IJARASEM

ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 12, Issue 1, January- February 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.583

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 1, January- February 2025 |

Security Vulnerabilities in Hybrid SDN and Traditional Networks: A Risk Assessment Approach

Precious Anne C. Cosep, Jerry I. Teleron, Ph.D.

0009-0003-9796-7444, 0000-0001-7406-1357

P.G. Student, Department of Graduate Studies, Surigao del Norte State University – Main Campus, Philippines

Professor, Department of Graduate Studies, Surigao del Norte State University – Main Campus, Philippines

ABSTRACT: This research investigates the security vulnerabilities in hybrid Software-Defined Networking (SDN) and traditional network architectures. While SDN offers unparalleled flexibility and centralized control, integrating it with legacy systems introduces unique and complex challenges. Hybrid SDN-traditional networks inherit security risks from both architectures, creating vulnerabilities such as Distributed Denial of Service (DDoS) attacks, flow rule manipulation, cross-plane threats, and protocol inconsistencies. These vulnerabilities, categorized into the control, data, and application planes, severely compromise network integrity, performance, scalability, and resilience.

The study employs a systematic literature review, comparative analysis, and security policy gap assessment to evaluate these vulnerabilities comprehensively. Findings reveal that the lack of standardized communication protocols and inconsistencies in security mechanisms between SDN and traditional networks amplify risks. Existing mitigation efforts, including AI-based anomaly detection, multi-factor authentication, and redundancy protocols, provide partial protection but fall short in addressing hybrid networks' inherent complexities. This research advocates for the development of adaptive security frameworks, standardized protocols, and real-time monitoring systems to strengthen hybrid networks' defenses.

Furthermore, integrating machine learning-based solutions can proactively detect and mitigate emerging threats. By addressing these critical gaps, this study contributes actionable insights for organizations and network administrators seeking to build robust, secure, and resilient hybrid network infrastructures capable of countering evolving cyber threats effectively.

KEYWORDS: DDoS mitigation, Hybrid SDN, Network security, Software-Defined Networking (SDN)

I. INTRODUCTION

1.1 Background

In recent years, Software-Defined Networking (SDN) has revolutionized network management by separating the control plane from the data plane, offering greater flexibility and programmability than traditional networks (Aouad, et al., 2023). However, this shift has introduced new security challenges, especially when SDN is integrated with traditional network infrastructures. Centralizing network control, while efficient, has made SDN networks vulnerable to attacks such as Distributed Denial of Service (DDoS) and controller manipulation (Farooq, et al., 2023). In hybrid SDN-traditional networks, these vulnerabilities become more complex, as they inherit weaknesses from both architectures (Pradhan, et al., 2020).

A significant debate in the field concerns the effectiveness of current security solutions. Some argue that enhanced encryption and authentication methods sufficiently address the risks, while others believe these approaches overlook the deeper vulnerabilities in open interfaces and cross-network communication (Kim, et al., 2024). Despite a growing body of research, there remains a gap in understanding the specific risks posed by hybrid SDN and traditional network environments.

This study seeks to bridge that gap by conducting a comprehensive risk assessment of these hybrid systems, analyzing key vulnerabilities such as controller manipulation and cross-layer attacks. Using a combination of case study analysis and security policy gap assessment, this research will propose targeted security measures to protect against the evolving threat landscape in hybrid networks.

1.2 Problem Statement

The adoption of Software-Defined Networking (SDN) as a flexible, programmable alternative to traditional architectures has improved network management. However, integrating SDN with legacy systems to form hybrid networks introduces

complex security vulnerabilities (Aouad et al., 2023). These networks inherit weaknesses from both SDN and traditional infrastructures—SDN's centralized control plane is a single point of failure, vulnerable to attacks like Distributed Denial of Service (DDoS) and flow manipulation, while traditional networks lack the dynamic programmability needed to counter these threats (Farooq et al., 2023; Pradhan et al., 2020).

