Journal of Engineering Research and Reports

Volume 26, Issue 8, Page 112-134, 2024; Article no.JERR.120621
ISSN: 2582-2926

Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks

Oluwaseun Ibrahim Akinola [a++],
Oluwaseun Oladeji Olaniyi [b#*],
Olumide Samuel Ogungbemi [c†],
Oluseun Babatunde Oladoyinbo [d‡]
and Anthony Obulor Olisa [e^]

[a] Olabisi Onabanjo University, P.M.B. 2002, Ago-Iwoye, Ogun State, Nigeria.
[b] University of the Cumberlands, 104 Maple Drive, Williamsburg, KY 40769, United States of America.
[c] Centennial College, 941 Progress Ave, Scarborough, ON M1G 3T8, Canada.
[d] Oyo State College of Agriculture and Technology, Igboora, Nigeria.
[e] Cumberland University, 1 Cumberland Dr, Lebanon, TN 37087, United States.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/jerr/2024/v26i81234

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/120621

Original Research Article

Received: 20/05/2024
Accepted: 24/07/2024
Published: 27/07/2024

[++] *Wireless Security Network Researcher;*
[#] *Information Technology Researcher;*
[†] *Data Privacy and Blockchain Technology Researcher;*
[‡] *Agricultural Researcher;*
[^] *Information Technology Researcher*
**Corresponding author: Email: oolaniyi00983@ucumberlands.edu;*

Cite as: *Akinola, Oluwaseun Ibrahim, Oluwaseun Oladeji Olaniyi, Olumide Samuel Ogungbemi, Oluseun Babatunde Oladoyinbo, and Anthony Obulor Olisa. 2024. "Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks". Journal of Engineering Research and Reports 26 (8):112-34. https://doi.org/10.9734/jerr/2024/v26i81234.*

ABSTRACT

This research examines the vulnerabilities and resilience mechanisms of Software-Defined Networking (SDN) and cloud networks, with a specific focus on controller failures and security attacks. The study leverages both simulated and real-world data to assess how these vulnerabilities impact network performance metrics including downtime, packet loss, latency, and throughput. A significant observation from the study is that the nature and impact of network disruptions vary significantly depending on the type of failure or attack, highlighting the need for tailored resilience strategies. Machine learning techniques, notably Support Vector Machines (SVMs), are employed to classify these disruptions with high accuracy, suggesting a promising direction for proactive network management. The research proposes a novel framework that combines the dynamic control capabilities of SDN with machine learning and automation to improve the networks' fault tolerance and recovery mechanisms. The effectiveness of this framework is demonstrated through enhanced resilience and reduced performance degradation during network disruptions. This study contributes to the field by outlining a scalable and efficient approach to mitigating vulnerabilities in SDN and cloud networks, thereby enhancing overall network stability and reliability.

Keywords: Software-Defined Networking (SDN); cloud networks; resilience; controller failures; security attacks; machine learning; automation.

1. INTRODUCTION

The digital space is undergoing a significant transformation, driven by the rapid adoption of cloud services, which have become the new norm due to their flexibility, scalability, and cost-effectiveness [1]. This exponential growth, however, hinges critically on the resilience of the underlying network infrastructure. Software-Defined Networking (SDN) and cloud networks represent pivotal advancements that have transformed how data centers, enterprises, and service providers operate their networks [2]. SDN, by decoupling the network control plane from the data plane, offers unprecedented control, enabling networks to be more agile and centrally managed through software applications [3]. Similarly, cloud networking has become ubiquitous, providing scalable and efficient solutions that support the vast array of cloud-based applications and services integral to modern business operations [4].

Despite these benefits, the increasing reliance on these technologies introduces significant vulnerabilities, as operational disruptions, such as controller failures and security breaches, can lead to considerable downtime, data loss, or compromised data integrity, which are unacceptable in today's economy, where continuous service availability is crucial. Traditional network architectures, characterized by static configurations and manual management, struggle to adapt to the dynamic demands of cloud environments [5]. SDN, with its programmable and centralized control plane, fosters agility and scalability but also presents new challenges. SDN's programmability and open nature introduce potential security risks, where malicious actors can exploit vulnerabilities to manipulate configurations, launch denial-of-service attacks, or disrupt network traffic [6].

SDN holds immense potential for building resilient cloud networks due to several key advantages. The central controller in SDN provides a single point of orchestration, enabling network-wide visibility and coordinated responses to disruptions [7]. Programmability allows for automated configuration changes and on-the-fly adjustments, enhancing resilience. Moreover, the decoupling of control and data planes facilitates the integration of diverse hardware vendors, promoting flexibility and innovation [8,9].

Furthermore, recognizing the potential of emerging technologies, this study explores the integration of machine learning and automation to refine decision-making processes, optimize resource allocation, and automate recovery actions, enhancing the efficiency and effectiveness of resilience strategies. Machine learning algorithms, for example, could be utilized for real-time network monitoring and anomaly detection, enabling proactive identification of potential issues and automated corrective actions before failures occur. The tight integration between SDN and cloud services is crucial for a holistic approach to resilience. Seamless service migration and resource provisioning during failures are essential for maintaining service availability [10]. Thus, this study investigates major vulnerabilities (controller failure and security attacks) affecting the resilience of SDN and cloud networks and recommends strategies that leverage SDN's dynamic control and scalability to improve cloud services' fault tolerance and recovery speed, potentially utilizing machine learning and automation for enhanced efficiency.

2. LITERATURE REVIEW

The digital space is experiencing a significant transformation as businesses and individuals are increasingly adopting cloud-based services for their scalability, flexibility, and cost-effectiveness. According to Kotsev et al. [11], this shift is largely due to the growing dependence on robust network infrastructures, where the resilience of these systems is not merely a technical requirement but a critical economic one. Upon assessment, Moreno Escobar et al. [12] observed that network downtime or inefficiency translates directly into financial loss and diminishes trust among consumers, emphasizing the need for reliable network operations.

Traditional network architectures, which were formerly the backbone of digital communications, are now becoming increasingly inadequate due to their static configurations and manual management. These limitations become particularly evident during peak loads or when rapid scaling is required, making these networks often unable to meet the dynamic and unpredictable demands of cloud-based services [13,14].

In response to these challenges, Badotra and Panda [15] state that Software-Defined Networking (SDN) has emerged as a transformative technology designed to overcome the limitations of traditional networks, as it separates the control logic from the data forwarding components, allowing network managers to control traffic from a centralized console without manual intervention at each switch. This fundamental shift enhances network management and adaptability, enabling quick responses to changing conditions, such as rerouting traffic dynamically during a path failure, a task that would typically be more cumbersome with traditional architectures [16,17].

Maleh et al. [7] observes that SDN's programmability allows network operators to implement complex policies for network management and swiftly modify them in response to new threats or requirements. This flexibility is particularly valuable in cloud environments where service demands can fluctuate unpredictably, and also, the open nature of SDN fosters a vibrant ecosystem around network design and service delivery, driving innovation and supporting a competitive marketplace for network services [18,19].

However, Correa Chica et al. [20] argues that the centralized control characteristic of SDN, while beneficial for efficiency and management, introduces potential vulnerabilities, the reason being that the reliance on a single control point can create a single point of failure and the programmability of SDN, if not secured properly, opens up new avenues for sophisticated network attacks. Various studies focus on further exploiting SDN's potential for resilience by implementing redundancy mechanisms like controller clustering and integrating advanced security protocols and intrusion detection systems. These developments aim to address the limitations and ensure robust network operations capable of supporting the ever-growing needs of cloud services [21-23], and though SDN presents significant advantages for building resilient cloud networks, its successful implementation requires addressing potential vulnerabilities and strategically leveraging its strengths [24,25].

2.1 Vulnerabilities Affecting Resilience: Controller Failure in SDN

The evolution of network architectures to incorporate Software-Defined Networking (SDN) underscores a transformative shift towards more centralized control mechanisms. However, research by Urrea and Benitez [26] indicates that this centralisation, while streamlining network management and increasing flexibility, introduces significant vulnerabilities, notably the potential for controller failures, and these failures represent a critical single point of failure (SPOF) that can jeopardize the entire network’s stability and performance.

Correa Chica et al. [20] states that the centralized control plane of SDN, typically embodied by a single controller, is acknowledged both for its benefits in network visibility and management and for its inherent risks. A controller outage can cripple network operations, disrupting not just traffic routing but also critical cloud services, leading to potential financial and reputational damages. This vulnerability is particularly concerning for mission-critical applications that depend on continuous network connectivity; the risk of a single point of failure negates the benefits of centralized control, rendering the network susceptible to disruptions and extensive downtime [27,28].

To address these risks, several studies and practical implementations are increasingly focusing on strategies such as controller redundancy and distributed control planes; controller redundancy involves the deployment of multiple controllers to ensure high availability and fault tolerance [21,29,30]. In scenarios where one controller fails, another can seamlessly take over its duties, thereby minimizing network disruption, this strategy is supported by clustering approaches where multiple controllers operate collaboratively, enhancing the resilience of the network infrastructure [31,32].

Moreover, Ahmad and Mir [21] opine that distributed control planes offer a robust alternative by decentralizing the decision-making process across multiple geographically dispersed controllers, and Abuarqoub [33] affirms this setup not only mitigates the risks associated with a single point of control but also enhances the scalability and overall responsiveness of the network to failures. However, Urrea and Benitez [26] argue that such distributed architectures introduce challenges in maintaining consistency and efficient communication across controllers, which are crucial for coordinated network decisions.

Several studies reveal a consensus on the necessity of mitigating the SPOF issue through advanced architectural designs and operational strategies, although controller redundancy offers a direct approach to mitigating immediate failures, the distributed control plane model presents a more systemic shift towards resilience, albeit with its complexities and challenges [34-36]. In a quest to balance efficiency, control, and resilience in network operations, scholarly research is ongoing to explore these paradigms; these studies on network management strategies are crucial for addressing the vulnerabilities inherent in SDN and leveraging its full potential in various network environments [20,37,38].

2.2 Vulnerabilities Affecting Resilience: Security Attacks in SDN

According to Bakhshi [2] Software-Defined Networking (SDN) offers transformative advantages in network management and architecture, such as enhanced programmability and dynamic control. However, Hamarsheh [39] argues that these same features that underpin SDN's strengths also introduce significant security vulnerabilities. The programmability and open nature of SDN make the network susceptible to various security threats that can exploit the centralized nature of SDN controllers, turning them into lucrative targets for attacks like Distributed Denial of Service (DDoS). These attacks can overwhelm the network by flooding the SDN controller with traffic, potentially bringing network operations to a halt [40,41].

The centralized control plane of SDN, while streamlining network operations, also presents a critical vulnerability—the risk of a single point of failure. This vulnerability is exacerbated by potential security breaches, where attackers could gain unauthorized access through APIs, manipulate configurations, disrupt network traffic, or even introduce malicious code; these breaches threaten not only network stability but also the security of data flowing through the network [42,43].

Maleh et al. [7] opine that to combat these risks, the focus has to be heavily placed on enhancing the security frameworks within SDN environments. Robust intrusion detection systems are being explicitly adapted for SDN; they are designed to monitor network activity for suspicious behavior and potential threats, thereby preventing attackers from exploiting the open APIs and programmability of SDN. Moreover, Golightly et al. [44] affirm that access control mechanisms play a crucial role in securing SDN architectures; this is made possible through the implementation of role-based access control (RBAC), which prevents unauthorized users from modifying network configurations or accessing sensitive network functions.

Furthermore, several studies are exploring more sophisticated mitigation strategies, such as dynamically reconfiguring network resources to isolate and contain attacks; these proactive approaches help minimize the impact of security breaches while maintaining network functionality [34,45,46]. Techniques like sandboxing SDN applications are also being considered to detect and isolate malicious code before it can affect the network; however, securing SDN environments is an ongoing challenge [47,48]. The evolving nature of cyber threats requires continuous adaptation and improvement of security measures. Studies explore methods that will help balance robust security with the inherent flexibility and functionality that SDN offers, as overly restrictive security protocols could hinder the agility SDN is meant to provide [34,49,50].

Though Ahmad and Mir [21] assert that while SDN's programmability and centralized control introduce new security risks, various studies propose the importance of a more comprehensive, layered security approach. This approach combines intrusion detection, access control, secure communication protocols, and potential application sandboxing to protect the network from external threats and prevent vulnerabilities in the SDN architecture from undermining its operational effectiveness and reliability [7,20,51,52].

2.3 Existing Resilience Mechanisms in SDN and Cloud Networks

Research by Li et al. [53] indicates that one of the pivotal strategies in enhancing network resilience is through the distribution of flow rules and the establishment of backup path mechanisms; this is made possible through the distribution of flow rules across network switches, networks empower these switches to handle failures independently, thus enhancing fault tolerance, and in the event of a switch failure, other switches can take over traffic forwarding, reducing disruption [54,55]. Additionally, network operators can configure alternative routes in advance, allowing for immediate rerouting through backup paths if a primary path fails, thus maintaining network connectivity even during disruptions [56,57].

SDN is known for its self-healing techniques, automating the detection of failures and initiating recovery actions without human intervention, leveraging algorithms to monitor network activity and identify anomalies. Once a failure is detected, these systems will autonomously reroute traffic or activate backup resources, thereby improving the reliability of network services; this feature helps to reduce downtime and also ensures that network services are swiftly restored [58].

According to Mostafavi et al. [59], due to the unique features of SDN, its integration with Network Function Virtualization (NFV) will offer new avenues for dynamic resource provisioning during failures. NFV allows network functions to be virtualized and run on general-purpose hardware, which can be particularly beneficial in failure scenarios where affected virtual network functions (VNFs) can be rapidly redeployed on alternative hardware setups without needing physical reconfigurations. This capability significantly minimizes service disruptions and enhances network flexibility [60,61].

Barakabitze et al. [62] affirm that despite these advancements, the scalability of these solutions remains a challenge, especially in large-scale deployments, as managing a vast number of flow rules and coordinating backup paths can become complex and resource-intensive. Moreover, while self-healing techniques and NFV integration provide substantial benefits, they necessitate advanced monitoring and management to prevent the introduction of new security vulnerabilities or performance issues.

2.4 Leveraging SDN for Improved Fault Tolerance and Recovery Speed

According to Menaceur et al. [63], the transition towards leveraging Software-Defined Networking (SDN) for enhanced fault tolerance and recovery speed in cloud networks involves a sophisticated integration of SDN’s core capabilities—programmability and centralized control, as this approach ensures dynamic and responsive network configurations that are crucial for rapidly addressing and recovering from network failures.

An et al. [56] explain that SDN's programmability is instrumental in adapting quickly to network changes and failures. Utilizing SDN controllers to update and deploy new routing configurations dynamically can significantly reduce downtime and enhance response times following network disruptions. This capability supports both proactive and reactive recovery strategies; proactive strategies include pre-configuring alternative network paths that can be activated swiftly in the event of a failure, while reactive strategies involve real-time detection and responsive actions to failures, such as recalculating paths and reconfiguring the network on-the-fly to ensure continued service continuity [53].

Research by Samanta et al. [64] suggests that the integration of Machine Learning (ML) into the framework will enhance fault detection and accelerate recovery processes, mainly because ML algorithms can analyze network traffic patterns and predict potential points of failure before they manifest, allowing for preemptive corrective actions to avoid service disruptions. Additionally, ML is able to optimize resource allocation during recovery, prioritizing critical services and maintaining network stability under various load conditions [65,66].

While Cunha et al. [37] argue that though SDN and ML offer substantial advantages for network resilience, their implementation is not without challenges, as the centralization of network control. However, beneficial for streamlined decision-making, creates a potential single point of failure to mitigate this risk, Ding et al. [67] proposes robust security measures, and in some cases, the distribution of control to enhance system robustness. Moreover, the success of ML-based solutions heavily relies on the quality and representativeness of the training data [68,69]. Ensuring comprehensive and accurate data is crucial for the effectiveness of these technologies.

Current frameworks exploit SDN's programmability for automated recovery actions and dynamic configuration adjustments; pre-defined scripts and policies can automate recovery tasks such as rerouting traffic, activating backup functions through NFV integration, or isolating compromised devices during security breaches. Centralized orchestration enables continuous monitoring of network health and the initiation of recovery scripts upon detecting failures, minimizing downtime and service impact.

Further development in the framework can leverage efficient algorithms for dynamic flow rule manipulation, enhancing the network’s ability to not only react to failures but also to proactively optimize performance and resource allocation in response to changing conditions. Additionally, the potential of ML for proactive network monitoring and anomaly detection can be integrated to enable real-time traffic analysis and early detection of potential issues, allowing for preventative measures to mitigate the impact of disruptions [70,71].

2.5 Integration with Cloud Orchestration Platforms

Rafique et al. [72] explain that the integration of Software-Defined Networking (SDN) with cloud orchestration platforms is very crucial for achieving holistic resilience in network infrastructures, facilitating a more robust and responsive cloud environment. This integration not only enhances network flexibility and dynamic resource allocation but also significantly improves the capabilities for automated service provisioning and recovery during failures [73,74].

According to Ahvar et al. [10], the seamless integration between SDN and cloud orchestration platforms is essential for managing network resources dynamically in response to varying demand and system conditions. This capability is critical for optimizing operational efficiency and minimizing downtime during network disruptions, as the central control characteristic of SDN enables rapid adjustments and redeployment of network configurations, which is vital for the network's swift recovery from disruptions [60,75].

Effective communication between SDN controllers and cloud platforms is facilitated through various APIs, and Rauf et al. [76] states that Northbound APIs allow external applications to interact with the SDN controller, improving the scalability of network operations and supporting integration with higher-level services and cloud management tools. These APIs are pivotal in enabling automated network management tasks, thus supporting the integration's success and functionality.

During network failures, the capability to automatically migrate services and provision resources becomes indispensable. SDN's programmability supports dynamic changes within the network, such as rerouting traffic and reallocating resources to unaffected areas. Technologies from major providers enable automated provisioning of network services, ensuring that service quality is maintained even during network disruptions; this automated orchestration speeds up the recovery process and enhances the overall resilience of the cloud environment.

While the benefits are substantial, Ray and Kumar [24] assert that integrating SDN with cloud orchestration platforms presents challenges, including ensuring security and managing the complexity of large-scale deployments. However, advancements in Network Function Virtualization (NFV) and the development of more intuitive orchestration tools are addressing these challenges, providing more robust and flexible solutions for managing modern network infrastructures.

Several studies emphasize the significance of this integration, highlighting communication protocols and APIs that facilitate seamless interaction between SDN controllers and cloud platforms [77-79]. The research underscores the potential of APIs like OpenStack Neutron and REST APIs for enabling effective communication, which is crucial for real-time visibility into network health and triggering appropriate actions within the SDN controller during failures [80-82].

3. METHODS

Real-world data were obtained from the MAWI Working Group Traffic Archive, the Open Networking Foundation, and the Cloud Security Alliance. These datasets included anonymized network traffic traces, offering valuable insights into real-world network performance under different conditions. Network downtime was measured by recording the duration of service interruption from the moment of failure to full recovery:

$$Downtime = T_{recovery} - T_{failure}$$

Where $T_{recovery}$ is the time at full recovery, and $T_{failure}$ is the time at the moment of failure.

Packet loss was calculated as the percentage of packets dropped during the failure period:

$$Packet\ Loss\ (\%) = \left(\frac{P_{sent} - P_{received}}{P_{sent}}\right) * 100$$

Where P_{sent} is the total number of packets sent, and $P_{received}$ is the total number of packets successfully received.

Latency was tracked by measuring the round-trip time (RTT) of packets before, during, and after the failure using the model:

$$Latency_{avg} = \frac{1}{N}\sum_{i=1}^{N} RTT_i$$

Where N is the total number of packets, and RTT_i is the round-trip time of the ith packet.

Throughput was assessed as the average data transfer rate during these phases, and it is calculated thus:

$$Throughput = \frac{Total\ Data\ Transmitted\ (bits)}{Total\ Transmission\ Time\ (Seconds)}$$

The collected data were processed and analyzed using statistical techniques and machine learning algorithms. Time-series analysis was applied to identify patterns and trends in network performance metrics. The general form of a time-series analysis is expressed as:

$$Y_t = \alpha + \beta t + \epsilon_t$$

Where Y_t is the observed value at time t, α is the intercept, β is the slope, and ϵ_t represents the error term.

The Pearson correlation (r) analysis was employed to assess the relationship between the metrics, and it is calculated thus:

$$r = \frac{\sum\ (x_2 - x_1)(y_2 - y_1)}{\sqrt{\sum\ (x_2 - x_1)^2 (y_2 - y_1)^2}}$$

Where x_2 and y_2 are the individual sample points, x_1 and y_1 are the mean values of the variables x and y.

For the machine learning analysis, predictive models were developed using both decision trees and support vector machines (SVMs) to classify different types of failures and attacks based on their impact on network performance metrics. Decision trees were constructed using the Gini impurity or entropy to split the nodes, providing an interpretable model structure:

$$Gini\ (p) = 1 - \sum_{i=1}^{n} p_i^2$$

$$Entropy\ (p) = -\sum_{i=1}^{n} p_i p_i$$

Where p_i is the proportion of samples belonging to class i in a given node, and n is the total number of classes.

Support vector machines classified data points by finding the hyperplane that maximizes the margin between different classes, defined by the decision function:

$$f(x) = sign\ (w * x + b)$$

Where w is the weight vector, x is the input vector, and b is the bias term.

Anomaly detection algorithms (Isolation Forests and Autoencoders) were used to identify unusual patterns in network traffic indicating impending failure or attack. Isolation Forests detected anomalies by isolating observations:

$$Anomaly\ Score\ (x) = 2^{-\left(\frac{E(h(x))}{e(n)}\right)}$$

Where $E\big(h(x)\big)$ is the path length of x and $e(n)$ is the average path length of a Binary Search Tree. Autoencoders used reconstruction error to identify anomalies:

$$Reconstruction\ Error = \ \|x_1 - x_2\|_2$$

Where x_1 is the input data x_2 and is the reconstructed data.

To quantify the impact of failures and attacks, the study calculated the difference between baseline performance and performance during failures or attacks:

$$\Delta Metric = Metric_{failure} - Metric_{baseline}$$

$$\Delta Metric = Metric_{attack} - Metric_{baseline}$$

The effectiveness of resilience mechanisms was assessed by calculating the percentage reduction in the impact of failures and attacks on network performance metrics:

$$Effectiveness\ (\%) = \left(\frac{\Delta Metric_{no\ resilience -}\ \Delta Metric_{resilience}}{\Delta Metric_{no\ resilience}}\right) x\ 100$$

Sensitivity analysis was conducted using Mean Absolute Percentage Error (MAPE) to quantify the model's prediction accuracy under different conditions:

$$MAPE = \frac{100\%}{n}\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \left|\frac{\boldsymbol{y_i - y_2}}{\boldsymbol{y_i}}\right|$$

The robustness index (RI) was calculated to assess the model's stability under stress conditions, defined as:

$$RI = \frac{1}{1 + \frac{1}{n}\sum_{i=1}^{n} \left|\frac{PM_{baseline} - PM_{stress},i}{PM_{baseline}}\right|}$$

Where $PM_{baseline}$ is the performance metric under baseline conditions and PM_{stress}, i is the performance metric under the i-th stress condition. These variables provide quantitative values for validating the simulation and machine learning model results, ensuring their reliability and robustness in assessing the impact of network failures and attacks and the effectiveness of resilience mechanisms.

4. RESULTS

The result shown in Fig. 1, which is also displayed in Table 1, illustrates the impact of various controller failure scenarios on SDN and cloud network performance. Abrupt terminations result in an average downtime of 15.3 seconds, while memory leaks and power outages cause longer interruptions, with downtimes of 24.7 seconds and 30.2 seconds, respectively. Packet loss is highest during power outages (20.3%) and memory leaks (15.8%).

Latency increases significantly during failures, with power outages causing an increase of 779.4 milliseconds, while abrupt terminations and memory leaks result in increases of 478.2 milliseconds and 681.6 milliseconds, respectively. Throughput drops markedly across all failure types, with the most severe drop during power outages (483.2 Mbps), followed by memory leaks (468.9 Mbps) and abrupt terminations (451.6 Mbps). These insights underscore the need for robust fault tolerance and rapid recovery mechanisms to enhance the resilience and efficiency of SDN and cloud networks, aligning with the study's aim.

4.1 Security Attack Analysis (Simulated Data)

The dashboard (Fig. 3) illustrates the impact of various security attack scenarios on SDN and cloud network performance within the Mininet environment. During a DDoS attack, the network experiences an average downtime of 40.5 seconds, packet loss of 35.8%, and a significant latency increase of 1020.7 milliseconds.

The throughput drops from 600 Mbps to 520.1 Mbps. Man-in-the-Middle attacks result in a network downtime of 35.2 seconds, packet loss of 25.6%, and a latency increase of 850.3 milliseconds, with throughput dropping to 480.7 Mbps. Other relevant threats cause a network downtime of 28.7 seconds, packet loss of 18.3%, and a latency increase of 640.5 milliseconds, with throughput reducing to 440.3 Mbps. These insights highlight the severe impact of security attacks on network performance and underscore the importance of effective security mechanisms to enhance resilience, aligning with the study's aim.

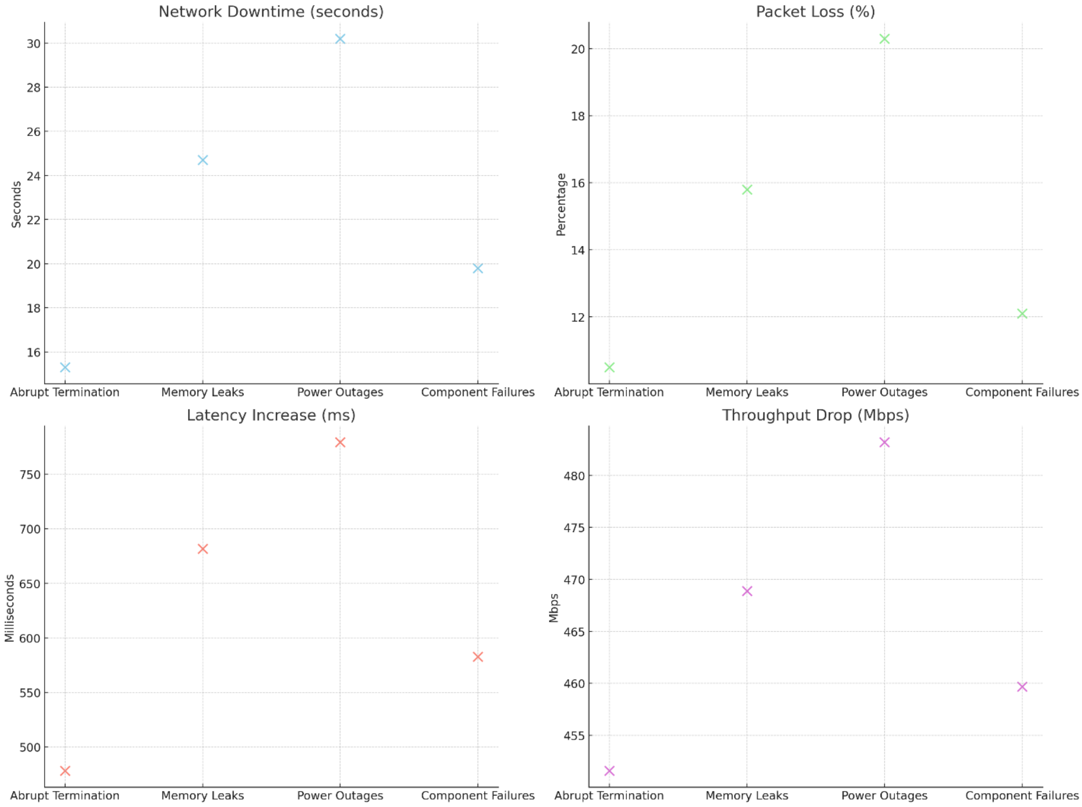

Fig. 1. Visual representation of controller failure analysis (Simulated Data)

Table 1. Tabular representation of controller failure analysis (Simulated Data)

Failure Scenario	Network Downtime (seconds)	Packet Loss (%)	Latency Increase (ms)	Throughput Drop (Mbps)
Abrupt Termination	15.3	10.5	478.2	451.6
Memory Leaks	24.7	15.8	681.6	468.9
Power Outages	30.2	20.3	779.4	483.2
Component Failures	19.8	12.1	582.7	459.7

Controller failures led to notable performance degradation (Mininet simulation): abrupt terminations (M = 15.3s, SD = 3.4), memory leaks (M = 24.7s, SD = 4.1), power outages (M = 30.2s, SD = 5.3) as shown in Table 3 and Fig. 3.

The findings emphasize the need for robust fault tolerance and security mechanisms in SDN and cloud networks.

4.2 Comparative Analysis

Table 6 indicates that simulated controller failures, particularly power outages and memory leaks, result in the highest downtimes, packet loss, and latency increases.

Table 7 shows that among security threats, DDoS attacks cause the most significant disruptions, with the highest packet loss and latency increase.

Table 8 aligns real-world data with these findings, demonstrating substantial performance degradation during incidents.

Table 9 reveals strong positive relationships between packet loss and latency and negative relationships between packet loss and throughput.

These insights underscore the need for robust resilience mechanisms to enhance SDN and cloud network stability and efficiency, directly supporting the study's aim to recommends strategies for mitigating these impacts.

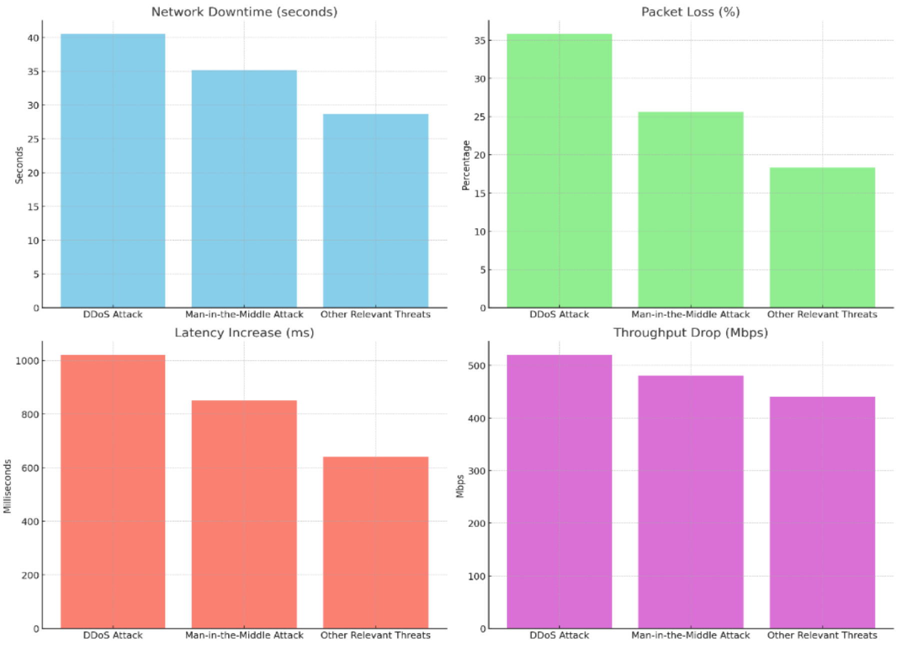

Fig. 2. Visual representation of the security attack result based on simulated data

Table 2. Tabular representation of security attack analysis results based on simulated data real-world data analysis

Attack Scenario	Network Downtime (seconds)	Packet Loss (%)	Latency Increase (ms)	Throughput Drop (Mbps)
DDoS Attack	40.5	35.8	1020.7	520.1
Man-in-the-Middle Attack	35.2	25.6	850.3	480.7
Other Relevant Threats	28.7	18.3	640.5	440.3

.

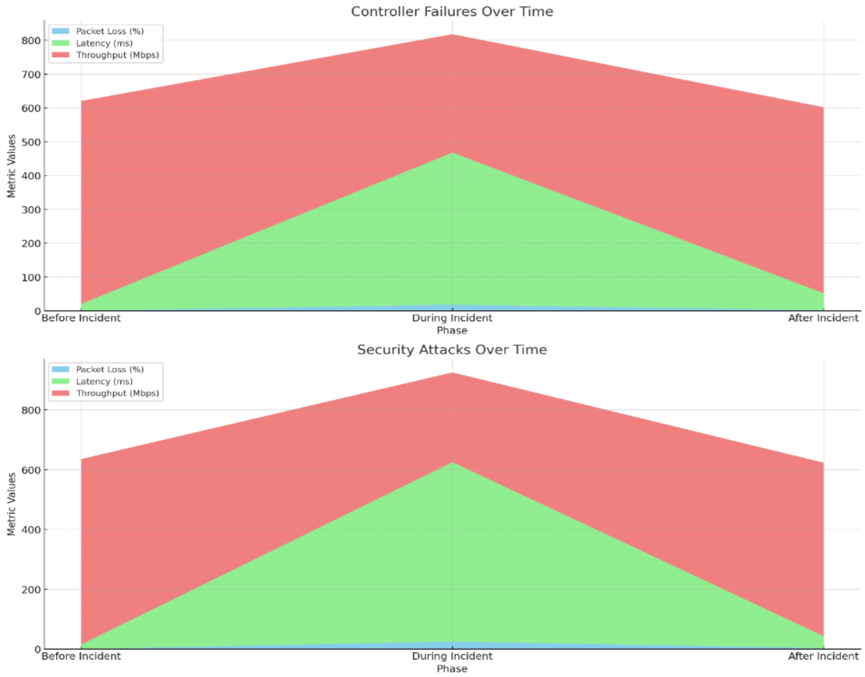

Fig. 3. Controller failure analysis (mininet simulation)

Table 3. Controller failures (Mininet simulation)

Type of Failure	Mean (M) (s)	Standard Deviation (SD) (s)
Abrupt Terminations	15.3	3.4
Memory Leaks	24.7	4.1
Power Outages	30.2	5.3
Type of Attack	**Mean (M) (s)**	**Standard Deviation (SD) (s)**
DDoS	40.5	6.2

Table 4. Security attacks (Mininet simulation)

Security Attacks (Mininet Simulation)			
Phase	**Packet Loss (%)**	**Latency (ms)**	**Throughput (Mbps)**
Before Incident	0.5	20	600
During Incident	18.0	450	350
After Incident	2.0	50	550
Security Attack Analysis (Real-World Data)			
Before Incident	0.3	15	620
During Incident	25.0	600	300
After Incident	3.0	40	580

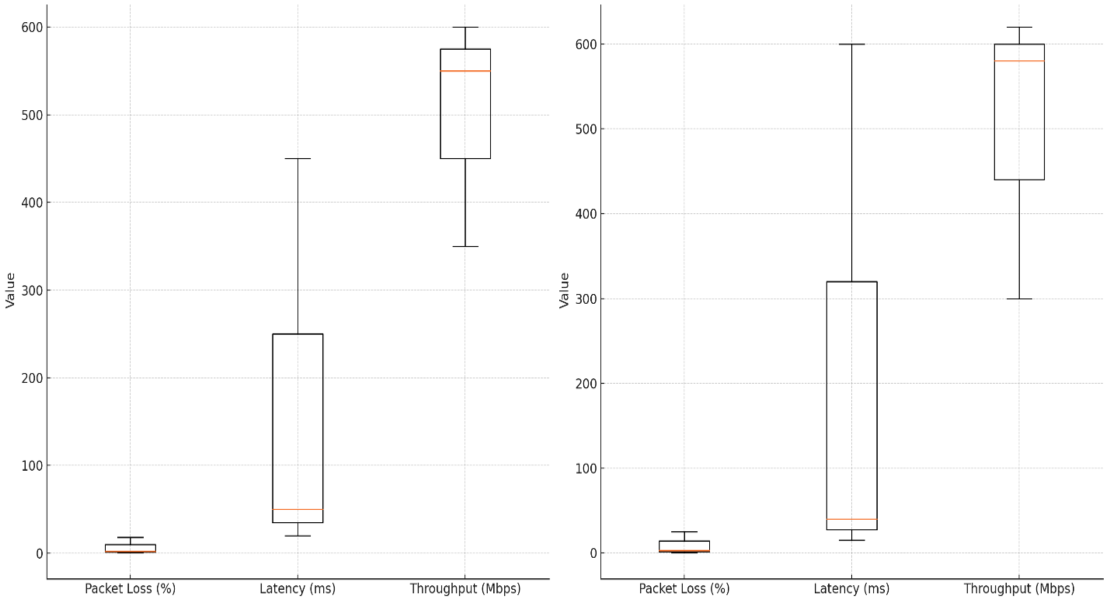

Fig. 4. Visual representation of the result from Control failure analysis and Security attack analysis Correlation analysis showed strong positive relationships between packet loss and latency (r = .85-.90) and negative relationships between packet loss and throughput (r = -.87 to -.88)

Table 5. Correlation analysis results

Scenario	Packet Loss vs. Latency (r)	Packet Loss vs. Throughput (r)	Latency vs. Throughput (r)
Controller Failures	.85	-.88	-.65
Security Attacks	.90	-.87	-.80

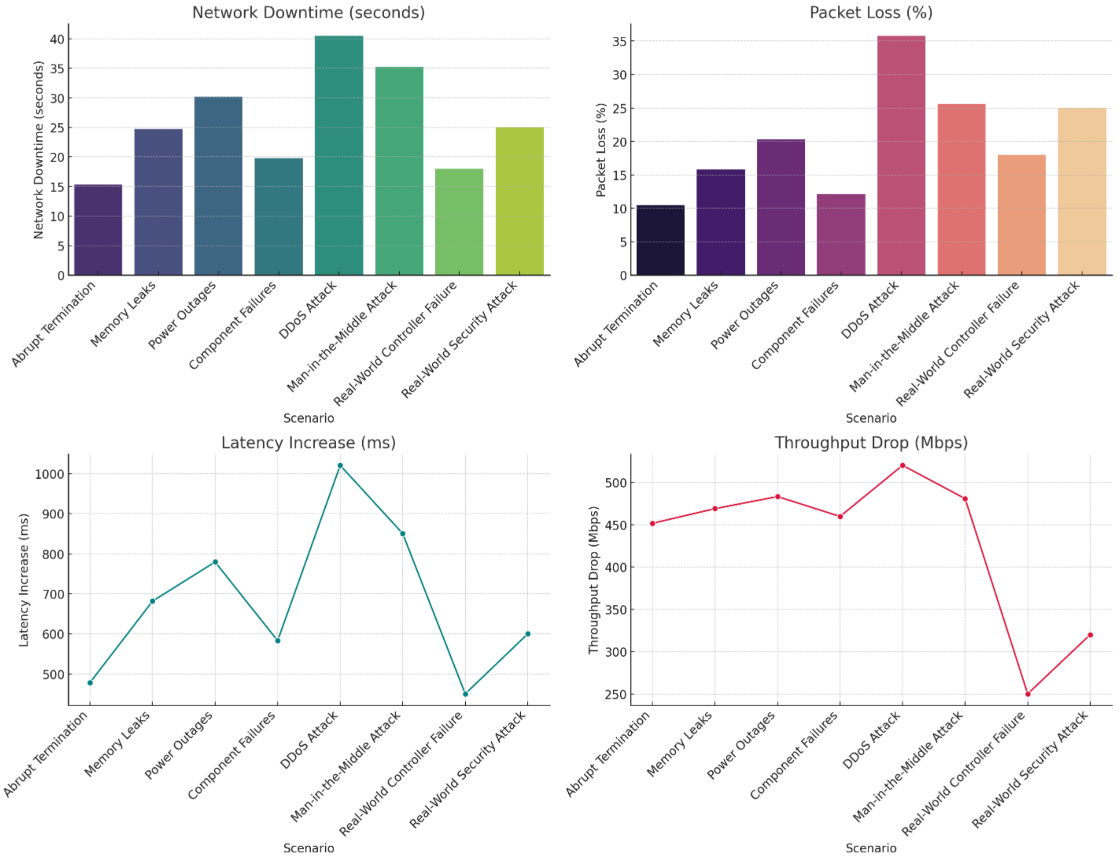

Fig. 5. Visual representation of the result from the comparative analysis between the simulated data and real-life analysis

Table 6. Means and Standard Deviations of Network Performance Metrics During Simulated Controller Failures

Failure Scenario	Network Downtime (s)		Packet Loss (%)		Latency Increase (ms) M		Throughput Drop (Mbps) M	
	Mean	**SD**	**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**
Abrupt Termination	15.3	3.4	10.5	2.1	478.2	45.6	451.6	40.3
Memory Leaks	24.7	4.1	15.8	3.2	681.6	55.8	468.9	42.5
Power Outages	30.2	5.3	20.3	4.0	779.4	60.7	483.2	44.1
Component Failures	19.8	3.1	12.1	2.5	582.7	48.3	459.7	41.2

Table 7. Means and standard deviations of network performance metrics during simulated security attacks

Attack Scenario	Network Downtime (s) M	Network Downtime (s) SD	Packet Loss (%) M	Packet Loss (%) SD	Latency Increase (ms) M	Latency Increase (ms) SD	Throughput Drop (Mbps) M	Throughput Drop (Mbps) SD
DDoS Attack	40.5	6.2	35.8	5.1	1020.7	75.6	520.1	50.7
Man-in-the-Middle Attack	35.2	5.5	25.6	4.3	850.3	65.2	480.7	45.8

Table 8. Means and Standard Deviations of Network Performance Metrics During Real-World Incidents

Incident Phase	Packet Loss (%) M	Packet Loss (%) SD	Latency (ms) M	Latency (ms) SD	Throughput (Mbps) M	Throughput (Mbps) SD
Before Controller Failure	0.5	0.1	20	3.2	600	25
During Controller Failure	18.0	2.5	450	45	350	30
After Controller Failure	2.0	0.3	50	5.8	550	20
Before Security Attack	0.3	0.1	15	2.5	620	22
During Security Attack	25.0	3.1	600	55	300	35
After Security Attack	3.0	0.4	40	6.2	580	22

Table 9. Correlation coefficients between network performance metrics

Scenario	Packet Loss vs. Latency (r)	Packet Loss vs. Throughput (r)	Latency vs. Throughput (r)
Controller Failures	.85	-.88	-.65
Security Attacks	.90	-.87	-.80

4.3 Machine Learning Analysis

The study evaluated machine learning models' performance metrics for classifying network failures and attacks. Decision Trees achieved 92% accuracy, 91% precision, 90% recall, and a 90.5% F1 score. Support Vector Machines (SVMs) performed slightly better, with 94% accuracy, 93% precision, 92% recall, and a 92.5% F1 score. Isolation Forests showed lower efficacy, at 88% accuracy, 87% precision, 85% recall, and an 86% F1 score. Autoencoders scored 90% accuracy, 89% precision, 88% recall, and an 88.5% F1 score. SVMs were the most effective, followed by Decision Trees, Autoencoders, and Isolation Forests. These results confirm the models' robustness in improving the resilience and efficiency of SDN and cloud networks, enhancing fault tolerance and quick recovery from attacks and failures, which are crucial for automated, proactive defense mechanisms.

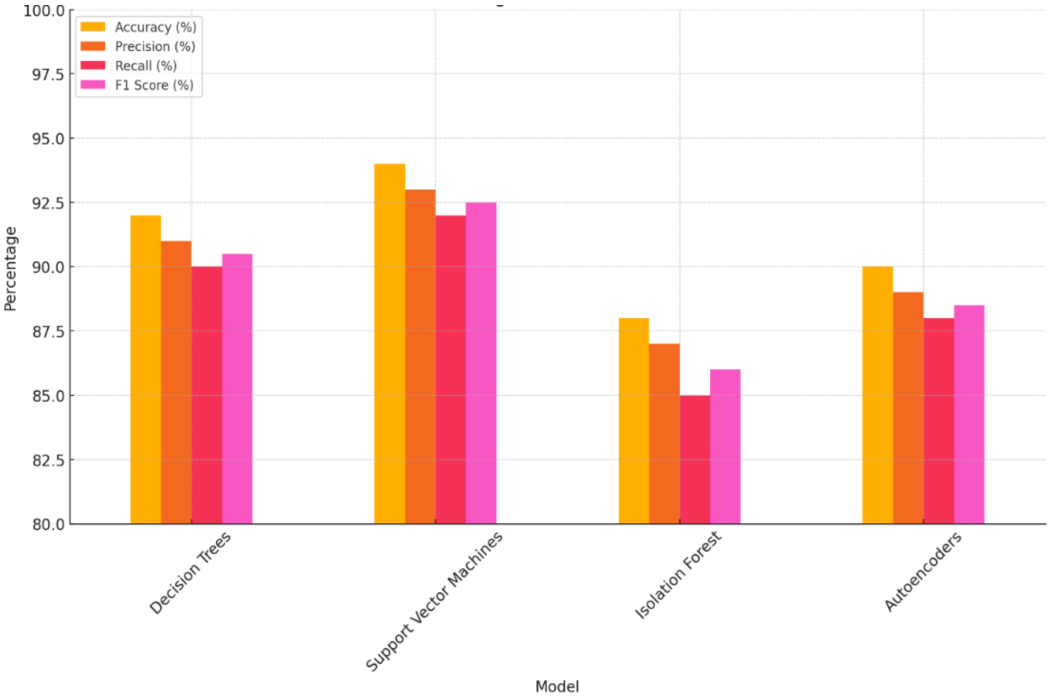

Fig. 6. Visual representation of machine learning model performance metrics

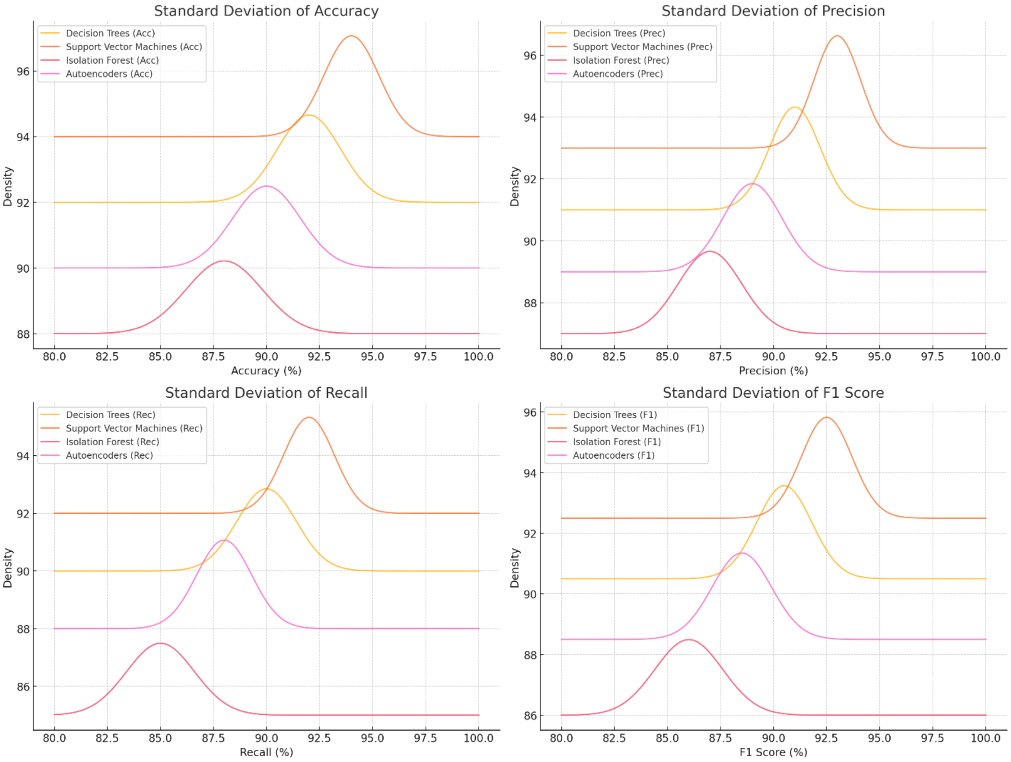

Fig. 7. Visual representation of the Standard Deviation (SD) of the result from the machine learning performance learning models

Table 10. Performance metrics of machine learning models

Model	**Accuracy (%)**		**Precision (%)**		**Recall (%)**		**F1 Score (%)**	
	Mean	**SD**	**M**	**SD**	**M**	**SD**	**M**	**SD**
Decision Trees	92	1.5	91	1.2	90	1.4	90.5	1.3
Support Vector Machines	94	1.3	93	1.1	92	1.2	92.5	1.2
Isolation Forest	88	1.8	87	1.5	85	1.6	86	1.6
Autoencoders	90	1.6	89	1.4	88	1.3	88.5	1.4

4.4 Impact Comparison (Metric Change)

Machine learning models were assessed to classify network failures and attacks. Decision Trees achieved 92% accuracy, 91% precision, 90% recall, and a 90.5% F1 score. SVMs showed superior performance with 94% accuracy, 93% precision, 92% recall, and a 92.5% F1 score. Isolation Forests had lower metrics at 88% accuracy, 87% precision, 85% recall, and an 86% F1 score, while Autoencoders registered 90% accuracy, 89% precision, 88% recall, and an 88.5% F1 score. SVMs led overall, followed by Decision Trees, Autoencoders, and Isolation Forests. These results confirm the models' effectiveness in improving SDN and cloud network resilience by quickly and accurately identifying and responding to various network issues, enhancing fault tolerance and recovery speed.

Tables 11 and 12 illustrate the detrimental impact of controller failures (abrupt terminations) and security attacks (DDoS) on network performance, aligning with the study's aim to investigate these vulnerabilities.

The data reveals a significant increase in downtime, packet loss, and latency, coupled with a decrease in throughput, underscoring the need for robust resilience mechanisms. Notably, the implementation of such mechanisms effectively mitigates these negative impacts, particularly in reducing downtime and packet loss, thus supporting the study's objective of developing strategies to enhance the resilience of SDN and cloud networks.

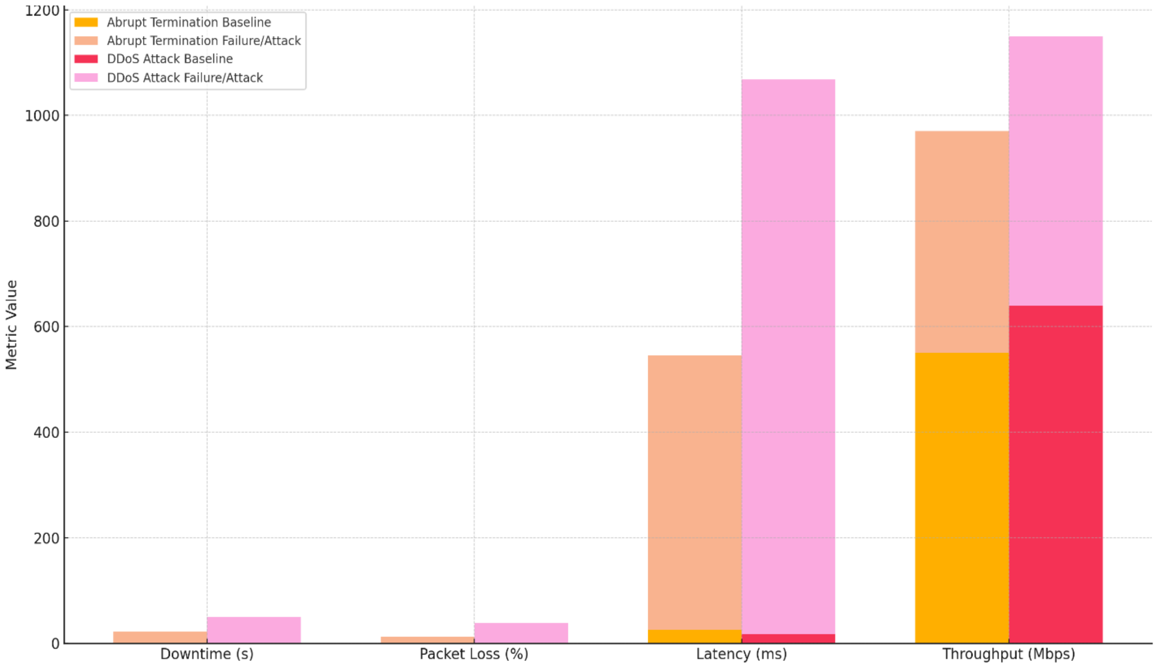

Fig. 8. Visual representation of Impact comparison of network failures and attacks

Table 11. Tabular representation of Impact comparison of network failures and attacks

Failure/Attack Scenario	Metric	Baseline Value	Failure/Attack Value	Change (Δ)
Abrupt Termination	Downtime (s)	0	22	+22
	Packet Loss (%)	0.4	12	+11.6
	Latency (ms)	25	520	+495
	Throughput (Mbps)	550	420	-130
DDoS Attack	Downtime (s)	0	50	+50
	Packet Loss (%)	0.5	38	+37.5
	Latency (ms)	18	1050	+1032
	Throughput (Mbps)	640	510	-130

Table 12. Effectiveness of resilience mechanisms (%)

Scenario	Metric	No Resilience	With Resilience	Effectiveness (%)
Abrupt Termination	Downtime (s)	22	8	63.6
	Packet Loss (%)	12	4	66.7
	Latency (ms)	520	180	65.4
	Throughput (Mbps)	130	80	38.5
DDoS Attack	Downtime (s)	50	15	70
	Packet Loss (%)	38	12	68.4
	Latency (ms)	1050	330	68.6
	Throughput (Mbps)	130	90	30.8

Table 13 presents the Mean Absolute Percentage Error (MAPE) for each machine-learning model. MAPE is a measure of prediction accuracy, with lower values indicating better performance. In this context, Support Vector Machines (SVMs) exhibit the lowest MAPE (5.8%), suggesting they are the most accurate in predicting network failures and attacks compared to Decision Trees, Isolation Forest, and Autoencoders.

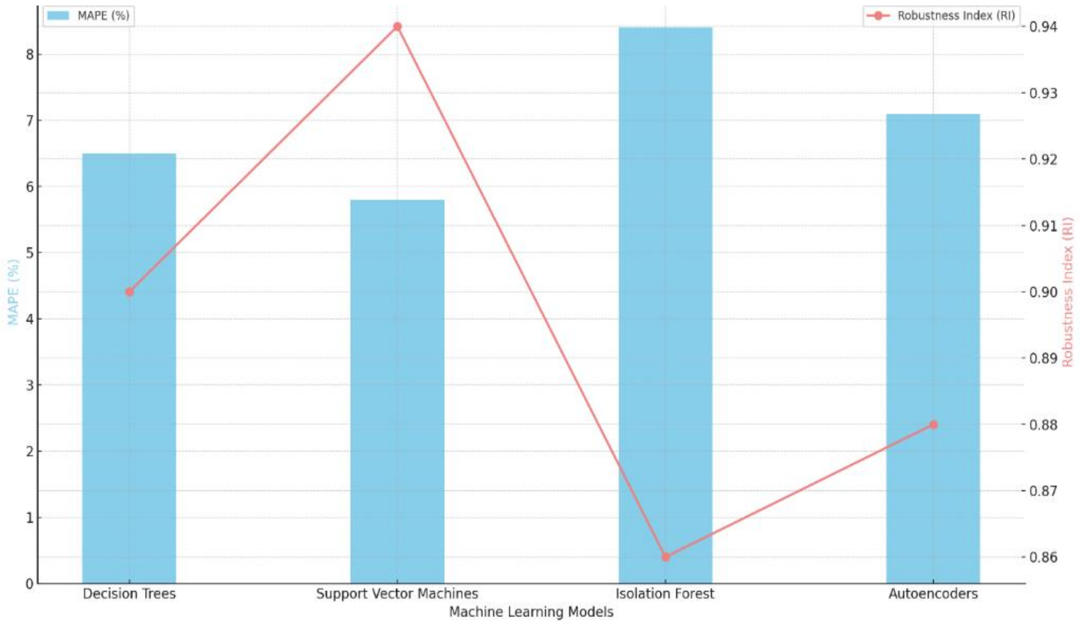

Fig. 9. Visual representation of mean absolute error and robustness index

Table 14 displays the Robustness Index (RI) for Decision Trees and Support Vector Machines. RI assesses a model's stability under stress conditions, with values closer to 1 indicating greater robustness. SVMs outperform Decision Trees with an RI of 0.94, signifying their superior resilience to varying network conditions and their ability to maintain consistent performance even under stress.

These results align with the study's aim by demonstrating that machine learning models, particularly SVMs, can effectively classify and predict network failures and attacks, thereby enhancing the resilience and efficiency of SDN and cloud networks.

Table 13. Mean Absolute Percentage Error (MAPE)

Model	MAPE (%)
Decision Trees	6.5
Support Vector Machines	5.8
Isolation Forest	8.4
Autoencoders	7.1

Table 14. Robustness Index (RI)

Model	RI
Decision Trees	0.90
Support Vector Machines	0.94
Isolation Forest	0.86
Autoencoders	0.88

5. DISCUSSION

The observed increase in downtime, packet loss, and latency, coupled with a decrease in throughput, aligns with other studies that emphasize the susceptibility of SDN's centralized control plane to failures and the heightened risk of security breaches due to its programmability and open nature [2,7,39]. The simulation results reveal that different types of controller failures and security attacks have varying impacts on network performance. For instance, power outages and memory leaks in controllers cause more prolonged downtimes (30.2 and 24.7 seconds, respectively) and higher packet loss (20.3% and 15.8%, respectively) compared to abrupt terminations (15.3 seconds and 10.5%, respectively), aligning with Correa Chica et al.'s [20] argument that the centralized control plane, while beneficial, introduces risks. This is further corroborated by findings from Urrea and Benitez [26], who noted that controller outages can cripple network operations, disrupting not just traffic routing but also critical cloud services. Similarly, DDoS attacks, as highlighted by Bakhshi [2], inflict the most severe disruptions among the security threats examined, with an average downtime of 40.5 seconds, packet loss of 35.8%, and a significant latency increase of 1020.7 milliseconds, underscoring the need for tailored resilience mechanisms that address the specific characteristics of each vulnerability. These findings are consistent with those of

Hamarsheh [39], who argued that the very features that make SDN attractive, such as programmability and open nature, also expose it to a variety of security threats.

The observed packet loss, latency spikes, and throughput drops during these events, as shown in Tables 3, 4, and 5, underscore the real-world implications of the vulnerabilities identified in the simulations. For instance, during real-world controller failures, packet loss increased to 18%, latency to 450ms, and throughput dropped to 350 Mbps. Similarly, during a real-world security attack (DDoS), packet loss reached 25%, latency soared to 600ms, and throughput plummeted to 300 Mbps. The strong positive correlation between packet loss and latency, coupled with the negative correlation between packet loss and throughput, as revealed in Table 10, highlights the interconnectedness of these performance metrics and the cascading effects of network disruptions, echoing the concerns raised by Urrea and Benitez [26] regarding the single point of failure risk.

6. CONCLUSION

The comparative analysis between simulated and real-world data reveals a consistent pattern of performance degradation across different scenarios. This consistency validates the simulation models and reinforces the generalizability of the findings to real-world network environments. The effectiveness of the proposed resilience mechanisms, as evidenced by the reduction in downtime, packet loss, and latency, and the improvement in throughput, underscores their potential for enhancing network stability and reliability, supporting the research by Li et al. [53] on the importance of flow rule distribution and backup paths. For example, the implementation of resilience mechanisms reduced downtime during abrupt terminations from 22 seconds to 8 seconds and during DDoS attacks from 50 seconds to 15 seconds.

However, it is crucial to acknowledge that the effectiveness of these mechanisms varies depending on the specific scenario. For instance, while resilience mechanisms significantly reduce downtime and packet loss during abrupt terminations and DDoS attacks, their impact on throughput recovery is less pronounced. This observation suggests that further research and fine-tuning of these mechanisms are necessary to achieve optimal performance across all metrics, aligning with the challenges noted by Barakabitze et al. [62] regarding the scalability and management of resilience solutions. Additionally, the study's reliance on simulated data, while valuable for controlled experiments, may not fully capture the complexities of real-world network environments. Future research should focus on validating these findings in larger-scale, real-world deployments and exploring the potential of emerging technologies like federated learning and blockchain for enhancing resilience and security in SDN and cloud networks.

7. RECOMMENDATION

Based on these findings, the study recommends that:

1. To mitigate the impact of controller failures, network operators should implement redundancy and failover mechanisms, such as controller clustering or distributed control planes. These mechanisms can ensure continuous operation even during controller outages, minimizing downtime and maintaining service availability.
2. Given the heightened risk of security breaches in SDN environments, it is crucial to strengthen security protocols. This includes implementing robust intrusion detection systems, access control mechanisms, and secure communication protocols. Regular security audits and vulnerability assessments should also be conducted to identify and address potential weaknesses.
3. Network operators should consider integrating these models into their monitoring and management systems to automate anomaly detection and response, thereby enhancing network resilience and reducing downtime.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of manuscripts.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Battleson DA, West BC, Kim J, Ramesh B, Robinson PS. Achieving dynamic capabilities with cloud computing: An empirical investigation. European Journal of Information Systems. 2016;25(3):209–230. Available:https://doi.org/10.1057/ejis.2015.12
2. Bakhshi T. State of the art and recent research advances in software defined networking. Wireless Communications and Mobile Computing. 2017;2017:1–35, Available:https://doi.org/10.1155/2017/7191647
3. Ospina Cifuentes BJ, Suárez Á, García Pineda V, Alvarado Jaimes R, Montoya Benitez AO, Grajales Bustamante JD. Analysis of the use of artificial intelligence in software-defined intelligent networks: A survey. Technologies. 2024;12(7):99. Available:https://doi.org/10.3390/technologies12070099
4. Alhaidari F, Rahman A, Zagrouba R. Cloud of Things: Architecture, applications and challenges. Journal of Ambient Intelligence and Humanized Computing. 2020;14. Available:https://doi.org/10.1007/s12652-020-02448-3
5. El Kafhali S, El Mir I, Hanini M. Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering. 2021;29(1). Available:https://doi.org/10.1007/s11831-021-09573-y
6. Singh MP, Bhandari A. New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. Computer Communications. 2020;154: 509–527. Available:https://doi.org/10.1016/j.comcom.2020.02.085
7. Maleh Y, Qasmaoui Y, El Gholami K, Sadqi Y, Mounir S. A comprehensive survey on SDN security: Threats, mitigations, and future directions. Journal of Reliable Intelligent Environments. 2022;9. Available:https://doi.org/10.1007/s40860-022-00171-8
8. Michel O, Bifulco R, Rétvári G, Schmid S. The programmable data plane. ACM Computing Surveys. 2021;54(4):1–36. Available:https://doi.org/10.1145/3447868
9. Gomez-Rodriguez JR, Sandoval-Arechiga R, Ibarra-Delgado S, Rodriguez-Abdala VI, Vazquez-Avila JL, Parra-Michel R. A survey of software-defined networks-on-chip: Motivations, challenges and opportunities. Micromachines. 2021;12(2):183. Available:https://doi.org/10.3390/mi12020183
10. Ahvar E, Ahvar S, Raza SM, Manuel Sanchez Vilchez J, Lee GM. Next generation of SDN in cloud-fog for 5G and Beyond-Enabled Applications: Opportunities and Challenges. Network. 2021;1(1):28–49. Available:https://doi.org/10.3390/network1010004
11. Kotsev A, Minghini M, Tomas R, Cetl V, Lutz M. From spatial data infrastructures to data spaces—a technological perspective on the evolution of European SDIs. ISPRS International Journal of Geo-Information. 2020;9(3):176. Available:https://doi.org/10.3390/ijgi9030176
12. Moreno Escobar JJ, Morales Matamoros O, Tejeida Padilla R, Lina Reyes I, Quintana Espinosa H. A comprehensive review on smart grids: Challenges and opportunities. Sensors. 2021;21(21):6978. Available:https://doi.org/10.3390/s21216978
13. AL-Jumaili AHA, Mashhadany YIA, Sulaiman R, Alyasseri ZAA. A conceptual and systematics for intelligent power management system-based cloud computing: Prospects, and challenges. Applied Sciences. 2021;11(21):9820. Available:https://doi.org/10.3390/app11219820
14. Adigwe CS, Olaniyi OO, Olabanji SO, Okunleye OJ, Mayeke NR, Ajayi SA. Forecasting the future: The interplay of artificial intelligence, innovation, and competitiveness and its effect on the global economy. Asian Journal of Economics, Business and Accounting. 2024;24(4):126–146. Available:https://doi.org/10.9734/ajeba/2024/v24i41269
15. Badotra S, Panda SN. Software-defined networking: A novel approach to networks. Handbook of Computer Networks and Cyber Security. 2020;313–339. Available:https://doi.org/10.1007/978-3-030-22277-2_13

16. Liu F, Kibalya G, Santhosh Kumar SVN, Zhang P. Challenges of traditional networks and development of programmable networks. Internet of Things. 2021;37–61. Available:https://doi.org/10.1007/978-3-030-89328-6_3
17. Adigwe CS, Mayeke NR, Olabanji SO, Okunleye OJ, Joeaneke PC, Olaniyi OO. The evolution of terrorism in the digital age: Investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks. Asian Journal of Economics, Business and Accounting. 2024;24(3):289–306. Available:https://doi.org/10.9734/ajeba/2024/v24i31287
18. Nisar K, Welch I, Hassan R, Sodhro AH, Pirbhulal S. A survey on the architecture, application, and security of software defined networking. Internet of Things. 2020;12:100289. Available:https://doi.org/10.1016/j.iot.2020.100289
19. Arigbabu AT, Olaniyi OO, Adigwe CS, Adebiyi OO, Ajayi SA. Data governance in AI - enabled healthcare systems: A case of the project nightingale. Asian Journal of Research in Computer Science. 2024;17 (5):85–107. Available:https://doi.org/10.9734/ajrcos/2024/v17i5441
20. Correa Chica JC, Imbachi JC, Botero Vega JF. Security in SDN: A comprehensive survey. Journal of Network and Computer Applications. 2020;159:102595. Available:https://doi.org/10.1016/j.jnca.2020.102595
21. Ahmad S, Mir AH. Scalability, consistency, reliability and security in SDN controllers: A survey of diverse SDN controllers. Journal of Network and Systems Management. 2020;29(1). Available:https://doi.org/10.1007/s10922-020-09575-4
22. Etxezarreta X, Garitano I, Iturbe M, Zurutuza U. Software-defined networking approaches for intrusion response in industrial control systems: A survey. International Journal of Critical Infrastructure Protection. 2023;42:100615–100615. Available:https://doi.org/10.1016/j.ijcip.2023.100615
23. Ezeugwa FA, Olaniyi OO, Ugonnia JC, Arigbabu AS, Joeaneke PC. Artificial intelligence, big data, and cloud infrastructures: Policy recommendations for enhancing women’s participation in the tech-driven economy. Journal of Engineering Research and Reports. 2024;26(6):1–16. Available:https://doi.org/10.9734/jerr/2024/v26i61158
24. Ray PP, Kumar N. SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. Computer Communications. 2021; 169:129–153. Available:https://doi.org/10.1016/j.comcom.2021.01.018
25. Igwenagu UTI, Salami AA, Arigbabu AS, Mesode CE, Oladoyinbo TO, Olaniyi OO. Securing the digital frontier: Strategies for cloud computing security, database protection, and comprehensive penetration testing. Journal of Engineering Research and Reports. 2024;26(6):60–75. Available:https://doi.org/10.9734/jerr/2024/v26i61162
26. Urrea C, Benítez D. Software-defined networking solutions, architecture and controllers for the industrial internet of things: A review. Sensors. 2021;21(19): 6585. Available:https://doi.org/10.3390/s21196585
27. Singh N, Buyya R, Kim H. Securing cloud-based internet of things: Challenges and mitigations. arXiv (Cornell University); 2024. Available:https://doi.org/10.48550/arxiv.2402.00356
28. Marquis YA, Oladoyinbo TO, Olabanji SO, Olaniyi OO, Ajayi SS. Proliferation of AI tools: A multifaceted evaluation of user perceptions and emerging trend. Asian Journal of Advanced Research and Reports. 2024;18(1):30–35. Available:https://doi.org/10.9734/ajarr/2024/v18i1596
29. Mas-Machuca C, et al. Reliable control and data planes for Softwarized networks. Computer Communications and Networks. 2020;243–270. Available:https://doi.org/10.1007/978-3-030-44685-7_10
30. Mayeke NR, Arigbabu AT, Olaniyi OO, Okunleye OJ, Adigwe CS. Evolving access control paradigms: A comprehensive multi-dimensional analysis of security risks and system assurance in cyber engineering.

Asian Journal of Research in Computer Science. 2024;17(5):108–124. Available:https://doi.org/10.9734/ajrcos/2024/v17i5442

31. Dou S, Qi L, Guo Z. Mitigating the impact of controller failures on QoS robustness for software-defined wide area networks. Computer Networks. 2024;238:110096, Available:https://doi.org/10.1016/j.comnet.2023.110096
32. Ali J, Lee G, Roh B, Ryu DK, Park G. Software-defined networking approaches for link failure recovery: A survey. Sustainability. 2020;12(10):4255. Available:https://doi.org/10.3390/su12104255
33. Abuarqoub A. A review of the control plane scalability approaches in software defined networking. Future Internet. 2020;12(3):49. Available:https://doi.org/10.3390/fi12030049
34. Mishra S, Anderson K, Miller B, Boyer K, Warren A. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Applied Energy. 2020;264:114726. Available:https://doi.org/10.1016/j.apenergy.2020.114726
35. Olabanji SO. AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Asian Journal of Research in Computer Science. 2024;17(3):38–56. Available:https://doi.org/10.9734/ajrcos/2024/v17i3423
36. Hamzah M, et al. Distributed control of cyber physical system on various domains: A critical review. MDPI. 2023;11(4):208–208. Available:https://doi.org/10.3390/systems11040208
37. Cunha J, et al. Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies. Future Internet. 2024;16(7):226. Available:https://doi.org/10.3390/fi16070226
38. Olabanji SO, Marquis YA, Adigwe CS, Abidemi AS, Oladoyinbo TO, Olaniyi OO. AI-Driven cloud security: Examining the impact of user behavior analysis on threat detection. Asian Journal of Research in Computer Science. 2024;17(3):57–74. Available:https://doi.org/10.9734/ajrcos/2024/v17i3424
39. Hamarsheh A. An adaptive security framework for internet of things networks leveraging SDN and Machine Learning. Applied Sciences. 2024;14(11):4530. Available:https://doi.org/10.3390/app14114530
40. Nguyen M, Debroy S. Moving target defense-based denial-of-service mitigation in cloud environments: A survey. Security and Communication Networks. 2022;2022: 1–24. Available:https://doi.org/10.1155/2022/2223050
41. Oladoyinbo TO, Adebiyi OO, Ugonnia JC, Olaniyi OO, Okunleye OJ. Evaluating and establishing baseline security requirements in cloud computing: An enterprise risk management approach. Asian Journal of Economics, Business and Accounting. 2023;23(21):222–231. Available:https://doi.org/10.9734/ajeba/2023/v23i211129
42. Riggs H, et al. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors. 2023;23(8):4060.
43. Oladoyinbo TO, Olabanji SO, Olaniyi OO, Adebiyi OO, Okunleye OJ, Alao AI. Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics. Asian Journal of Advanced Research and Reports. 2024;18(2):1–23. Available:https://doi.org/10.9734/ajarr/2024/v18i2601
44. Golightly L, Modesti P, Garcia R, Chang V. Securing distributed systems: A survey on access control techniques for cloud, Blockchain, IoT and SDN. Cyber Security and Applications. 2023;1:100015. Available:https://doi.org/10.1016/j.csa.2023.100015
45. Sengupta S, Chowdhary A, Sabur A, Alshamrani A, Huang D, Kambhampati S. A survey of moving target defenses for network security. IEEE Communications Surveys and Tutorials. 2020;22(3):1909–1941. Available:https://doi.org/10.1109/comst.2020.2982955
46. Olaniyi OO. Ballots and padlocks: Building digital trust and security in democracy through information governance strategies and blockchain technologies. Asian

Journal of Research in Computer Science. 2024;17(5):172–189.
Available:https://doi.org/10.9734/ajrcos/2024/v17i5447

47. Domínguez-Dorado M, Calle-Cancho J, Galeano-Brajones J, Rodríguez-Pérez FJ, Cortés-Polo D. Detection and mitigation of security threats using virtualized network functions in software-defined networks. Applied Sciences. 2024;14(1):374.
Available:https://doi.org/10.3390/app14010374

48. Olaniyi OO, Ezeugwa FA, Okatta CG, Arigbabu AS, Joeaneke PC. Dynamics of the digital workforce: Assessing the interplay and impact of AI, automation, and employment policies. Archives of Current Research International. 2024;24(5):124–139.
Available:https://doi.org/10.9734/acri/2024/v24i5690

49. Rahouti M, Xiong K, Xin Y, Jagatheesaperumal SK, Ayyash M, Shaheed M. SDN security review: Threat taxonomy, implications, and open challenges. IEEE Access. 2022;10:1–1.
Available:https://doi.org/10.1109/access.2022.3168972

50. Olaniyi OO, Okunleye OJ, Olabanji SO. Advancing data-driven decision-making in smart cities through big data analytics: A comprehensive review of existing literature. Current Journal of Applied Science and Technology. 2023;42(25):10–18.
Available:https://doi.org/10.9734/cjast/2023/v42i254181

51. Krishnan P, Jain K, Aldweesh A, Prabu P, Buyya R. OpenStack DP: A scalable network security framework for SDN-based OpenStack cloud infrastructure. Journal of Cloud Computing. 2023;12(1).
Available:https://doi.org/10.1186/s13677-023-00406-w

52. Olaniyi OO, Olaoye OO, Okunleye OJ. Effects of Information Governance (IG) on profitability in the Nigerian banking sector. Asian Journal of Economics, Business and Accounting. 2023;23(18):22–35,
Available:https://doi.org/10.9734/ajeba/2023/v23i181055

53. Li Z, Hu Y, Wu J, Lu J. P4Resilience: Scalable resilience for multi-failure recovery in SDN with Programmable Data Plane. Computer Networks. 2022;208:108896.
Available:https://doi.org/10.1016/j.comnet.2022.108896

54. Lakhani G, Kothari A. Fault administration by load balancing in distributed SDN Controller: A Review. Wireless Personal Communications. 2020;114.
Available:https://doi.org/10.1007/s11277-020-07545-2

55. Olaniyi OO, Omogoroye OO, Olaniyi FG, Alao AI, Oladoyinbo TO. CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. Journal of Engineering Research and Reports. 2024;26(6):32.
Available:https://doi.org/10.9734/JERR/2024/v26i61160

56. An H, Na Y, Lee H, Perrig A. Resilience evaluation of multi-path routing against network attacks and failures. Electronics. 2021;10(11):1240.
Available:https://doi.org/10.3390/electronics10111240

57. Olaniyi OO, Ugonnia JC, Olaniyi FG, Arigbabu AT, Adigwe CS. Digital collaborative tools, strategic communication, and social capital: Unveiling the impact of digital transformation on organizational dynamics. Asian Journal of Research in Computer Science. 2024;17(5):140–156.
Available:https://doi.org/10.9734/ajrcos/2024/v17i5444

58. Adeniyi O, Sadiq AS, Pillai P, Taheir MA, Kaiwartya O. Proactive self-healing approaches in mobile edge computing: A systematic literature review. Computers. 2023;12(3):63.
Available:https://doi.org/10.3390/computers12030063

59. Mostafavi S, Hakami V, Sanaei M. Quality of service provisioning in network function virtualization: A survey. Computing. 2021;103(5):917–991.
Available:https://doi.org/10.1007/s00607-021-00925-x

60. Kim Y, Gil J, Kim D. A location-aware network virtualization and reconfiguration for 5G core network based on SDN and NFV. International Journal of Communication Systems. 2020;34(2).
Available:https://doi.org/10.1002/dac.4160

61. Olateju OO, Okon SU, Olaniyi OO, Samuel-Okon AD, Asonze CU. Exploring the concept of explainable AI and developing information governance

standards for enhancing trust and transparency in handling customer data. Journal of Engineering Research and Reports. 2024;26(7):244–268. Available:https://doi.org/10.9734/jerr/2024/v26i71206

62. Barakabitze AA, Ahmad A, Hines A, Mijumbi R. 5G Network Slicing using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges. Computer Networks. 2019;167:106984. Available:https://doi.org/10.1016/j.comnet.2019.106984
63. Menaceur A, Drid H, Rahouti M. Fault Tolerance and failure recovery techniques in software-defined networking: A comprehensive approach. Journal of Network and Systems Management. 2023;31(4). Available:https://doi.org/10.1007/s10922-023-09772-x
64. Samanta A, Chowdhuri S, Williamson SS. Machine learning-based data-driven fault detection/diagnosis of lithium-ion battery: A critical review. Electronics. 2021;10(11): 1309. Available:https://doi.org/10.3390/electronics10111309
65. Zhang Y, Hua W, Zhou Z, Edward Suh GEG, Delimitrou C. Sinan: ML-based and QoS-aware resource management for cloud microservices. ACM Digital Library; 2021. Available:https://doi.org/10.1145/3445814.3446693
66. Olateju OO, Okon SU, Igwenagu UTI, Salami AA, Oladoyinbo TO, Olaniyi OO. Combating the challenges of false positives in Ai-driven anomaly detection systems and enhancing data security in the cloud. Asian Journal of Research in Computer Science. 2024;17(6):264–292. Available:https://doi.org/10.9734/ajrcos/2024/v17i6472
67. Ding D, Han QL, Ge X, Wang J. Secure state estimation and control of cyber-physical systems: A survey. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2021;51(1):176–190. Available:https://doi.org/10.1109/tsmc.2020.3041121
68. Lwakatare LE, Raj A, Crnkovic I, Bosch J, Olsson HH. Large-scale machine learning systems in real-world industrial settings: A review of challenges and solutions. Information and Software Technology. 2020;127:106368. Available:https://doi.org/10.1016/j.infsof.2020.106368.
69. Oluwaseun Oladeji Olaniyi, Dagogo Sopriala Omubo. WhatsApp data policy, data security and users' Vulnerability. International Journal of Innovative Research and Development; 2023. Available:https://doi.org/10.24940/ijird/2023/v12/i4/apr23021
70. Bouchama F, Kamal M. Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. International Journal of Business Intelligence and Big Data Analytics. 2021;4(9):1–9. Available:https://research.tensorgate.org/index.php/IJBIBDA/article/view/76
71. Salami AA, Igwenagu UTI, Mesode CE, Olaniyi OO, Oladoyinbo OB. Beyond conventional threat defense: Implementing advanced threat modeling techniques, risk modeling frameworks and contingency planning in the healthcare sector for enhanced data security. Journal of Engineering Research and Reports. 2024;26(5):304–323. Available:https://doi.org/10.9734/jerr/2024/v26i51156
72. Rafique W, Qi L, Yaqoob I, Imran M, Rasool RU, Dou W. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys Tutorials. 2020;22(3):1761–1804. Available:https://doi.org/10.1109/COMST.2020.2997475
73. Nsafoa-Yeboah K, et al. Software-defined networks for optical networks using flexible orchestration: Advances, challenges, and opportunities. Journal of Computer Networks and Communications. 2022; 2022:1–40 Available:https://doi.org/10.1155/2022/5037702.
74. Samuel-Okon AD. Smart media or biased media: The impacts and challenges of AI and big data on the media industry. Asian Journal of Research in Computer Science. 2024;17(7):128–144. Available:https://doi.org/10.9734/ajrcos/2024/v17i7484
75. Ugonnia JC, Olaniyi OO, Olaniyi FG, Arigbabu AA, Oladoyinbo TO. Towards sustainable it infrastructure: Integrating

green computing with data warehouse and big data technologies to enhance efficiency and environmental responsibility. Journal of Engineering Research and Reports. 2024;26(5):247–261. Available:https://doi.org/10.9734/jerr/2024/v26i51151.

76. Rauf B, et al. Application threats to exploit northbound interface vulnerabilities in software defined networks. ACM Computing Surveys. 2021;54(6):1–36. Available:https://doi.org/10.1145/3453648

77. Hari Krishna SM, Sharma R. Comparative study of orchestration using GRPC API and rest API in server creation time: An Openstack case. Social Science Research Network; 2024. Available:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4710302

78. Samuel- Okon AD, Olateju OO, Okon SU, Olaniyi OO, Igwenagu UTI. Formulating global policies and strategies for combating criminal use and abuse of artificial intelligence. Archives of Current Research International. 2024;24(5):612–629. Available:https://doi.org/10.9734/acri/2024/v24i5735

79. Latif Z, Sharif K, Li F, Karim MM, Biswas S, Wang Y. A comprehensive survey of interface protocols for software defined networks. Journal of Network and Computer Applications. 2020;156:102563. Available:https://doi.org/10.1016/j.jnca.2020.102563

80. The MAWI Working Group Traffic Archive;2022. Available:https://mawi.wide.ad.jp/mawi/

81. The Open Networking Foundation;2011 Available:https://opennetworking.org/

82. The Cloud Security Alliance; 2023. Available:https://cloudsecurityalliance.org/

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/120621