Sciforce

Journal of Artificial Intelligence and Machine Learning

Journal homepage: www.sciforce.org
ISSN : 2995-2336

Open Access Review Article

Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis

Varun Venkatesh Dandasi*

BI Data Engineer, HCL GLobal Systems Inc., AZ ,United States

Abstract

This study delves into the intricate security and privacy challenges inherent in Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) ecosystems, highlighting an urgent imperative for robust security solutions in contemporary network architectures. As the Internet of Things (IoT) proliferates and the complexity of networks escalates, the integration of effective security measures emerges as an essential safeguard for protecting network infrastructures against the relentless tide of evolving cyber threats. The significance of this research lies in its comprehensive evaluation and comparative analysis of six leading security solutions—OpenFlow, FortNOX, FRESCO, Rosemary, VeriFlow, and SE-Floodlight—offering network administrators and security professionals critical quantitative insights to facilitate informed decision-making. Employing the Weighted Sum Method (WSM) as its primary research methodology, the study presents a systematic framework for multi-criteria decision analysis specifically tailored to network security implementations.

The evaluation criteria encompass a range of parameters, including the attack detection rate, attack prevention rate, network overhead, false positive and false negative rates, and encryption latency. Furthermore, alternative metrics such as network scalability, resource utilization, and implementation complexity are considered across diverse network environments. To ensure an objective comparison of all solutions, the research methodology utilizes normalized matrices coupled with weighted calculations, thereby enhancing the rigor and depth of the analysis. The results of the analysis illuminate that VeriFlow not only excels but also establishes a benchmark with an impressive preference score of 0.8907. This remarkable system showcases formidable capabilities in attack detection, boasting a rate of 90%, alongside a commendable prevention rate of 85%. However, this prowess comes at a slight cost, as evidenced by an increased encryption latency of 20 ms. In contrast, FortNOX emerges as a strong contender, securing the second position with a score of 0.7878. This system strikes a commendable balance, delivering a robust suite of security features while maintaining a moderate latency of 15 ms. Meanwhile, Rosemary trails in third place with a score of 0.7260, reflecting its comparatively lesser efficacy. The findings unveil a discernible relationship between the effectiveness of security measures and the concomitant system overhead. This interplay suggests that optimal security solutions frequently necessitate a delicate equilibrium—wherein enhanced protection levels inevitably lead to trade-offs concerning network performance. Ultimately, the study posits that while high-security implementations may engender additional latency and overhead, the exemplary cases presented by VeriFlow and FortNOX underscore the feasibility of achieving formidable security without severely compromising network functionality. These revelations significantly enrich the existing corpus of knowledge in the realm of SDN NFV security, offering valuable insights for organizations striving to bolster their network infrastructure's security posture.

Keywords: Software-Defined Networking (SDN), Network Functions Virtualisation (NFV), Security Solutions, Weighted Sum Method (WSM), Attack Detection, Network Performance Optimization.

Introduction

The Internet of Things (IoT) represents a transformative technology that intricately links human life with digital networks, enabling everyday objects to function as "smart" devices. Through the integration of embedded sensors and actuators, items ranging from refrigerators to watches to light bulbs can now engage in digital interactions, streamlining and enhancing daily routines. For instance, a smart watch, equipped with biosensors, not only displays the time but also actively tracks heart rate, playing a role in health and wellness monitoring. Among IoT's notable applications, the smart home stands out as a prominent example. Here, a network seamlessly connects key household devices, allowing for remote monitoring, control, and real-time access. Statist's projections underscore the rapid growth of this market: smart-home revenue, valued at $78.9 billion in 2020, is anticipated to surge to $182.3 billion by 2025, highlighting its broad appeal—and the parallel rise in cyber vulnerabilities that accompanies its adoption [1-2]. IoT's rapid expansion has not gone unnoticed by malicious actors. In 2021, recorded IoT attacks surged by 6%, amassing a staggering 60.1 million incidents, a statistic that underscores the inherent security weaknesses of many smart-home devices. As such, fortifying the security of these interconnected systems becomes not merely advisable but essential to safeguarding users' quality of life. Enhancing smart-home resilience demands advanced technologies that address access control, data privacy, integrity, and overall system security.

Approaches such as block chain, software-defined networking (SDN), and network function virtualization (NFV) are emerging as crucial strategies in this domain. Block chain fosters a foundation of trust and verifiability across IoT networks; SDN offers agile network management capabilities; and NFV supports high availability and scalability, reinforcing the overall stability of the IoT infrastructure [3].Recent studies reveals an escalating interest in leveraging these technologies to secure smart-home environments. The integration of block chain, SDN, and NFV

Received date: November 07, 2023 **Accepted date:** November 18, 2023; **Published date:** December 05, 2023

***Corresponding Author:** *Dandasi, V. V*, BI Data Engineer, HCL GLobal Systems Inc., AZ ,United States., E- mail: varundandasi85@gmail.com

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282

could represent a powerful confluence in the architecture of IoT security, amplifying confidentiality, availability, privacy, and trust. Therefore, developing a robust, multi-layered security framework that combines these innovations may be key to creating secure, resilient, and adaptable smart homes for the future [4].