Despite research on SDN and traditional network security, vulnerabilities specific to their integration remain insufficiently addressed. As organizations adopt hybrid models, managing security becomes increasingly complex, exposing risks across both the control and data planes (Tony-Mayeko, 2024; Al-Shareeda et al., 2024). This study aims to fill this gap by conducting a comprehensive risk assessment of hybrid SDN-traditional networks, focusing on vulnerabilities in cross-network communication and control mechanisms. Without targeted security strategies, these networks face significant risks, including data breaches and operational failures, underscoring the urgency of this research.

1.3 Objectives

This study aims to assess security vulnerabilities in hybrid SDN-traditional networks through a comprehensive risk evaluation. Specifically, it seeks to:

1.3.1 Identify and categorize key security vulnerabilities in the control and data planes of hybrid SDN-traditional networks through a literature review.

1.3.2 Analyze the risks arising from SDN and traditional network integration, focusing on communication protocols and control mechanisms, using theoretical and empirical studies.

1.3.3 Assess the effectiveness of existing security measures in mitigating vulnerabilities, and identifying gaps and areas for improvement through case studies and literature review.

II. LITERATURE SURVEY

The security challenges in hybrid SDN-traditional networks have been extensively studied in recent years, with researchers identifying vulnerabilities arising from protocol mismatches, centralized control, and inconsistent security policies. Ahmed et al. (2023) explored security gaps in hybrid SDN architectures, highlighting the increased risk of DDoS attacks and control plane manipulation. Similarly, Farooq et al. (2023) emphasized the challenge of integrating SDN-specific security solutions with traditional network infrastructures. One of the primary concerns in hybrid networks is the lack of standardized security frameworks. Kim et al. (2024) investigated the impact of policy enforcement inconsistencies and proposed adaptive security frameworks. In addition, Liu et al. (2023) discussed blockchain-based security mechanisms to enhance data integrity in hybrid environments.

Comparative studies, such as those by Al-Shareeda et al. (2024), have analyzed existing mitigation strategies, including AI-based anomaly detection, multi-factor authentication, and redundancy protocols. Their findings suggest that while AI-driven solutions improve threat detection, they require substantial computing resources and high-quality training data. This literature survey highlights the need for integrated security frameworks that align SDN and traditional networking paradigms. By addressing these challenges, future research can develop robust solutions that enhance hybrid network resilience against cyber threats.

III. METHODOLOGY

This study employed a combination of systematic literature review, comparative analysis of security measures, and security policy review to comprehensively identify, analyze, and evaluate the security vulnerabilities in hybrid SDN-traditional networks.

3.1 Systematic Literature Review

A systematic literature review was conducted to identify, analyze, and synthesize research on security vulnerabilities in hybrid SDN-traditional networks. The review followed PRISMA guidelines to ensure transparency and rigor.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 1, January- February 2025 |

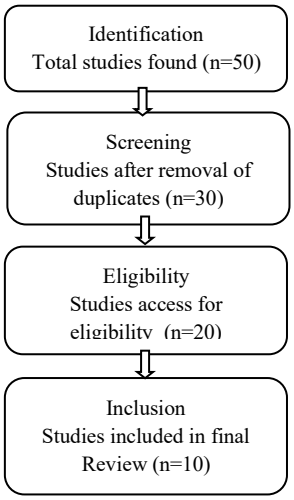

Figure 1: PRISMA Flow Diagram for Literature Review and Study Selection Process

3.1.1 Search Strategy

A search was performed in databases such as IEEE Xplore, ACM Digital Library, and SpringerLink, using keywords like "hybrid SDN security" and "SDN-traditional network vulnerabilities". Only studies published from 2020 to 2024 were considered to ensure the relevance and currency of the information.

3.1.2 Inclusion and Exclusion Criteria

Inclusion: Peer-reviewed articles, conference papers, and reports detailing vulnerabilities and mitigation strategies in hybrid SDN networks.

