAC), Chennai, India, pp. 1–7.
[15] M.-H. Cheng et al. 2023. Intelligent allocation of virtual functions to mitigate controller strain in SDN clusters. 9th International Conference on Applied System Innovation (ICASI), Chiba, Japan, pp. 241–243.
[16] M. Raza et al. 2024. Utilizing federated learning for secure intrusion detection in software-defined networks. *IEEE Access* 12 (2024), pp. 69551–69567.
[17] [M. Blose et al. 2024. Examining scalability challenges in hybrid SDN with reinforcement learning. *IEEE Access* 12 (2024), pp. 63334–63350. DOI: https://doi.org/10.1109/ACCESS.2024.3387273.
[18] B. Isong et al., 2020. An extensive analysis of SDN controller placement strategies. *IEEE Access* 8 (2020), pp. 170070–170092. DOI: https://doi.org/10.1109/ACCESS.2020.3023974.
[19] N.G. and A.M. 2023. Improving network resilience and stability using software-defined networking. 8th International Conference on Science, Technology, Engineering, and Mathematics (ICONSTEM)*, Chennai, India, pages 1–6.
[20] O. David et al., 2023. The impact of software-defined networking on campus networks, wide area networks, and data centers. 2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, conducted in Istanbul, Turkey, pages 1–8.
[21] S. Karnani and H. K. Shakya, 2021. Utilizing software-defined networking to improve network load distribution in educational institutions. 13th International Conference on Computational Intelligence and Communication Networks (CICN), held in Lima, Peru, pp 167–171. DOI: https://doi.org/10.1109/CICN51697.2021.9574640.
[22] K. William, B. Brockelsby, and R. Dutta. 2023. Enhancing wireless networks in educational settings with SDN technologies. 2023 International Conference on Networking and Communications (ICNC)*, pp. 1-6. DOI: https://doi.org/10.1109/ICNC57223.2023.10074202.
[23] S. Karnani and H. K. Shakya. 2023. Application of SDP authentication methodologies in SDN inside campus environments. D. Gupta et al. (Eds.), https://doi.org/10.1007/978-981-19-2821-5_17.
[24] Udo, E., Isong, E., & Nyoho, E. (2020). A systematic approach for managing campus networks with SDN techniques. International Journal of Computer Networks & Communications 12, no. 2 (2020): 47–58. DOI: https://doi.org/10.5121/ijcnc.2020.12205.
[25] P. Baniya and colleagues, 2024. Addressing the challenges related to the installation of SDN systems. F. P. García Márquez et al. (Eds.) DOI: https://doi.org/10.1007/978-3-031-56728-5_45.
[26] A. H. Abdi et al. 2024. Comprehensive analysis of security solutions in software-defined networks. *IEEE Access* 12 (2024), pp. 69941–69980. DOI: https://doi.org/10.1109/ACCESS.2024.3393548.
[27] B. Ahmed et al., 2020. A study on the fingerprinting of Software-Defined Networking policy parameters. *IEEE Access* 8 (2020), pp. 142379–142392. DOI: https://doi.org/10.1109/ACCESS.2020.3012176.
[28] M. W. Nadeem et al. 2023. Deep learning techniques for detecting botnet attacks in Software-Defined Networks. *IEEE Access* 11 (2023), pp. 49153–49171. DOI: https://doi.org/10.1109/ACCESS.2023.3277397.
[29] W. P. Rey. 2023. Establishing a centralized Software-Defined Networking management framework for a university in Marinduque, Philippines. In *Proceedings of the 2023 International Conference on Information Network and Computer Communications (INCC)*, Beijing, China, pp. 36–41. DOI: https://doi.org/10.1109/INCC58754.2023.00011.
[30] K. William et al. 2023. Advancing campus networks via innovations in software-defined networking. DOI: https://doi.org/10.1109/ICNC57223.2023.10074202.