The Network Function Virtualization (NFV) framework fundamentally rests on three pivotal components: the infrastructure, service, and the management and orchestration layers. Central to the infrastructure layer—designated as NFV Infrastructure (NFVI)—are the hardware assets, associated software, and an encompassing virtualization environment that collectively enable functional abstraction. In the service layer, Virtual Network Functions (VNFs) are dynamically selected from a repository, functioning within these virtualized environments rather than on fixed, dedicated hardware—a significant shift in network design.

Meanwhile, the Management and Orchestration (NFV-MANO) layer orchestrates specialized operations, from establishing VNF processing sequences for network traffic to optimizing the interplay of these functions. For example, in scenarios with VNFs for firewall protection and Intrusion Detection System (IDS) monitoring, NFV-MANO dictates packet flow through each function in a designated order, bolstering security and operational coherence [5-6]. As the Internet of Things (IoT) landscape expands, Software-Defined Networking (SDN) introduces a robust virtualization framework designed to enhance network efficacy, management, and resource optimization. SDN solutions address entrenched IoT networking obstacles—heterogeneity, interoperability, scalability—while refining service deployment and enabling agile adaptation to emerging services. Research categorizes SDN-based architectural proposals into overarching frameworks that focus on architecture, security, and management. Within these frameworks, the control plane directs traffic management, while the data plane is dedicated to data forwarding, achieving distinct operational clarity. This separation empowers applications to interact directly with the control plane, enabling administrators to exert fine-grained control over network processes—an approach that bolsters both scalability and functionality [7-8].

NFV, by decoupling network functionalities from proprietary hardware, facilitates the adoption of virtualization across networked systems, allowing these functions to operate as software within virtual machines (VMs) instead. Standardized by the European Telecommunications Standards Institute (ETSI), this approach enables conventional network functions—such as firewalls, traffic management, and virtual routing—to function as Virtual Network Functions (VNFs). Through NFV, infrastructure can operate independently of specific hardware configurations, allowing multiple VMs to share a single server, thereby enabling resource scaling as demands fluctuate. This adaptive model not only optimizes resource allocation in data centers but also reduces idle capacity, enhancing overall efficiency. Moreover, NFV enables virtualization of both data and control planes across data centers and extended networks, further streamlining operations and facilitating seamless integration [9-10].

The architecture of Network Function Virtualization (NFV) is built around three foundational elements: infrastructure, service, and the management and orchestration layer. At its base, the NFV Infrastructure (NFVI) layer integrates hardware, software, and a comprehensive virtualization environment to support flexible operations. The service layer, in contrast, acts as a hosting platform for Virtual Network Functions (VNFs), which are selected from a curated repository and deployed in virtual environments instead of traditional hardware. Overarching these layers is the Management and Orchestration (NFV-MANO) component, which handles intricate coordination tasks—such as defining the precise processing sequence for VNFs involved in network traffic routing. Consider a scenario where firewall and Intrusion Detection System (IDS) VNFs are deployed; here, NFV-MANO would sequence packet flow meticulously through these functions to maximize both security and operational efficiency [11-12].

In the realm of Software-Defined Networking (SDN), a standardized API serves as a linchpin, enabling developers to integrate innovative and programmable functionalities, enhancing network adaptability and control. This API-driven approach not only centralizes management but also provides a global view of the network, facilitating swift, on-demand configuration adjustments. However, as SDNs gain traction across sensitive infrastructures—such as cloud platforms and peer-to-peer systems—critical security challenges emerge. Core issues of scalability, optimal controller placement, and latency, compounded by vulnerabilities to targeted attacks, persist. Typical security threats to SDN frameworks include unauthorized access attempts, conflicts in flow rule implementation, and breaches targeting inter-layer communication interfaces [13-14]. The layered architecture of SDN introduces diverse security concerns unique to each layer. For example, the application layer, which governs security applications, remains vulnerable to unauthorized intrusions and potential data exposure. Conversely, the data layer faces its own risks, such as limited flow rule capacities that can trigger Denial-of-Service (DoS) scenarios or propagate configuration errors. Although research continues to propose innovative solutions, securing SDN's deployment remains an evolving field—especially within high-stakes environments like data centers and enterprise-level networks [15].

Recent studies have examined software-defined fog computing networks, particularly delving into the intricate security and privacy challenges embedded within fog-based network architectures. In parallel, the integration of block chain technology within Software-Defined Networking (SDN) paradigms has emerged as a novel approach to bolster security in these environments. This integration allows a nuanced evaluation of block chain's advantages and constraints in the context of SDN. Moreover, the triadic convergence of SDN, IoT, and block chain illustrates substantial potential, indicating an evolving framework for securing network infrastructures more comprehensively [16].Further, SDN-driven IoT architecture advancements target multiple dimensions: seamless device connectivity, cohesive cloud and fog integrations, and the complex demands of scalability. Certain proposed models adopt layered frameworks, delineating device, control, network, and application layers, thereby facilitating interoperability while enhancing security protocols. Despite these innovations, some architectural propositions, such as SDN-enhanced gateways, linger primarily in theoretical or experimental stages, lacking widespread, real-world deployment. Nonetheless, such gateways are pivotal, particularly for accommodating the diverse configurations inherent to heterogeneous IoT landscapes, potentially enhancing both flexibility and operational efficiency [17].On the management front, SDN's capacity for irtualizat configuration proves essential for the orchestration of extensive IoT deployments. Current solutions aim to streamline application deployment, enable device discovery, implement network slicing, and manage both cloud and edge environments, thus enhancing network adaptability, load balancing, and latency irtualizati. However, achieving true scalability and precise device irtualization remains a challenge, necessitating further rigorous testing and irtualizati. The fusion of SDN with irtualization technologies and programmable gateways promises a promising trajectory, addressing critical architectural and management hurdles and laying the groundwork for scalable, high-performance IoT ecosystems [18].

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282

Materials and Methods

This investigation applies the WSM approach to evaluate security and privacy dynamics within SDN NFV networks, targeting technologies like OpenFlow, FortNOX, FRESCO, Rosemary, VeriFlow, and SE-Floodlight. Through Augmented Reality, network scenarios become visually navigable, while the Ant System algorithm optimises essential factors, including attack frequencies, network overhead, rates of false positives and negatives, and encryption-induced latency. Together, these tools bolster decision-making precision and deepen security fortifications. Attack Detection and Prevention Rates: These indicators assess the robustness of a network solution's ability to detect and intercept security threats. Superior detection and prevention rates directly correlate with enhanced defensive capability, underscoring the network's readiness against potential breaches.

Network Overhead: Network overhead refers to the additional resources—such as bandwidth or processing power—required by the implemented solution. Lower overhead suggests leaner resource utilisation, which is beneficial in promoting an efficient and agile network structure. False Positive and Negative Rates: False positives denote legitimate activities mistakenly flagged as threats, whereas false negatives indicate actual threats overlooked by the system. A reduction in these rates enhances both the precision and reliability of the security system, yielding fewer disruptions and heightened confidence in threat detection.

Encryption Latency: Encryption latency reflects the delay introduced into data transmission processes due to encryption activities. Minimising encryption latency is crucial, as it ensures swift, secure communication without compromising the timeliness required for data transmission. These collective metrics furnish a comprehensive view of each SDN NFV solution's capacity to uphold security and privacy standards. By dissecting these performance benchmarks, researchers and stakeholders gain critical insights into how effectively each solution addresses the intricate challenges of network security, empowering strategic decision-making for implementation and refinement.

Weighted Sum Method:

An influential framework for strategic decision-making, known as Multi-Criteria Decision Making (MCDM), is widely implemented to evaluate and prioritise diverse options under the constraints of multiple, often contradictory, criteria. MCDM methodologies serve as a systematic, structured means for dissecting complex problems, offering a coherent pathway for decision-makers to not only assess each challenge but also customise the analysis to suit precise requirements and specific contexts [19-20]. In applications involving Multi-Criteria Decision Making (MCDM), the ordering and prioritisation of options depend critically on a detailed examination of data, which includes the relative significance and characteristics of attributes within both the decision-making and application matrices. The weight attributed to this data, crucially, has a pronounced effect on the outcomes produced by MCDM methods. Input data in MCDM systems, however, frequently exhibits variability and lacks consistency; as a result, the algorithms may produce outcomes that are often unreliable, with unpredictability stemming directly from the intrinsic instability of the input [21-22]. A particularly prominent yet straightforward approach within MCDM Is the "Weighted Sum Model" (WSM). The WSM enjoys notable popularity for its simplicity and broad appeal, especially when the objective is to facilitate participation from individuals who may lack technical expertise. This simplicity, however, should not be mistaken for superficiality; rather, its widespread use in Sustainable Urban Mobility Plans (SUMPs), where structured problem identification and systematic solution exploration are paramount, attests to its effectiveness in conveying concepts in an accessible format. Nevertheless, the dependability of the WSM is intrinsically linked to the transparent elucidation of the criteria weights, underscoring the necessity for rational and defensible criteria assignment [23-24].A core technique within MCDM, the Weighted Sum Approach (WSA), aims to determine the optimal option by calculating each alternative's composite utility based on normalised criteria weights. This process unfolds in two primary stages: the initial normalisation of criteria values and the subsequent computation of an aggregate score. Due to its simplicity, the WSA is highly versatile and practical, making it a preferred method in a variety of everyday decision-making contexts. Where varying units of measurement exist, the qualification values are standardised to a common scale, ensuring that the criteria weights reflect each attribute's true influence. Ultimately, each option receives an overall score derived from the weighted aggregation of its component scores, thus enabling clear, comprehensible prioritisation of available choices [25-26].

Analysis and Discussion

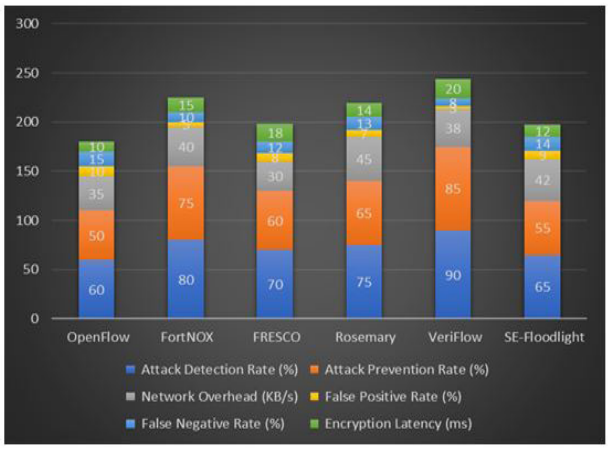

Figure 1:

Figure 1 delineates a nuanced comparative analysis of various security and privacy solutions employed within Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) frameworks. This assessment elucidates pivotal performance indicators, including attack detection rates, prevention efficacy, network overhead, and the rates of false positives and negatives, as well as encryption latency. OpenFlow emerges with relatively modest detection and prevention rates of merely 60% and 50%, respectively. Its accompanying network overhead, recorded at 35 KB/s, contributes to an unsettlingly high false positive rate of 10% and a false negative rate of 15%. Intriguingly, however, OpenFlow boasts a low encryption latency of just 10 milliseconds, suggesting it might serve well in scenarios prioritising the minimisation of encryption delays over the precision of security measures.

In contrast, FortNOX significantly eclipses OpenFlow, achieving commendable detection and prevention rates of 80% and 75%, albeit with a marginally increased network overhead of 40 KB/s. This solution exhibits lower false positive (5%) and negative (10%) rates, reflecting a judicious balance between security robustness and operational overhead, complemented by a moderate encryption latency of 15 milliseconds. FRESCO occupies a more centrist position, recording detection and prevention rates of 70% and 60%, respectively, while managing to lower network overhead to 30 KB/s. Its performance on false positive and negative rates—8% and 12%—offers a slight improvement over OpenFlow, although it does incur a slightly elevated encryption latency of

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282

18 milliseconds. Both Rosemary and SE-Floodlight manifest moderate efficacy in terms of detection, prevention, and overhead, simultaneously achieving enhanced latency. This makes them appealing choices for networks striving for a balanced security posture without incurring significant delays. Finally, VeriFlow stands out as the vanguard of security solutions, boasting the highest detection (90%) and prevention rates (85%) in this analysis. However, this robust performance is counterbalanced by a higher network overhead of 38 KB/s and a latency of 20 milliseconds. Notably, its impressively low false rates—3% for positives and 8% for negatives—position it as the ideal candidate for environments where stringent security measures are non-negotiable, despite the accompanying latency considerations.

Table 1: The data presented in Table 1 delivers a nuanced comparative analysis of diverse security and privacy solutions

Alternatives:	Attack Detection Rate (%)	Attack Prevention Rate (%)	Network Overhead (KB/s)	False Positive Rate (%)	False Negative Rate (%)	Encryption Latency (ms)
OpenFlow	60	50	35	10	15	10
FortNOX	80	75	40	5	10	15
FRESCO	70	60	30	8	12	18
Rosemary	75	65	45	7	13	14
VeriFlow	90	85	38	3	8	20
SE-Floodlight	65	55	42	9	14	12

The data presented in Table 1 delivers a nuanced comparative analysis of diverse security and privacy solutions tailored for Software-Defined Networking and Network Functions Virtualization (SDN NFV) ecosystems. This analysis hinges on several pivotal metrics, namely: attack detection rate, attack prevention rate, network overhead, and the rates of false positives and negatives, alongside encryption latency. Open Flow emerges as a relatively suboptimal contender, showcasing a detection rate of merely 60% and a prevention rate of 50%. It grapples with a moderate network overhead of 35 KB/s, which unfortunately culminates in elevated false positive (10%) and negative rates (15%). Notably, its encryption latency is commendably low at 10 ms, indicating potential suitability for scenarios where the minimization of encryption delays supersedes concerns for security efficacy.

In contrast, FortNOX exhibits superior performance, achieving a detection rate of 80% and a prevention rate of 75%, albeit with a marginally increased network overhead of 40 KB/s. Its false positive rate is notably lower at 5%, and the false negative rate rests at 10%, suggesting a more harmonious balance between overhead and security whilst maintaining a moderate encryption latency of 15 ms. FRESCO presents itself as a viable intermediary solution, reporting detection and prevention rates of 70% and 60%, respectively, coupled with a reduced network overhead of 30 KB/s. Its rates of false positives and negatives show slight improvement (8% and 12%, respectively) when juxtaposed with Open Flow, while encryption latency is marginally higher at 18 ms. Rosemary and SE-Floodlight, while offering moderate performance in detection, prevention, and overhead, excel in terms of latency. This suggests that they may represent a judicious choice for networks where a balanced approach is favored, prioritizing moderate security alongside limited latency. Lastly, VeriFlow distinguishes itself with the highest detection (90%) and prevention rates (85%). However, this commendable security comes at the expense of increased network overhead (38 KB/s) and a latency of 20 ms. Its impressively low false rates (3% positive, 8% negative) position it as an optimal solution for scenarios where robust security is paramount, even in the face of heightened latency concerns.

Table 2: The normalized matrix detailed in Table 2 employs the Weighted Sum Method

0.66667	0.58824	0.77778	0.30000	0.53333	1.00000
0.88889	0.88235	0.88889	0.60000	0.80000	0.66667
0.77778	0.70588	0.66667	0.37500	0.66667	0.55556
0.83333	0.76471	1.00000	0.42857	0.61538	0.71429
1.00000	1.00000	0.84444	1.00000	1.00000	0.50000
0.72222	0.64706	0.93333	0.33333	0.57143	0.83333

The normalized matrix detailed in Table 2 employs the Weighted Sum Method to rigorously assess a spectrum of alternatives, gauging them against an array of performance metrics. Each alternative undergoes a thorough evaluation, scrutinized for its efficacy across diverse facets of network security and efficiency, articulated as percentages pertaining to attack detection and prevention rates. Additional metrics include network overhead, false positive and negative rates, alongside encryption latency. In the realm of Attack Detection Rate, VeriFlow emerges as the frontrunner, achieving a flawless score of 1, signifying its remarkable proficiency in identifying every attempted attack. Closely trailing are FortNOX and Rosemary, attaining commendable rates of approximately 0.89 and 0.83, respectively. The Attack Prevention Rate mirrors this trend, with VeriFlow again taking the lead, recording an identical perfect score. FortNOX demonstrates formidable capabilities in this area as well, boasting a rate around 0.88. When analyzing network performance through the lens of Network Overhead, Rosemary ascends to the pinnacle with a score of 1, indicative of its minimal overhead, whilst FRESCO lags behind, clocking in at about 0.67. Conversely, the False Positive Rate reveals that VeriFlow excels, securing a score of 1 and thereby minimizing erroneous alerts. In contrast, FortNOX presents a higher false positive rate of 0.6, suggesting potential vulnerabilities in its detection mechanisms. The False Negative Rate unveils a more troubling narrative, where all alternatives, barring VeriFlow, demonstrate significant rates, highlighting critical opportunities for enhancement in accurately identifying attacks. Finally, the scores for Encryption Latency fluctuate from 0.5 for VeriFlow, indicating low latency, to 1 for OpenFlow, signaling an urgent need for optimization. Collectively, this normalized matrix serves as a robust comparative analysis, elucidating each alternative's strengths and weaknesses across an array of pivotal performance indicators.

Table 3: Delineates a nuanced comparative analysis of various network security alternatives, scrutinising them through an array of performance metrics

0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
0.1667	0.1667	0.1667	0.1667	0.1667	0.1667

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282

Table 3 delineates a nuanced comparative analysis of various network security alternatives, scrutinising them through an array of performance metrics. Each alternative is assessed against six pivotal parameters: Attack Detection Rate, Attack Prevention Rate, Network Overhead, False Positive Rate, False Negative Rate, and Encryption Latency. Remarkably, the homogeneity of the results across all alternatives is evident, with each metric hovering around a value of approximately 0.1667. This observation raises intriguing questions regarding the efficacy of these alternatives; specifically, the Attack Detection and Prevention Rates underscore their capacity to identify and neutralise threats. The uniformity of these rates insinuates a baseline performance level, indicating that all alternatives might possess equivalent capabilities in both detecting and averting attacks. Furthermore, the Network Overhead metric, indicative of bandwidth consumption by security protocols, reveals a similar consistency, signifying a uniform impact on network performance. Such uniformity facilitates streamlined decision-making for network administrators selecting the optimal solution. Additionally, the False Positive and False Negative Rates exhibit comparable performance levels, hinting at each alternative's equivalent propensity for misclassifying benign activities as threats or inadequately identifying genuine threats. Finally, the constancy of Encryption Latency is paramount, preserving operational efficiency within network environments.

Table 4: Unveils a meticulously constructed weighted normalized matrix, employing the weighted sum method

0.11111	0.09804	0.12963	0.05000	0.08889	0.16667
0.14815	0.14706	0.14815	0.10000	0.13333	0.11111
0.12963	0.11765	0.11111	0.06250	0.11111	0.09259
0.13889	0.12745	0.16667	0.07143	0.10256	0.11905
0.16667	0.16667	0.14074	0.16667	0.16667	0.08333
0.12037	0.10784	0.15556	0.05556	0.09524	0.13889

Table 4 unveils a meticulously constructed weighted normalized matrix, employing the weighted sum method to assess a variety of alternatives through multiple performance metrics. The contenders in this evaluation—OpenFlow, FortNOX, FRESCO, Rosemary, VeriFlow, and SE-Floodlight—are scrutinized against six distinct criteria: Attack Detection Rate, Attack Prevention Rate, Network Overhead, False Positive Rate, False Negative Rate, and Encryption Latency. The results are standardized, presenting values ranging from 0 to 1, which facilitates comparative analysis. The Attack Detection Rate, a pivotal measure of each alternative's capability to discern potential security threats, highlights VeriFlow's prominence with a detection rate of 0.1667, signifying superior threat recognition. In the realm of Attack Prevention Rate, VeriFlow maintains its lead, showcasing its robust dual functionality in both detecting and thwarting attacks. In stark contrast, Open Flow lags in both dimensions, revealing significant limitations in its security framework. The consideration of Network Overhead is critical, with Rosemary emerging as the alternative that potentially burdens network resources the most, evidenced by its peak normalized value of 0.1667. Conversely, FRESCO is positioned as the most resource-efficient, exhibiting the lowest normalized value for Network Overhead. Assessing the False Positive and False Negative Rates is crucial for gauging the reliability of detection mechanisms. Here, both VeriFlow and FortNOX manifest elevated scores for False Positive Rates, signaling a trade-off between detection efficacy and false alarm occurrences. Lastly, Encryption Latency, a determinant of overall performance, favors FRESCO, which boasts the lowest latency at 92.59 ms, thereby minimizing delays in secure communications. Collectively, this weighted normalized matrix encapsulates a nuanced perspective on the equilibrium between security efficacy and network performance across the evaluated alternatives.

Table 5: elucidates the preference scores and rankings of a diverse array of alternatives evaluated through the weighted sum method

Alternatives:	Preference Score	Rank
OpenFlow	0.6443	5
FortNOX	0.7878	2
FRESCO	0.6246	6
Rosemary	0.7260	3
VeriFlow	0.8907	1
SE-Floodlight	0.6735	4

Table 5 elucidates the preference scores and rankings of a diverse array of alternatives evaluated through the weighted sum method. The contenders—OpenFlow, FortNOX, FRESCO, Rosemary, VeriFlow, and SE-Floodlight—are assigned distinct preference scores that encapsulate their overall performance across a spectrum of pertinent criteria. VeriFlow emerges as the clear frontrunner, achieving a remarkable preference score of 0.8907, thus clinching the highest rank. This stellar rating implies that VeriFlow surpasses its peers across the evaluated parameters, potentially signalling its superiority in functionality, reliability, and user satisfaction. Trailing closely behind is FortNOX, with a commendable score of 0.7878, placing it second. While this indicates robust performance, it falls short of VeriFlow's apex, affirming its status as a credible alternative. Occupying the third position; Rosemary boasts a preference score of 0.7260. Though respectable, it pales compared to the top two contenders. SE-Floodlight, in fourth place, registers a score of 0.6735, illustrating moderate efficacy within the assessed criteria. Finally, OpenFlow and FRESCO find themselves in fifth and sixth positions with scores of 0.6443 and 0.6246, respectively, suggesting they lag behind in meeting the benchmarks established by their higher-ranking counterparts. Collectively, the table facilitates a nuanced comparison of these alternatives, underpinning informed decision-making grounded in quantitative analysis.

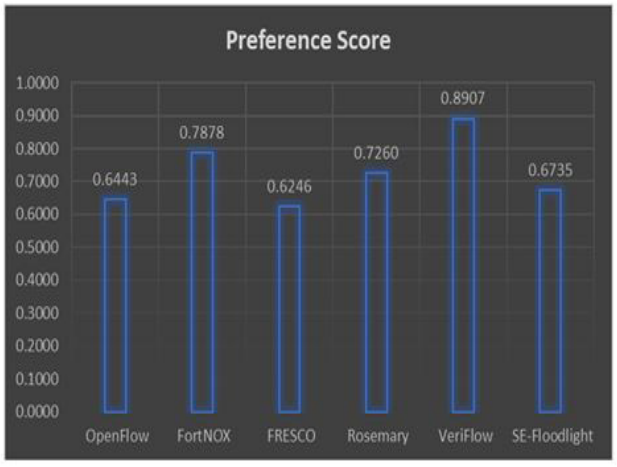

Figure 2:

Figure 2 illustrates the preference scores of several alternatives, derived through the weighted sum method—a prevalent technique in multi-criteria decision-making analysis. This methodology adeptly synthesises the individual scores assigned to various criteria, facilitating a comprehensive assessment of each alternative's performance. The options analyzed include OpenFlow, FortNOX, FRESCO, Rosemary,

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282

VeriFlow, and SE-Floodlight, each accompanied by its unique preference score. Prominently, VeriFlow emerges as the frontrunner, boasting an impressive preference score of 0.8907. This figure signifies its superior standing among the alternatives evaluated, underscoring its exceptional capabilities in pivotal criteria that significantly enhance its effectiveness. Following closely is FortNOX, which commands a noteworthy score of 0.7878, reflecting a robust performance that positions it firmly as the second-best contender. Conversely, FRESCO languishes at the lower end of the spectrum, with a preference score of merely 0.6246, indicating its comparative inadequacy in satisfying the requisite criteria. Mid-range positions are occupied by OpenFlow and Rosemary, scoring 0.6443 and 0.7260, respectively. Notably, SE-Floodlight, achieving a score of 0.6735, edges just above OpenFlow, further complicating the decision landscape.

Figure 3:

Figure 3 elucidates the rankings of diverse alternatives evaluated through the Weighted Sum Method (WSM), a prevalent technique within the realm of multi-criteria decision-making. This methodology meticulously aggregates the performance of each option against a set of predefined criteria, facilitating a thorough and nuanced evaluation. Among the array of alternatives examined, VeriFlow emerges as the unequivocal leader, securing the highest rank of 1. This prominence signifies that, according to the established criteria, VeriFlow exhibits superior performance in comparison to its competitors. Its attributes are likely to resonate with the prioritized requirements, positioning it as the optimal choice within this context. Conversely, FRESCO languishes at the bottom of the rankings with a score of 6, suggesting it falls short in meeting the evaluative criteria relative to its counterparts. This may unveil intrinsic limitations in its functionality or overall performance, meriting an in-depth exploration to ascertain its deficiencies. Additionally, FortNOX and Rosemary claim the 2nd and 3rd positions, respectively, indicating their status as formidable contenders. Their rankings imply that they offer substantial features and performance metrics that align favorably with the decision-making criteria. Following closely, SE-Floodlight and OpenFlow, ranked 4 and 5, respectively, while not leading, still exhibit commendable value among the alternatives assessed.

The investigation rigorously assessed six distinct security solutions tailored for Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) frameworks, employing the Weighted Sum Method (WSM) for evaluation. Dominating the landscape, VeriFlow emerged as the premier solution, boasting an impressive preference score of 0.8907, and clinching the top rank. Its prowess in attack detection soared to 90%, with prevention capabilities at 85%, whilst simultaneously registering the most favorable metrics in false positives (3%) and negatives (8%). Notably, this efficacy came at the expense of a marginal increase in encryption latency, recorded at 20ms. In a commendable second place, FortNOX attained a preference score of 0.7878, showcasing commendable detection (80%) and prevention rates (75%), coupled with a more moderate encryption latency of 15ms. This equilibrium between security robustness and performance establishes it as a noteworthy alternative to VeriFlow. Trailing closely, Rosemary garnered a score of 0.7260, followed by SE-Floodlight (0.6735), OpenFlow (0.6443), and FRESCO (0.6246). Despite its minimal encryption latency of 10ms, OpenFlow exhibited notably inferior detection (60%) and prevention rates (50%), underscoring the intricate trade-offs between security and operational efficiency. This analysis elucidates that while enhanced security capabilities frequently entail increased latency and network overhead, solutions such as VeriFlow and FortNOX adeptly navigate the delicate balance between security effectiveness and operational efficiency. Consequently, it is imperative for organizations to meticulously assess their unique requirements when selecting security solutions, judiciously weighing the trade-offs between robust security measures and potential impacts on network performance.

Conclusion

1. Bhuyan, Monowar, Shigeru Kashihara, Doudou Fall, Yuzo Taenaka, and Youki Kadobayashi. "A survey on blockchain, SDN and NFV for the smart-home security." Internet of Things 20 (2022): 100588.

2. Qashlan, Amjad, Priyadarsi Nanda, Xiangjian He, and Manoranjan Mohanty. "Privacy-preserving mechanism in smart home using blockchain." IEEE Access 9 (2021): 103651-103669.

3. Latif, Sohaib A., Fang B. Xian Wen, Celestine Iwendi, F. Wang Li-Li, Syed Muhammad Mohsin, Zhaoyang Han, and Shahab S. Band. "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems." Computer Communications 181 (2022): 274-283.

4. Shahzadi, Shumaila, Fahad Ahmad, Asma Basharat, Madallah Alruwaili, Saad Alanazi, Mamoona Humayun, Muhammad Rizwan, and Shahid Naseem. "Machine learning empowered security management and quality of service provision in SDN-NFV environment." Computer, Materials and Continua 66, no. 3 (2020): 2723-2749.

5. Bendale, Shailesh Pramod, and Jayashree Rajesh Prasad. "Security Challenges to provide Intelligence in SDN with the help of Machine Learning or Deep Learning." IJAST 29, no. 05 (2020): 356-363.

6. Sridhar Kakulavaram. (2022). Life Insurance Customer Prediction and Sustainbility Analysis Using Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 10(3s), 390 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7649

7. Shi, Xiaojun, Yangyang Li, Haiyong Xie, Tengfei Yang, Linchao Zhang, Panyu Liu, Heng Zhang, and Zhiyao Liang. "An openflow-based load balancing strategy in SDN." Comput. Mater. Contin 62, no. 1 (2020): 385-398.

8. Ahmadvand, Hossein, Chhagan Lal, Hadi Hemmati, Mehdi Sookhak, and Mauro Conti. "Privacy-preserving and security in SDN-based IoT: A survey." IEEE Access 11 (2023): 44772-44786.

9. Garouani, Moncef, Adeel Ahmad, Mourad Bouneffa, Mohamed Hamlich, Gregory Bourguin, and Arnaud Lewandowski. "Using meta-learning for automated algorithms selection and configuration: an experimental framework for industrial big data." Journal of Big Data 9, no. 1 (2022): 57.

10. Galeano-Brajones, Jesús, Javier Carmona-Murillo, Juan F. Valenzuela-Valdés, and Francisco Luna-Valero. "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach." Sensors 20, no. 3 (2020): 816.

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282

11. Rahdari, Ahmad, Ahmad Jalili, Mehdi Esnaashari, Mehdi Gheisari, Alisa A. Vorobeva, Zhaoxi Fang, Panjun Sun et al. "Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions." Computers, Materials & Continua 80, no. 2 (2024).

12. Wani, Sharyar, Mohammed Imthiyas, Hamad Almohamedh, Khalid M. Alhamed, Sultan Almotairi, and Yonis Gulzar. "Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight." Symmetry 13, no. 2 (2021): 227.

13. Adari. VK, Kishor Kumar, A., Praveen Kumar, K., Srinivas, G., & Vinay Kumar, Ch. (2021). The evolution of software maintenance. Journal of Computer Science and Applied Information Technology, 6(1), 1-8. https://doi.org/10.15226/2474-9257/6/1/00150

14. Islam, Md Jahidul, Anichur Rahman, Sumaiya Kabir, Md Razaul Karim, Uzzal Kumar Acharjee, Mostofa Kamal Nasir, Shahab S. Band, Mehdi Sookhak, and Shaoen Wu. "Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities." IEEE Internet of Things Journal 9, no. 5 (2021): 3850-3864.

15. Farooq, Muhammad Shoaib, Shamyla Riaz, and Atif Alvi. "Security and privacy issues in software-defined networking (SDN): A systematic literature review." Electronics 12, no. 14 (2023): 3077.

16. Agapiou, Stelios, AdamantiniPeratikou, and Stavros Stavrou. "Providing Network Resilience through an Intelligent SDN Network." In 2024 Panhellenic Conference on Electronics & Telecommunications (PACET), pp. 1-6. IEEE, 2024.

17. Alade, Oluwaseun, and John Alabi. "Secure Network Monitoring using Software Defined Networking (SDN) with Ryu Controller." (2024).

18. Alam, Iqbal, Kashif Sharif, Fan Li, Zohaib Latif, Md Monjurul Karim, Sujit Biswas, Boubakr Nour, and Yu Wang. "A survey of network virtualization techniques for Internet of Things using SDN and NFV." ACM Computing Surveys (CSUR) 53, no. 2 (2020): 1-40.

19. Bernabe, Jorge Bernal, Alejandro Molina, Antonio Skarmeta, Stefano Bianchi, Enrico Cambiaso, Ivan Vaccari, Silvia Scaglione et al. "Key Innovations in ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures." In Challenges in Cybersecurity and Privacy-the European Research Landscape, pp. 23-53. River Publishers, 2022.

20. Ahuja, Nisha, and Debajyoti Mukhopadhyay. "Identification of DDoS Attack on IoT Network Using SDN." In 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), pp. 879-884. IEEE, 2023.

21. Marler, R. Timothy, and Jasbir S. Arora. "The weighted sum method for multi-objective optimization: new insights." Structural and multidisciplinary optimization 41 (2010): 853-862.

22. San Cristóbal Mateo, José Ramón, and José Ramón San Cristóbal Mateo. "Weighted sum method and weighted product method." Multi criteria analysis in the renewable energy industry (2012): 19-22.

23. Stanimirovic, Ivan P., Milan LjZlatanovic, and Marko D. Petkovic. "On the linear weighted sum method for multi-objective optimization." Facta Acta Univ 26, no. 4 (2011): 49-63.

24. Kim, Il Yong, and Oliver L. De Weck. "Adaptive weighted-sum method for bi-objective optimization: Pareto front generation." Structural and multidisciplinary optimization 29 (2005): 149-158.

25. Wang, Rui, Zhongbao Zhou, Hisao Ishibuchi, Tianjun Liao, and Tao Zhang. "Localized weighted sum method for many-objective optimization." IEEE Transactions on Evolutionary Computation 22, no. 1 (2016): 3-18.

26. Ehrgott, Matthias. "The weighted sum method and related topics." Multicriteria Optimization (2005): 65-95.

27. Hazelrigg, George A. "A note on the weighted sum method." Journal of Mechanical Design 141, no. 10 (2019): 100301.

28. Weeraddana, Pradeep Chathuranga, Marian Codreanu, Matti Latva-aho, Anthony Ephremides, and Carlo Fischione. "Weighted sum-rate maximization in wireless networks: A review." Foundations and Trends® in Networking 6, no. 1–2 (2012): 1-163.

Citation: Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis" JJournal of Artificial intelligence and Machine Learning., 2023, vol.1, no. 3, pp. 1–7. doi: https://dx.doi.org/10.55124/jaim.v1i3.282