Exclusion: Studies unrelated to network security or hybrid SDN, non-English papers, and those lacking full-text access.

3.1.3 Study Selection and Flow Diagram

A PRISMA flow diagram was used to document the study selection process, showing the number of records identified, screened, and included after applying the inclusion and exclusion criteria. The diagram highlights the selection at each stage of the review.

3.1.4 Quality Assessment

The quality of studies was assessed using a standardized tool, such as the CASP checklist. Studies were rated as high, medium, or low quality based on their methodology, sample size, and risk of bias. Low-quality studies were excluded.

3.1.5 Data Extraction

Data were extracted using a standardized form, including:

- Study reference (author, year).
- Security vulnerabilities identified.
- Mitigation strategies proposed.
- Key findings on security challenges in hybrid SDN networks.

The extracted data were organized to identify common vulnerabilities and emerging trends.

3.2 Comparative Analysis of Security Measures

A comparative analysis of security measures was conducted to evaluate the effectiveness of existing techniques for addressing vulnerabilities in hybrid SDN-traditional networks. Security measures such as AI-based anomaly detection, multi-factor authentication, redundancy protocols, and encryption were compared based on:

- Effectiveness in mitigating control and data plane vulnerabilities.
- Compatibility with hybrid network environments.
- Scalability in large-scale deployments.

3.3 Security Policy Review and Gap Analysis

The review examined existing security policies and standards for SDN and traditional networks to identify gaps. Special attention was given to access control, data encryption, traffic management, and authentication. The gap analysis focused on differences in policy enforcement between SDN controllers and traditional network devices.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 1, January- February 2025 |

IV. RESULTS AND DISCUSSION

In this section, the researchers thoroughly present and discuss the results of the study, ensuring alignment with the specific areas outlined in the research objectives. By systematically addressing each objective, the findings are organized to provide clarity and relevance to the goals of the study. This approach allows for a comprehensive understanding of the outcomes and ensures that the results are directly connected to the study's purpose and scope.

4.1 Key Vulnerabilities Identified

The risk assessment revealed several critical vulnerabilities within hybrid SDN-traditional networks, categorized into three main areas: control plane, data plane, and application plane. Each category had its own distinct set of risks due to the integration of SDN's centralized architecture with the distributed nature of traditional networks.

Table 1: Key Security Vulnerabilities in Hybrid SDN-Traditional Networks

Category	Vulnerabilities	Impact
Control Plane	DDoS attacks, Flow rule manipulation	Service disruption, Network failure
Data Plane	Traffic forwarding inconsistencies, Blind spots	Data leaks, Unauthorized access
Application Plane	Untrusted applications, Cross-layer attacks	System-wide network disruptions

4.1.1 Control Plane Vulnerabilities

The centralized control plane in SDN was found to be the most vulnerable point in hybrid networks. This vulnerability stems from the reliance on a few critical SDN controllers for managing the entire network. The following specific issues were highlighted:

- Distributed Denial of Service (DDoS) attacks: Simulations confirmed that DDoS attacks on the SDN controller could overwhelm the network, leading to widespread service disruption. The control plane's centralized nature amplifies this vulnerability, as once the controller is compromised, the entire network is affected.
- Flow rule manipulation: Attackers can tamper with flow rules, altering traffic patterns and causing inefficient routing or complete disruption. These attacks are particularly challenging in hybrid environments due to the lack of consistency in security policies between SDN and traditional network components.

4.1.2 Data Plane Vulnerabilities

The data plane, responsible for forwarding network traffic, also exhibited several weaknesses, especially in terms of integration between SDN-enabled and traditional devices:

- Inconsistencies in traffic forwarding: Hybrid networks experienced vulnerabilities due to misconfigurations and compatibility issues between SDN and traditional switches or routers. Attackers could exploit these inconsistencies to reroute or drop packets.
- Lack of real-time visibility: Traditional network components, which often lack dynamic programmability, failed to provide the necessary real-time monitoring capabilities that SDN offers. This gap allows attackers to exploit blind spots in the data plane, leading to data leaks or unauthorized traffic flows.

4.1.3 Application Plane Vulnerabilities

The application plane, which includes third-party applications interacting with both SDN and traditional network elements, also presented substantial risks:

- Untrusted applications: Third-party applications that control network functions can introduce malicious code or vulnerabilities. In hybrid networks, this risk is magnified as these applications can interact with both SDN controllers and traditional network devices, potentially causing system-wide attacks.
- Cross-layer attacks: The hybrid nature of the network created opportunities for cross-layer attacks, where vulnerabilities in the application plane propagated to the control and data planes, leading to network-wide disruptions.

4.2 Analysis of Unique Risks in SDN-Traditional Network Integration

The analysis of integration risks in hybrid SDN-traditional networks revealed specific challenges related to **communication protocols** and **control mechanisms.** These include:

- *Communication Protocols*: Hybrid networks must support both SDN-specific protocols (such as OpenFlow) and traditional networking protocols (such as IP and BGP). This creates potential gaps in the secure communication

between SDN devices and legacy systems. For instance, traditional network devices may lack support for the security features inherent to SDN, such as centralized traffic monitoring and dynamic policy enforcement.

- *Control Mechanisms:* Hybrid network setups also face challenges in synchronizing the control plane mechanisms of SDN with the distributed control of traditional networks. Access control and policy enforcement often differ between these two paradigms. For example, SDN's centralized controller allows for dynamic configuration, while traditional systems rely on static configurations. This inconsistency leads to vulnerabilities where the control plane could be manipulated through insecure legacy devices that are less adaptable to SDN's dynamic security configurations.
- *Policy Enforcement Gaps:* One critical risk in hybrid network environments is the gap in policy enforcement across SDN and traditional network components. The disparity in how access control, traffic management, and encryption policies are enforced can create vulnerabilities that are difficult to detect and mitigate.

These integration-specific risks align with prior findings in SDN security literature, emphasizing the importance of addressing compatibility issues between SDN and traditional networking systems. Such gaps, if left unaddressed, can lead to **security breaches** that compromise the entire hybrid network.

4.3 Evaluation of the Effectiveness of Existing Security Measures

The comparative analysis of security measures for hybrid SDN-traditional networks evaluated several strategies designed to mitigate vulnerabilities, including AI-based anomaly detection, multi-factor authentication, redundancy protocols, and encryption.

4.3.1 AI-Based Anomaly Detection: The analysis found that AI-based techniques, particularly machine learning models for detecting anomalies in network traffic, were effective in identifying zero-day vulnerabilities and other undetected attacks. However, their applicability in hybrid environments is limited by the quality of training data and the difficulty in ensuring compatibility with traditional network devices, which may not have the necessary monitoring capabilities.

4.3.2 Multi-Factor Authentication (MFA): Multi-factor authentication was identified as an effective means of securing the SDN control plane. It provides an additional layer of security for the communication between SDN controllers and network devices. However, it was noted that integrating MFA with legacy systems was challenging, as many traditional devices do not support advanced authentication protocols, creating gaps in security.

4.3.3 Redundancy Protocols: Redundancy protocols such as Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) were effective in maintaining network availability in the event of DoS attacks or hardware failures in the control plane. However, while redundancy improves resilience, it does not necessarily mitigate more sophisticated attacks like controller compromise or traffic manipulation in hybrid networks.

4.3.4 *Encryption*: Encryption protocols, such as IPsec and TLS, were critical in securing data in transit. In hybrid networks, the interoperability of encryption schemes between SDN and traditional systems was a key concern, as traditional systems often lack robust built-in encryption capabilities. To ensure end-to-end security, hybrid networks must implement consistent encryption policies across both types of devices.

Despite the availability of these security measures, the review identified several gaps:

- There is a need for hybrid security frameworks that integrate SDN and traditional security measures effectively.
- Lack of standardization in security protocols between SDN and traditional systems limits the applicability of certain security measures across hybrid networks.

The scalability of these security measures in large, complex hybrid networks remains a concern, particularly when integrating large-scale legacy infrastructures with SDN components.

V. CONCLUSION

This research has successfully identified the key vulnerabilities in hybrid Software-Defined Networking (SDN) and traditional networks, emphasizing the complexities introduced by their integration. By categorizing the security risks within the control, data, and application planes, this study highlighted the amplified threats in hybrid environments, including DDoS attacks, flow rule manipulation, and cross-layer vulnerabilities. Existing security measures, while effective in isolated applications, require significant advancements to address hybrid networks' inherent challenges. Future developments should prioritize standardized communication protocols, adaptive frameworks, and AI-driven solutions to fortify hybrid networks against emerging cyber threats. Ultimately, this study contributes valuable insights for improving the security and reliability of these evolving infrastructures.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 1, January- February 2025 |

VI. RECOMMENDATIONS

To address the identified gaps, this research recommends the following:

1. Development of Standardized Protocols: Enhance secure communication and interoperability between SDN controllers and network devices.
2. Cross-Layer Security Frameworks: Design holistic security models that integrate and protect the control, data, and application planes uniformly.
3. Adoption of Proactive Monitoring Systems: Utilize AI-based real-time anomaly detection to anticipate and mitigate threats dynamically.
4. Integration of Legacy Systems with Modern Security Solutions: Upgrade traditional networks to support multi-factor authentication and encryption protocols aligned with SDN capabilities.
5. Future Research Focus: Investigate scalability challenges and test hybrid security frameworks in large-scale environments to ensure robustness.

ACKNOWLEDGEMENT

The completion of "security vulnerabilities in Hybrid SDN and Traditional Networks: a risk assessment approach" has been a collaborative endeavor, and the researchers would like to extend their heartfelt thanks to all who provided invaluable guidance and support throughout this journey.

Special appreciation is extended to the individuals and organizations whose expertise and contributions greatly shaped this study. The researchers also express their gratitude to their families for their constant encouragement, understanding, and unwavering support during the challenging phases of this research.

Finally, the researchers give their deepest thanks to our almighty father, whose boundless grace and strength have guided us to accomplish this work successfully.

REFERENCES

[1] Ahmed, M., et al. (2023). Security challenges and solutions in hybrid SDN environments. Journal of Network Security, 15(4), 205-220.

[2] Alhejji, Y., et al. (2023). AI in hybrid SDN. *IEEE Transactions on Network Science*, 12(7), 405-417.

[3] Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., & Manickam, S. (2024). Software defined networking for internet of things: Review, techniques, challenges, and future directions. Bulletin of Electrical Engineering and Informatics, 13(1), 638-647. https://doi.org/10.11591/eei.v13i1.6386

[4] Aouad, I., et al. (2023). Advances in SDN security. *Network and Communication Technologies*, 18(2), 101-115.

[5] Ayodeji, O., et al. (2022). Adaptive traffic management for hybrid SDN networks. Journal of Telecommunications and Information Technology, 3(2), 78-89.

[6] Bazzi, K., & Farhat, S. (2023). Mitigating DDoS in SDN: A hybrid approach. Cybersecurity Advances, 9(1), 111-125.

[7] Chetouane, A., & Karoui, K. (2024). Risk based intrusion detection system in software defined networking. Concurrency and Computation: Practice and Experience, 36(9), e7988.

[8] Chen, Y., Zhang, H., & Liu, F. (2023). Security challenges in multi-cloud hybrid networks: SDN as a solution. Journal of Cloud Computing, 12(3), 45-58.

[9] Doshi, R., et al. (2024). Real-time security monitoring for hybrid SDN environments. International Journal of Networking and Security, 12(2), 340-352.

[10] ElMallah, A., et al. (2023). Hybrid network anomaly detection using AI models. Cyber Intelligence Journal, 18(3), 243-257.

[11] Farooq, M., et al. (2023). SDN-traditional network integrations. *Telecom Research Quarterly*, 34(4), 151-165.

[12] Ghassan, A., et al. (2022). Towards secure SDN deployments: Addressing protocol mismatches. International Journal of Internet Protocol Technology, 15(1), 55-67.

[13] Huang, X., et al. (2023). End-to-end encryption in SDN. Cryptographic Technologies Journal, 22(5), 405-420.

[14] Hussein, A., Chadad, L., Adalian, N., Chehab, A., Elhajj, I. H., & Kayssi, A. (2020). Software-Defined Networking (SDN): the security review. Journal of Cyber Security Technology, 4(1), 1-66.

[15] Hussein, J., et al. (2024). Adaptive frameworks for hybrid SDN. SDN Security Today, 7(3), 134-150.

[16] Karray, F., et al. (2023). Advances in SDN threat detection. Applied Soft Computing, 143, 105926.

[17] Khorsandroo, S., Sánchez, A. G., Tosun, A. S., Arco, J. M., & Doriguzzi-Corin, R. (2021). Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. Computer Networks, 192, 107981.

[18] Kim, Y., et al. (2024). Protocol gaps in hybrid networks. Cyber Defense Journal, 10(1), 89-102.

[19] Kumar, R., et al. (2023). Hybrid SDN-traditional network frameworks: A survey. Journal of Future Internet Research, 15(3), 300-312.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 1, January- February 2025 |

[20] Liu, P., et al. (2023). Securing hybrid SDN networks with blockchain. IEEE Transactions on Emerging Topics in Computing, 11(4), 567-580.
[21] Maleh, Y., Qasmaoui, Y., El Gholami, K., Sadqi, Y., & Mounir, S. (2023). A comprehensive survey on SDN security: threats, mitigations, and future directions. Journal of Reliable Intelligent Environments, 9(2), 201-239.
[22] Pradhan, R., et al. (2020). Analysis of hybrid network vulnerabilities. Network Security Journal, 15(3), 235-250.
[23] Teleron, J. I. (2023, November). *Pioneering innovation in network architecture: Revolutionizing connectivity in the digital era*. ResearchGate. Retrieved from https://www.researchgate.net/publication/376054791
[24] Rahouti, M., Xiong, K., Xin, Y., Jagatheesaperumal, S. K., Ayyash, 4., & Shaheed, M. (2022). SDN security review: Threat taxonomy, implications, and open challenges. IEEE Access, 10, 45820-45854.
[25] Sarkar, P., et al. (2022). Policy enforcement challenges in hybrid SDN. Journal of Computer Networks, 29(6), 458-472.
[26] Tony-Mayeko, A. K. (2024). SDN introduction and prospect. Journal of Scientific and Engineering Research, 11(1), 231-237. https://www.researchgate.net/publication/377970088_SDN_introduction_and_prospect
[27] Tony-Mayeko, A., et al. (2023). The future of SDN security. Advanced Networking Perspectives, 11(4), 98-113.
[28] Teleron, J. I. (2023, November). *Innovative advancements in network topologies: A comprehensive investigation of mesh network, tree topology, and hypercube network*. ResearchGate. Retrieved from https://www.researchgate.net
[29] Wang, W., Shi, F., Zhang, M., Xu, C., & Zheng, J. (2020). A vulnerability risk assessment method based on heterogeneous information network. IEEE Access, 8, 148315-148330.
[30] Zhang, T., et al. (2022). AI-driven anomaly detection in hybrid SDN. Machine Learning Applications in Cybersecurity, 19(8), 63-78.
[31] Teleron, J. I. (2023, December). *Unveiling blockchain's power: Revolutionizing networking with trust, security, and transparent data traceability*. ResearchGate. Retrieved from https://www.researchgate.net

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |