Next-Generation Network Security: An Analysis of Threats, Challenges and Emerging Intelligent Defenses Within SDN and NFV Architectures

Amina SAHBI[1], Faouzi JAIDI[2], Adel BOUHOULA[3]
University of Carthage, Higher School of Communications of Tunis,
LR11TIC03 Innov'COM Innovation of Communicant and Cooperative Mobiles Laboratory,
LR18TIC01 Digital Security Research Lab, Tunis, Tunisia[1,2]
University of Carthage, National School of Engineers of Carthage, Tunis, Tunisia[2]
Arabian Gulf University, Department of Computing, University of Carthage, Kingdom of Bahrain[3]

***Abstract*—The integration of Software Defined Networking (SDN) and Network Function Virtualization (NFV) offers considerable advantages in terms of scalability, interoperability, and cost-efficiency. They redefine network architecture, replacing rigid hardware-based control with a more flexible, software-driven approach. However, this convergence also introduces significant security threats and challenges due to architectural vulnerabilities and an expanded attack surface. This study presents a comprehensive overview of the key security risks associated with SDN/NFV networks. It analyzes existing countermeasures, highlighting their effectiveness in addressing specific threats while identifying limitations in achieving comprehensive security due to inherent architectural vulnerabilities. The study concludes with a discussion on open challenges and future research directions toward more secure and resilient network infrastructures. This study highlights the importance of an integrated security approach and identifies areas where further research is required to enhance SDN/NFV security.**

***Keywords*—Next generation network security; software defined networking; network function virtualization; network security; artificial intelligence**

I. Introduction

In today's hyper-connected world, networks have become the backbone of modern communications and services, from enterprise operations to personal applications. As networks grow in size and complexity, traditional networking architectures face limitations in terms of scalability, flexibility, and manageability. Therefore, centralized administration and virtualized infrastructures have become essential for effective remote management and configuration [1].

This has led to the development of SDN, a novel paradigm that decouples the control plane from the data plane, offering greater programmability. SDN provides a centralized view of the entire network, enabling administrators to dynamically manage network traffic and resources through software applications. By separating control functions from the physical infrastructure, SDN allows the rapid deployment of new network services, particularly in environments such as data centers, cloud computing, and large-scale enterprise networks [2].

While SDN centralizes and simplifies network control, NFV focuses on decoupling network services from physical devices by running them as software applications on virtualized platforms. Through this change, hardware costs are reduced, scalability is enhanced, and service provision is accelerated. Combining SDN with NFV provides a more responsive and controlled network architecture, especially for dynamic environments [3].

Despite these promising benefits, the integration of SDN/NFV causes new vulnerabilities and security issues. The centralized control in SDN makes controllers potential targets for cyber attacks [4]. Furthermore, open interfaces such as Northbound and Southbound Application Programming Interfaces (APIs) expand the attack surface, creating more entry points for attackers [5].

Given these emerging security challenges, traditional security mechanisms become inadequate. Artificial Intelligence (AI) has increasingly become essential to detect, mitigate, and prevent sophisticated attacks proactively [6]. Similar perspectives have been developed in our prior works, where AI and Machine Learning (ML) were applied to enhance SDN/NFV security [7], [8]. AI techniques enable automated anomaly detection, adaptive threat response, and intelligent decision-making that considerably surpass the capabilities of conventional security solutions.

To frame the scope of this research, our study is guided by a central inquiry: How can intelligent defense mechanisms enhance the security of SDN and NFV architectures by addressing their inherent vulnerabilities and evolving threats? More specifically, we ask in what ways such defenses can strengthen these architectures against critical weaknesses and emerging cyberattacks, and furthermore, how next-generation intelligent strategies may be leveraged to secure SDN and NFV while overcoming their most pressing challenges. These complementary perspectives establish the foundation for the analysis and recommendations presented in this work.

This study contributes by offering a thorough examination of security vulnerabilities within SDN and NFV ecosystems, a critical review of AI-based defense strategies, and the identification of research gaps that hinder robust implementation. Furthermore, it outlines key recommendations to guide future developments toward more resilient and secure programmable networks.

This study intends to encourage further studies towards enhancing the security of next-generation network environments by highlighting the need of an integrated security strategy. In our study, we provide an overview of the main security risks influencing network topologies based on SDN and NFV. To address these vulnerabilities, we review the countermeasures that have been proposed in the literature and assess their effectiveness and limitations. In addition, we discuss current research gaps and open challenges that may hinder the implementation of reliable and secure SDN/NFV networks.

The structure of this study is as follows : Section II introduces background and foundational concepts related to SDN and NFV, followed by an overview of major security threats and challenges in Section III. Section IV presents countermeasures and a discussion on future directions. Section V provides concluding remarks and perspectives for future research.

II. Background and Fundamentals

A. From Traditional Network to Software-Defined Networking

The rapid progress of digital technologies, the virtualization of services, and data intensive applications has revealed the limitations of traditional network infrastructures [9]. Traditional networks rely on a distributed control model where configuration and management tasks, such as routing policies, access control rules, and software updates, must be applied individually to each device. This lack of centralized orchestration raises operational complexity, extends the time required to deploy updates or resolve misconfigurations, and leads to higher maintenance costs [10]. Additionally, these architectures frequently suffer from insufficient use of computational and bandwidth resources, as well as a restricted capacity.

SDN emerged as a solution to overcome these limitations. By separating the control plane from the data plane, SDN enables centralized network control and simplifies the deployment of new services, as illustrated in Fig. 1.

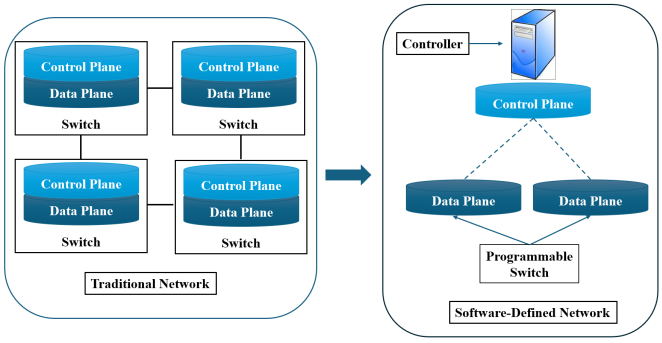

Fig. 1. Traditional Network vs Software-defined networks.

The main benefit of SDN is its ability to decouple network control from hardware, allowing administrators to manage and modify the network through software interfaces without need for physical alterations [11]. The abstraction is improved by the vendor-neutral architecture of SDN, which ensures seamless interoperability across multiple network devices and platforms. This allows enterprises to extend their infrastructure, optimize performance on customer demand, and respond quickly to operational changes or security incidents [11]. The inherent programmability and adaptability of SDN environments also contribute to significantly better resource utilization, allowing networks to operate more efficiently and respond dynamically to real-time demands [12].

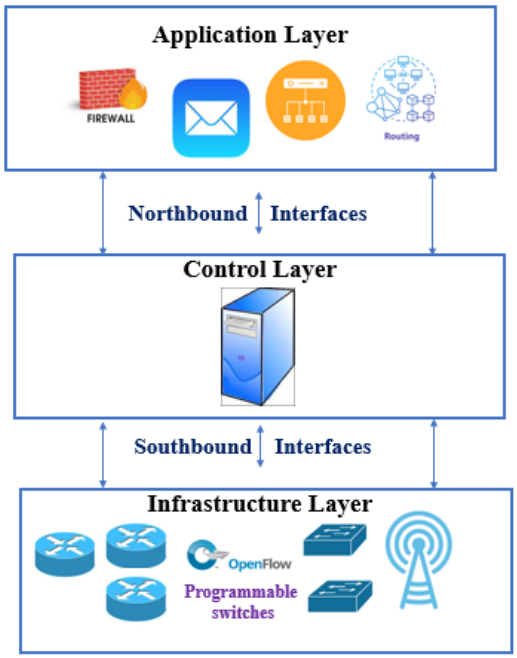

Fig. 2. Software-defined networks architecture.

Fig. 2 displays the fundamental architecture of SDN. It consists of three main layers: the application layer, the control layer, and the infrastructure or the data layer [13]. These layers are connected to one another by well-defined interfaces, known as northbound and southbound interfaces. This ensures that interactions and communication are carried out without any disruptions across the framework. Network behavior and policies are defined by software services hosted at the application layer. These services may include traffic engineering, quality of service (QoS) management, intrusion detection, load balancing, and security monitoring. Instead of explicitly configuring hardware, applications communicate policies to the controller through the northbound interface. This abstraction allows developers to introduce new features or security functions rapidly without being constrained by the limitations of proprietary hardware. In SDN systems, this layer is ultimately responsible for enabling innovation and service agility [14].

The control layer is the most important part of SDN. It makes decisions by transforming application-level requirements into precise routing rules [14]. The SDN controller has a global, real-time view of the whole network, which allows it to make smart decisions about how traffic should be routed or managed. This layer converts high-level application requirements into low-level forwarding rules, which are installed dynamically on switches and routers. By decoupling decision-making from the physical devices, the controller ensures coherent policy enforcement, optimized resource usage, and rapid adaptation to network changes or security events. More-

over, this layer supports programmability, allowing network operators to define behavior through APIs and automation frameworks.

The last layer, known as the infrastructure layer, also referred to as the data plane, consists of physical or virtual forwarding devices, such as switches and routers, that execute the instructions received from the controller through the southbound interface [15]. These devices are simplified to focus exclusively on packet forwarding, which reduces their complexity, cost, and management overhead. The controller may change their behavior dynamically, allowing for precise traffic flow management and effective network resource use.

These layers together represent the four basic principles of SDN: network programmability, abstraction of physical infrastructure, centralized intelligence, and the separation of control and data planes. Supported by protocols such as OpenFlow, this architecture simplifies network management, enhances scalability, and delivers the flexibility needed to respond quickly to evolving operational and security demands.

B. The Need for Network Function Virtualization

Although SDN significantly enhances network control by decoupling the control logic from forwarding devices, it does not virtualize the network services themselves [16]. Middleboxes such as load balancers, firewalls, and NAT devices are still dependent on proprietary hardware. This limits flexibility and drives up operational costs. To address these constraints and fully exploit the paradigm of SDN, NFV was developed.

The goal of NFV is to enable network functions to perform as software instances on common, commodity servers by separating them from specialized hardware [17]. This change removes reliance on specific vendor appliances and allows operators to deploy, scale, and manage services flexibly. SDN offers centralized intelligence, and NFV delivers virtualized services, creating an agile and cost effective networking environment.

According to the European Telecommunications Standards Institute (ETSI), NFV is built upon three essential key components, illustrated in Fig. 3.

The components include Virtual Network Functions (VNFs), Network Function Virtualization Infrastructure (NFVI), and the Management and Orchestration (MANO) system. Together, NFVI, VNFs, and MANO enable a software-driven network that is automated and easily adaptable to operational demands.

The first is the NFVI, which includes the physical hardware, virtualization layer, and the virtualized resources. It serves as the foundational layer, integrating the physical hardware (servers, storage, and network resources) with a virtualization layer that abstracts these resources into pools of compute, storage, and connectivity. This abstraction allows for the dynamic allocation of virtualized resources, supporting the instantiation of virtual machines (VMs) and containers that host the network functions [18]. This layer provides the foundation to host virtual machines and containers.

The second block is VNFs, which implement specific network functions using the virtual resources offered by the

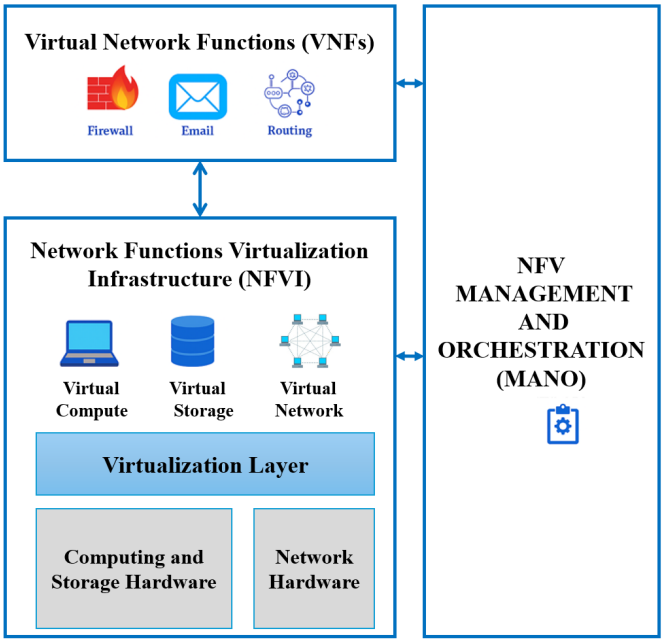

Fig. 3. Network function virtualization.

NFVI. Examples include virtual routers (vRouter), firewalls (vFW), and NAT (vNAT). These VNFs are modular and can be deployed, updated, or removed dynamically [18].

The third and most critical block is MANO [18]. MANO interacts with both the VNFs and the NFVI to manage the lifecycle of services and resources. It is responsible for automating tasks such as deployment, scaling, monitoring, and resource allocation. This block ensures that virtual services can be managed efficiently and adjusted in real-time based on traffic demands or system policies.

NFV offers several benefits, as shown in Fig. 4:

By replacing dedicated appliances with software instances, NFV reduces capital expenditures (CAPEX) and operational expenditures (OPEX) while accelerating service deployment. It also enables faster deployment of new services and better scalability, since virtual functions can be instantiated or terminated as needed. In addition, NFV simplifies updates and promotes vendor independence, allowing service providers to choose flexible software solutions without being locked to specific hardware platforms [19]. These characteristics position NFV as a key enabler of flexible, automated, and future-proof network infrastructures.

C. SDN and NFV Complementarity

SDN and NFV are two complementary technologies that aim to modernize and optimize network architecture. While SDN focuses on the separation of the control and data planes to enable centralized overview and programmable control, NFV addresses the virtualization of network services that traditionally relied on dedicated hardware.

These two paradigms operate at different layers of the network but are designed to work together [20]. SDN provides the intelligence and global view necessary to control

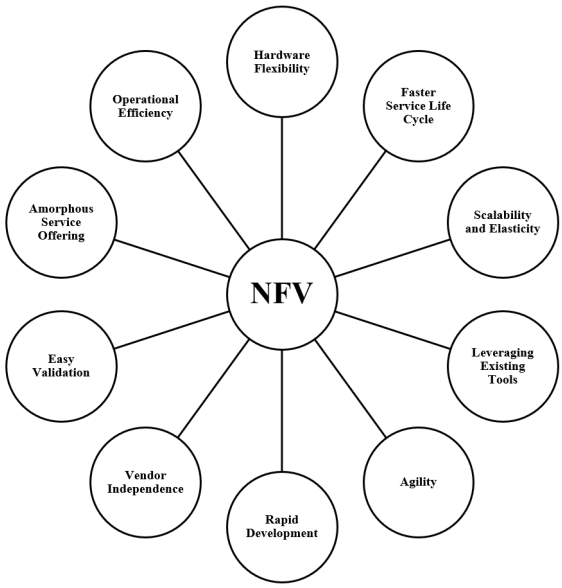

Fig. 4. Advantages of network function virtualization.

how data flows across the network, while NFV delivers the actual network functions as software running on virtualized infrastructure. The integration of SDN and NFV results in a flexible and programmable networking model, where services and control are both decoupled from rigid infrastructures and can evolve dynamically to meet operational requirements.

This synergy allows for greater agility, faster service deployment, and reduced operational complexity. It also supports automation and resource optimization by enabling flexible service chaining and centralized orchestration. The combination of SDN and NFV is particularly beneficial in modern use cases such as 5G, cloud-native infrastructure, and edge computing, where scalability and adaptability are essential [21]. To better understand the roles and differences of SDN and NFV, Table I presents a comparative summary of their key aspects.

TABLE I. COMPARISON BETWEEN SDN AND NFV

Aspect	SDN	NFV
Primary Focus	Separation of control and data planes	Virtualization of network functions
Key Component	SDN Controller	VNFs, NFVI, MANO
Control Mechanism	Centralized control via software	Lifecycle and resource management via MANO
Infrastructure	Programmable switches and routers	Servers and virtualization layers
Deployment Speed	Faster path control and policy updates	Rapid deployment of virtual services
Vendor Dependency	Vendor-neutral (via OpenFlow and APIs)	Reduces reliance on proprietary hardware
Example Use Cases	Dynamic routing, traffic engineering	Virtual firewalls, NAT, load balancing
Relationship	Controls how data flows in the network	Provides the services that flow over the network infrastructure

While SDN enables centralized control and dynamic network management, it does not cover the virtualization of the network functions themselves. For this reason, a complementary approach called NFV was introduced to decouple network services from dedicated hardware. NFV enables these services such as routing, firewalls, or load balancing to run as software on general purpose servers.

III. SECURITY THREATS AND CHALLENGES

A. Software-Defined Networking Challenges

SDN introduces a revolutionary network architecture; however, this change brings several challenges. One of the most critical is the centralization of control. Acting as the brain of the network, the controller becomes a single point of failure. Any malfunction, misconfiguration, or successful intrusion against this component can lead to a complete collapse of network services. Attackers who manage to compromise the controller gain unprecedented control, enabling them to alter flow rules, inject malicious policies, and disrupt or hijack traffic across the entire infrastructure. If compromised, the controller could enable full network disruption [22]. In this context, our earlier research proposed intelligent approaches to detect and resolve policy violations within SDN control and data planes [23], [24].

In addition, communication between SDN components introduces another layer of vulnerability. The southbound interface, typically relying on protocols such as OpenFlow [25], lacks robust native security features, leaving it exposed to message spoofing, tampering, and man-in-the-middle attacks (MitM). Similarly, northbound interfaces often suffer from insufficient access control. When improperly secured, these interfaces may allow unauthorized access or the injection of malicious services which significantly weakens the trust model of the entire architecture.

Scalability [26], also represents a persistent challenge. As networks grow in size and complexity, optimizing controller placement, balancing workloads, and minimizing latency in control messages become increasingly challenging. In distributed deployments, where multiple controllers must synchronize to maintain a coherent global view, inconsistencies may arise, resulting in policy conflicts and operational instability [27]. These architectural weaknesses are aggravated by the absence of unified security frameworks and the reliance on open-source components that often lack rigorous hardening against advanced threats.

A particularly severe threat to SDN infrastructures is the Distributed Denial of Service (DDoS) attack. In traditional networks, such attacks aim to overwhelm servers or network links with excessive traffic, but in SDN, the impact is often more damaging because of the centralized nature of control. During a DDoS attack, large volumes of malicious traffic are generated from multiple sources and directed toward the data plane, triggering a flood of control messages sent to the controller. This sudden surge of requests can exhaust the controller's processing capacity, resulting in delays, instability, or even total network failure. Attackers may also target the controller directly, exploiting its role as the decision-making hub to paralyze its operations. The consequences of a successful DDoS attack include severe service degradation, unavailability of critical applications, and disruption of communication across the entire network [28].

Beyond these aspects, SDN operates in a highly dynamic environment where policies, flows, and states change continuously. Ensuring consistent visibility across all elements, preventing rule conflicts, and maintaining traceability in such rapidly evolving conditions require sophisticated monitoring systems that are still under development [29]. Without adequate oversight, misconfigurations or silent intrusions can remain undetected for extended periods, undermining the overall security posture of the network.

Table II summarizes the main threats affecting each SDN domain, outlines the associated risks, and highlights defensive measures capable of mitigating these vulnerabilities. This analysis emphasizes the urgent need for integrated security mechanisms capable of addressing both the architectural weaknesses and the evolving threat landscape that characterizes SDN deployments [30].

B. Network Function Virtualization Challenges

NFV reshapes traditional network architectures by decoupling network functions from proprietary hardware and deploying them as software instances on commodity servers [19]. This transformation provides unprecedented scalability and operational flexibility, but at the same time introduces complex risks that threaten the reliability and security of virtualized infrastructures [31]. The dynamic and distributed nature of NFV, where VNFs are instantiated, migrated, or terminated on demand, creates an environment in which ensuring consistency, isolation, and performance becomes highly challenging. Unlike static hardware-based systems, NFV relies on virtualization layers, orchestration components, and multi-domain coordination, all of which may become sources of vulnerabilities if not carefully secured [31].

The threats associated with NFV extend across multiple layers, from the physical hardware to virtualized resources and orchestration control, each requiring tailored countermeasures. Table III consolidates the main threat categories, describes their mechanisms, and links them to appropriate mitigation strategies. This table demonstrates that achieving security in NFV is not the responsibility of a single component but rather the result of coordinated efforts across all layers, combining isolation, authentication, monitoring, and resilience techniques to ensure that flexibility does not come at the expense of security.

One major concern is the complexity of orchestration and management of virtualized resources across multiple domains. The dynamic nature of VNFs makes it difficult to ensure consistent performance, availability, and isolation. Furthermore, resource allocation and scaling mechanisms can lead to unpredictable performance and increased attack surfaces. Another challenge lies in interoperability and standardization. NFV environments often consist of heterogeneous components from different vendors, making integration and management more error prone. Additionally, the reliability and fault tolerance of VNFs must be guaranteed, especially in critical applications such as vehicular or industrial networks.

The orchestration of VNFs across heterogeneous infrastructures is one of the primary difficulties in NFV deployment. Managing resources dynamically while maintaining service continuity requires precise coordination of computing, storage, and network elements, a task that becomes increasingly complex in multi-tenant or cross domain environments. Inconsistent resource allocation, poor synchronization, or errors during VNF migration may lead to unpredictable QoS, degradation in performance, and in some cases complete service disruption [32]. Furthermore, the lack of standardized interfaces and uniform protocols between components from different vendors hampers interoperability, making integration error prone and potentially insecure. These architectural constraints are even more critical in latency sensitive environments such as industrial control systems and vehicular networks, where reliability and fault tolerance are non negotiable requirements [33].

From a security perspective, NFV inherits threats from both traditional networks and cloud computing while introducing new attack surfaces specific to virtualization. Hypervisors, which manage the virtualization layer, are particularly sensitive targets. Also, a successful exploitation can compromise all hosted VNFs and give attackers control over the underlying infrastructure. The orchestration layer, known as MANO, also becomes a high-value target because of its privileged role in managing the entire NFV lifecycle. Exploiting insecure APIs or misconfigurations at this level can lead to unauthorized operations, data leaks, or the injection of malicious components [34]. The trustworthiness of third-party VNFs is another major concern, as these functions may contain backdoors, hidden malware, or exploitable vulnerabilities that compromise the entire chain of services once deployed.

Another significant challenge arises from the lifecycle of VNFs. Each instantiation, scaling, migration, or termination presents specific vulnerabilities [35]. For example, during migration, data and states are transferred across domains, and insufficient protection during this process can allow interception or tampering. Similarly, insecure onboarding of VNFs can facilitate the deployment of malicious images, while improper termination may leave residual data or open configurations exploitable by attackers. The absence of continuous monitoring during these operations further increases the likelihood of undetected intrusions or misconfigurations persisting within the infrastructure [36].

The complexity of NFV also lies in its dependency on cloud-like environments and programmable interfaces, where the attack surface expands rapidly with each added component or tenant. An adversary can exploit poorly monitored orchestration decisions, manipulate inter-VNF communications, or overload physical resources to trigger cascading failures. These scenarios highlight the urgent need for context-aware intrusion detection, runtime verification mechanisms, and automated incident response capable of adapting to evolving threats. At the same time, strict verification of VNF integrity, secure software supply chains, and robust cryptographic protections for management channels are essential to strengthen trust within NFV ecosystems. Fig. 5 highlights some of the most critical threats affecting NFV environments. These threats arise at multiple layers of the architecture, ranging from physical resources to virtualization platforms and orchestration mechanisms, underscoring the need for comprehensive and coordinated defense strategies.

TABLE II. RISKS AND THREATS IN SDN SECURITY DOMAINS

Security Component	Vulnerability/Threat	Risk Consequences	Defensive Action
Control Plane	Over dependence on a single controller instance	Loss of orchestration, network paralysis	Use distributed architectures, backup controllers, and high availability frameworks
Northbound Interfaces	APIs exposed to orchestration platforms and apps without strict security controls	Unauthorized access, policy override, service injection	TLS encryption, API gateway, strong RBAC, input validation
Southbound Interfaces	Message injection or tampering in protocols like OpenFlow	Corrupted flow tables, misrouting, loss of trust	Message authentication, channel encryption, switch-level access policies
Application Layer	Malicious or vulnerable apps interacting with the controller	Flow conflicts, data leakage, service disruption	App sandboxing, behavioral monitoring, application certification workflows
Flow Management	Conflicts or outdated flows in switch tables	Policy violation, packet loops, resource waste	Implement rule expiration, rule audits, consistency validation engines
Inter Communication	Lack of verification between East and West control domains	Propagation of compromised state, unsynchronized behavior	Signed messaging, secure sync protocols, consensus mechanisms
Monitoring	Unlogged configuration changes, missing traceability	Persistent misconfigurations, undetected policy violations	Continuous auditing, automated logging, version control and rollback systems

TABLE III. VIRTUAL NETWORK SECURITY: THREATS VS COUNTERMEASURES

Threat Category	Threats	Countermeasure Category	Countermeasures
Disclosure	Information Leakage, Information Interception, Introspection Exploitation	Access Control	Trusted Virtual Domains, Sandboxes
Deception	Identity Fraud, Loss of Registry Entries, Replay Attacks	Authentication	Interoperability Between Federations, Certificate-Based, Key-Based
Disruption	Physical Resource Overloading, Physical Resource Failure	Confidentiality	VLANs and VPNs, Tunneling and Cryptography, Firewalling and Subnetting
Usurpation	Identity Fraud, Software Vulnerability Exploitation	Integrity, Nonrepudiation, Availability	Path Splitting, Limiting Introspection, Cryptography, Timestamping, Physical Resource Isolation, Virtual Network Resilience

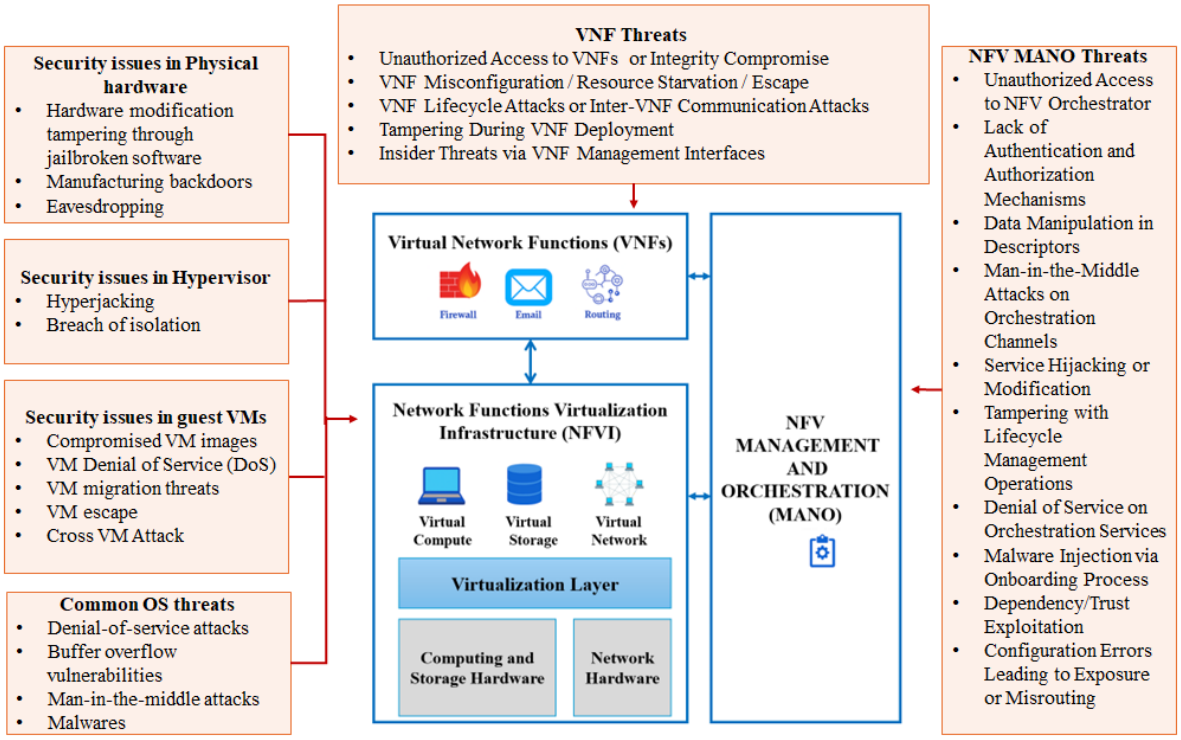

Fig. 5. Network function virtualization threats.

C. Security Threats within SDN and NFV

Nowadays, the majority of existing frameworks are focused on migrating network functions from hardware devices to virtualization environments. SDN and NFV are two independent but complementary concepts. When combined, they provide an additional benefit in terms of simplified management, rapid service deployment, and reduced operational costs. However,

it also significantly expands the attack surface, as each technology introduces its vulnerabilities while their interaction creates new, composite risks that span multiple layers of the architecture [36].

In SDN, the centralized controller is an essential asset but also a critical weakness. Its compromise can disrupt the entire network, enabling attackers to manipulate flow rules or shut down services altogether. Similarly, NFV introduces threats at the virtualization layer, where hypervisors and VNFs become primary targets. Malicious VNFs or hypervisor exploits may breach isolation boundaries, gaining access to the host environment and other tenants. The orchestration layer, shared between SDN and NFV, faces its own set of threats. Weakly secured MANO components or misconfigured APIs can allow privilege escalation, unauthorized control operations, or the deployment of rogue VNFs that compromise the network.

MitM attacks [37], represent another severe risk in these ecosystems. Interception of traffic can occur both in SDN control channels and during NFV operations such as VNF migration, allowing adversaries to manipulate or spy on communications. DoS attacks are also particularly damaging in this context. Overwhelming the SDN controller, the NFV orchestrator, or the underlying infrastructure can degrade performance or even cause complete service outages. These attacks become more difficult to mitigate in dynamic environments, where large volumes of traffic are legitimate and distinguishing malicious flows is challenging.

The programmability of SDN and NFV, while central to their flexibility, also creates opportunities for misconfiguration. Incorrect policies, insecure automation scripts, and flawed orchestration workflows can unintentionally expose the network to vulnerabilities without any direct attacker involvement. Furthermore, unpatched software in SDN applications or VNF packages provides attackers with exploitable weaknesses that can propagate rapidly across virtualized infrastructures. Third-party VNFs pose an additional risk, as they may include hidden backdoors or malicious code capable of undermining the integrity of the network once deployed [38].

The integration of SDN and NFV introduces complex interdependencies between control, orchestration, and virtualization layers. This tight coupling means that an attack on one component can cascade, affecting other layers and amplifying its impact. Securing such an environment requires more isolated defense mechanisms. It demands a holistic approach, where isolation, strong authentication, integrity verification, and continuous monitoring are enforced consistently across all layers. Real-time intrusion detection, secure orchestration policies, and rigorous VNF verification processes are crucial for ensuring that the benefits of SDN/NFV adoption are not undermined by evolving cyber threats [39].

Table IV synthesizes the main threat domains observed in SDN and NFV environments, and highlights how their integration increases exposure to attacks. This summary underlines the necessity for coordinated security mechanisms capable of addressing vulnerabilities at every level of the SDN/NFV stack, preventing isolated weaknesses from escalating into systemic failures.

TABLE IV. SUMMARY OF SECURITY CHALLENGES IN SDN AND NFV

Domain	Challenges / Threats
NFV	VNF isolation failure, insecure lifecycle management, hypervisor vulnerabilities, untrusted VNF onboarding
SDN	Centralized controller exposure, insecure APIs, third-party app vulnerabilities, southbound protocol threats
SDN/NFV Integration	DoS attacks, MitM, VNF escape, orchestration manipulation, privilege escalation

IV. COUNTERMEASURES REVIEW AND FUTURE DIRECTIONS

A. Countermeasures Review

In recent years, research on SDN and NFV security has evolved considerably, moving from traditional protection mechanisms to intelligent, adaptive frameworks. Countermeasures have been proposed for every architectural layer, including the control plane, data plane, virtualization infrastructure, orchestration systems, and exposed APIs.

For SDN, earlier studies recommended strengthening the controller through redundancy, fine-grained access controls, and secure southbound communication. Jiménez et al. [40] applied the STRIDE methodology to analyze threats across SDN layers and recommended tighter access policies, controller hardening, and secure APIs. Despite these enhancements, they noted unresolved challenges such as dynamic policy conflicts and insufficient protection against zero-day vulnerabilities.

Beyond static defenses, several studies have proposed AI-enhanced security frameworks. Shobowale et al. [41] explored 5G threats focusing on SDN and NFV layers, introducing a combination of blockchain-based authentication, layered access control, and AI-driven intrusion detection. However, their framework faced scalability challenges, high computational overhead, and limited coverage against emerging side-channel and supply-chain attacks.

In the NFV context, Pattaranantakul et al. [42] proposed countermeasures such as hypervisor isolation, trust domains, and adaptive access control. While these techniques improved security at individual layers, the lack of orchestration-level integration allowed sophisticated interlayer attacks to persist.

Other research explored entropy-based detection. Fan et al. [43] developed a lightweight approach using fusion entropy to detect DDoS attacks in SDN. Their model combined information entropy and logarithmic energy entropy to identify anomalies with high precision. Although effective in simulations, it required manual threshold settings and lacked evaluation in complex multi-controller deployments.

More recent works emphasized hybrid and intelligent systems. Nadeem et al. [44], reviewed ML techniques for securing SDN, focusing on detecting DDoS, botnets, and ransomware. They demonstrated how supervised and deep learning models can improve detection accuracy, while also highlighting vulnerabilities to adversarial samples and the need for explainability. Similarly, the Hybrid SDN-IDS framework leveraged dynamic SDN control and NFV monitoring to detect and mitigate threats in real-time. Its evaluation showed improved detection rates, but its performance under large-scale traffic conditions remains uncertain.

TABLE V. FUTURE RESEARCH DIRECTIONS FOR ENHANCING SDN/NFV SECURITY

Research Direction	Objective	Addressed Challenge
Unified Threat Intelligence [40], [46]	Enable cross-layer visibility and event correlation across SDN, NFV, and cloud domains	Fragmented monitoring, lack of coordination between components
Lightweight, Real-Time Detection [43], [44]	Design efficient anomaly detection models suitable for resource-constrained environments	High computational cost of current AI methods; unsuitable for IoT/edge
Autonomous and Self-Adaptive Security [47]	Develop self-healing systems that react to evolving threats and reconfigure policies automatically	Inability to respond dynamically to zero-day or stealth attacks
Secure VNF Marketplaces [19], [42]	Ensure trust in third-party VNFs through attestation, certification, and runtime monitoring	VNF tampering, backdoors, and insecure onboarding
Formal Verification of Orchestration Policies [41]	Apply formal methods to validate orchestration rules before deployment	Misconfiguration risks, policy inconsistencies, privilege escalation
Post-Quantum Cryptography and Trusted Execution Environments (TEEs) [48]	Strengthen data confidentiality and control-plane integrity in next-gen programmable networks	Future cryptographic attacks; lack of hardware-assisted security primitives

For Next-Generation Networks, AI-driven cross-layer frameworks have gained traction. Alnaim [45] critically examined SDN, NFV, and network slicing in 5G, proposing security-by-design methodologies and UML-based reference models. However, the lack of standardized enforcement limits their adoption. The study [46] proposed integrating SDN controllers, NFV orchestration, and AI anomaly detection for slice-aware protection in 5G/6G. While promising, its real-world latency and scalability remain to be validated. Complementary to these studies, our contributions investigated how ML-based algorithms can strengthen intrusion detection in SDN/NFV environments [8] and proposed frameworks for automated policy enforcement [23].

Finally, Li et al. [47] introduced a proactive defense combining Moving Target Defense (MTD) and Reinforcement Learning (RL). This approach dynamically reconfigures network parameters to counter stealthy attacks, yet introduces new risks tied to the vulnerabilities of RL models themselves.

Although several AI-based security mechanisms have been proposed in the literature, most are evaluated in ideal or simulated settings. There remains a lack of critical assessment under adversarial scenarios or across heterogeneous infrastructures combining SDN controllers, NFV orchestrators, and multi-tenant environments.

In summary, literature shows a clear progression toward adaptive, AI-enhanced, and cross-layer security frameworks for SDN and NFV. However, common limitations persist such as high computational demands, lack of standardized orchestration, and limited validation under real world conditions. These findings highlight the need for lightweight AI models, resilient orchestration-level controls, and robust defenses against adversarial threats.

B. Discussion and Future Directions

The reviewed literature confirms a clear evolution toward AI-augmented, cross-layer, and adaptive security frameworks for SDN and NFV networks. These solutions aim to address complex threats in highly dynamic environments such as 5G, IoT, and vehicular networks. Nevertheless, several persistent challenges remain unresolved.

Among AI techniques, supervised models dominate current literature, yet their dependence on labeled data limits its real-world generalization [44]. RL and unsupervised approaches, while promising, still lack extensive benchmarking in SDN/NFV contexts [47]. This observation is consistent with earlier surveys that emphasized the gap between simulation-based validation and practical deployment in operational infrastructures [40], [44]. For instance, [40] highlights how current solutions often remain limited to laboratory environments, reducing their applicability to real-world programmable infrastructures.

Another key limitation lies in the absence of standardized and interoperable security frameworks. Current solutions often address threats at isolated layers (control, data, or virtualization), but fail to ensure consistent protection across the entire architecture [41], [46]. Moreover, many approaches are validated only under ideal laboratory conditions, with limited assessment under realistic network traffic and latency scenarios [45]. This limitation is particularly evident in large-scale SDN deployments, where orchestration complexity and latency constraints cannot be ignored [46].

AI and ML have shown significant potential in improving detection and response capabilities, as demonstrated in recent works on SDN security [44], [45]. However, they bring new risks such as high computational demands, lack of explainability, and exposure to adversarial manipulation [25], [47]. The complexity of training and deploying robust AI models remains a barrier, particularly in edge and multi-tenant scenarios where resources are constrained, a limitation which is also emphasized in studies on real-time SDN/NFV security frameworks [41], [46]. These findings are consistent with our previous proposals, which stressed the importance of lightweight and explainable AI for practical deployment in programmable networks [7], [24]. As noted in [47], adversarial interference against AI-driven systems represents an emerging risk that requires more resilient and transparent defense mechanisms.

Moreover, a critical gap remains in evaluating these security frameworks under realistic, heterogeneous environments. Very few approaches have been tested across operational SDN/NFV infrastructures involving cross-domain orchestration, adversarial interference, or third-party VNF integrations factors, that are crucial for assessing their robustness and scalability.

In summary, while substantial progress has been made toward intelligent and adaptive SDN/NFV defenses, the lit-

erature highlights clear research gaps. Addressing interoperability, ensuring scalability, and developing robust, adversarial-resilient AI models remain essential for advancing secure and trustworthy programmable networks.

To guide future work, several promising directions have emerged from the literature. These focuses on enhancing security intelligence, improving the adaptability of defenses, and addressing the unique challenges of highly dynamic SDN/NFV ecosystems. Table V summarizes these key directions and their corresponding objectives.

In addition to these conceptual directions, future work will include experimental validation of selected approaches, particularly AI-driven detection mechanisms, through implementation and evaluation in real-world programmable network environments such as SDN-based vehicular or cloud-edge architectures.

In conclusion, while existing studies have laid a strong foundation, the increasing complexity of SDN and NFV demands new generations of security frameworks that are not only intelligent and adaptive but also lightweight, verifiable, and resilient to emerging attack strategies.

V. Conclusion

Next-Generation Networks, built upon concepts like SDN and NFV, have emerged as innovative and diverse architectures. By decoupling the control and data planes and virtualizing network functions, they offer unprecedented flexibility, programmability, and operational efficiency. However, this paradigm shift also brings forth new attack vectors, architectural weaknesses, and orchestration challenges that demand proactive and adaptive security measures.

This study underscores the necessity of adopting a unified and cross-layer security framework to mitigate the evolving threats specific to SDN and NFV deployments. By identifying critical gaps in existing solutions and evaluating their limitations, it aims to inspire more effective approaches tailored to the demands of programmable and distributed infrastructures. Furthermore, the integration of intelligent techniques, such as AI and ML, emerges as a promising direction offering dynamic, context-aware defenses suited for complex environments such as 5G, IoT, and edge networks.

In line with our guiding research questions, this work has shown that intelligent defense mechanisms can enhance the security of SDN and NFV by addressing their inherent vulnerabilities. They can also strengthen these architectures against emerging cyberattacks, while next-generation intelligent strategies hold strong potential to overcome their most pressing challenges. Nevertheless, certain limitations remain: most proposed solutions are evaluated in simulated settings, lack cross-layer interoperability, and do not fully consider adversarial manipulation or real-world scalability.

Future research must therefore prioritize resilient, lightweight, and verifiable security mechanisms validated under realistic deployment conditions. By closing these gaps, the community can move closer to achieving robust and trustworthy programmable networks capable of supporting critical infrastructures in 5G, IoT, and beyond.

References

[1] Awais, Muhammad, et al. "Comparative analysis of traditional and software defined networks." 2021 Mohammad Ali Jinnah University International Conference on Computing (MAJICC). IEEE, 2021.

[2] Çetin, Ahmet, Derya Gültekin, and Nihan Yıldırım. "Implications of NFV-SDN technology: An exploratory study of Turkish telecom industry." Journal of Global Information Technology Management 28.2 (2025): 111-135.

[3] Herrera, Juliver Gil, and Juan Felipe Botero. "Resource allocation in NFV: A comprehensive survey." IEEE Transactions on Network and Service Management 13.3 (2016): 518-532.

[4] Ebadinezhad, Sahar, and Pierre Fabrice Nlend Bayemi. "SDN and NFV security challenges and solutions for minimizing failures in IoT networks: Literature review." Research Advances in Network Technologies (2025): 22-40.

[5] Xu, Chunxue. "Resource Optimization Algorithm for 5G Core Network Integrating NFV and SDN Technologies." International Journal of Intelligent Networks (2025).

[6] Hatim, J. A. A. D. O. U. N. I., C. H. A. O. U. I. Habiba, and S. A. A. D. I. Chaimae. "Evolving Security for 6G: Integrating Software-Defined Networking and Network Function Virtualization into Next-Generation Architectures." International Journal of Advanced Computer Science & Applications 15.6 (2024).

[7] A. Sahbi, F. Jaidi, and A. Bouhoula, "Artificial Intelligence for SDN Security: Analysis, Challenges and Approach Proposal," in 2022 15th International Conference on Security of Information and Networks (SIN), IEEE, 2022.

[8] A. Sahbi, F. Jaidi, and A. Bouhoula, "Machine Learning Algorithms for Enhancing Intrusion Detection Within SDN/NFV," in 2023 International Wireless Communications and Mobile Computing (IWCMC), IEEE, 2023

[9] Priyadarsini, Madhukrishna, and Padmalochan Bera. "Software defined networking architecture, traffic management, security, and placement: A survey." Computer Networks 192 (2021): 108047.

[10] Abdelrahman, Abdallah Mustafa, et al. "Software-defined networking security for private data center networks and clouds: vulnerabilities, attacks, countermeasures, and solutions." International Journal of Communication Systems 34.4 (2021): e4706.

[11] Domínguez-Dorado, Manuel, et al. "Detection and mitigation of security threats using virtualized network functions in software-defined networks." Applied Sciences 14.1 (2023): 374.

[12] Abd-Allah, Ahmed Gaber Abu, et al. "A Comprehensive Survey on Security Challenges and Solutions in Software-Defined Network." JOURNAL OF COMPUTER SCIENCE (ISSN NO: 1549-3636) 18.04 (2025).

[13] Kenner, Andrea, and Oluwaseyi Oladele. "Software-defined networking (sdn) and network function virtualization (nfv) in telecommunication: A computer science perspective." (2024).

[14] Ashodia, Namita, and Kishan Makadiya. "Detection and mitigation of ddos attack in software defined networking: A survey." 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). IEEE, 2022.

[15] Ahmad, Shakir Salman, and Mohammed I. Habelamateen. "Application of Artificial Intelligence and Machine Learning in Software Defined Networks." Journal of Smart Internet of Things 2023.1 (2023): 14-22.

[16] Hasneen, Jehan, and Kazi Masum Sadique. "A survey on 5G architecture and security scopes in SDN and NFV." Applied Information Processing Systems: Proceedings of ICCET 2021. Singapore: Springer Singapore, 2021. 447-460.

[17] Rauf, Bilal, et al. "Application threats to exploit northbound interface vulnerabilities in software defined networks." ACM Computing Surveys (CSUR) 54.6 (2021): 1-36.

[18] Melkov, Dmitrij, and Sarunas Paulikas. "Security benefits and drawbacks of software-defined networking." 2021 IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream). IEEE, 2021.

[19] Zahran, Bilal, et al. "Security and Privacy Issues in Network Function Virtualization: A Review from Architectural Perspective." International Journal of Advanced Computer Science & Applications 15.6 (2024).

[20] Razvan, Florea, and Craus Mitica. "Enhancing network security through integration of game theory in software-defined networking framework." International Journal of Information Security 24.3 (2025): 100.

[21] Babbar, Himanshi, et al. "Role of network slicing in software defined networking for 5G: Use cases and future directions." IEEE Wireless Communications 29.1 (2022): 112-118.

[22] Anand, Nemalikanti, et al. "Securing software defined networks: A comprehensive analysis of approaches, applications, and future strategies against DoS attacks." IEEE Access (2024).

[23] Sahbi, Amina, Faouzi Jaidi, and Adel Bouhoula. "Towards a reliable and smart approach for detecting and resolving security violations within SDWN." 2023 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2023.

[24] Sahbi, Amina, Faouzi Jaidi, and Adel Bouhoula. "An intelligent solution to detect security policy violations in sdn data plane." SYMBOLIC COMPUTATION IN SOFTWARE SCIENCE (2021): 46.

[25] Taheri, Roya, Habib Ahmed, and Engin Arslan. "Deep learning for the security of software-defined networks: a review." Cluster Computing 26.5 (2023): 3089-3112.

[26] Aziz, Israa T., and Ihsan H. Abdulqadder. "An overview on SDN and NFV security orchestration in cloud network environment." Cihan University-Erbil Scientific Journal 5.1 (2021): 20-27.

[27] Pliekhova, Ganna, et al. "Software-configured network architecture vulnerabilities." AIP Conference Proceedings. Vol. 3238. No. 1. AIP Publishing LLC, 2025.

[28] Scott-Hayward, Sandra. "Security-focused Networks of the Future." Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security. 2021.

[29] Varma, Koppada Durgaprasad, et al. "Software-defined network and network function virtualization: a comparative study." Software-Defined Networking for Future Internet Technology. Apple Academic Press, 2021. 255-276.

[30] Gaur, Kuntal, et al. "Software defined networking: a review on architecture, security and applications." IOP Conference Series: Materials Science and Engineering. Vol. 1099. No. 1. IOP Publishing, 2021.

[31] Mustafa, Zaid, et al. "Intrusion detection systems for software-defined networks: a comprehensive study on machine learning-based techniques." Cluster Computing 27.7 (2024): 9635-9661.

[32] Bilal, Noura, Shavan Askar, and Karwan Muheden. "Challenges and Outcomes of Combining Machine Learning with Software-Defined Networking for Network Security and management Purpose: A Review." The Indonesian Journal of Computer Science 13.2 (2024).

[33] Aditya, T., et al. "Nfv and sdn: A new era of network agility and flexibility." Int. J. Adv. Res. Sci. Commun. Technol (2023): 482-493.

[34] Sanghavi, Preet, Sheel Sanghvi, and Ramchandra S. Mangrulkar. "Software-defined networks a brief overview and survey of services." Software Defined Networking for Ad Hoc Networks (2022): 1-31.

[35] Snehi, Manish, and Abhinav Bhandari. "An SDN/NFV based intelligent fog architecture for DDoS defense in cyber physical systems." 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE, 2021.

[36] Soylu, Mustafa, et al. "NFV-Guard: Mitigating flow table-overflow attacks in SDN using NFV." 2021 IEEE 7th International Conference on Network Softwarization (NetSoft). IEEE, 2021.

[37] Rankothge, W. H., et al. "Network traffic prediction for a software defined network based virtualized network functions platform." 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE). Vol. 6. IEEE, 2021.

[38] Piakaray, Divya, et al. "A survey on the utilization of artificial intelligence and machine learning in the field of network functions virtualization and software defined networking." 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, 2023.

[39] Buzhin, I., et al. "Integrity, Resilience and Security of 5G Transport Networks Based on SDN/NFV Technologies." International Conference on Distributed Computer and Communication Networks. Cham: Springer International Publishing, 2021.

[40] Jimenez, Maria B., et al. "A survey of the main security issues and solutions for the SDN architecture." Ieee Access 9 (2021): 122016-122038.

[41] Shobowale, K. O., et al. "Latest advances on security architecture for 5G technology and services." International Journal of Software Engineering and Computer Systems 9.1 (2023): 27-38.

[42] Pattaranantakul, Montida, Chalee Vorakulpipat, and Takeshi Takahashi. "Service function chaining security survey: Addressing security challenges and threats." Computer Networks 221 (2023): 109484.

[43] Fan, Cong, et al. "Detection of DDoS attacks in software defined networking using entropy." Applied Sciences 12.1 (2021): 370.

[44] Nadeem, Muhammad Waqas, et al. "Toward Secure Software-Defined Networks Using Machine Learning: A Review, Research Challenges, and Future Directions." Computer Systems Science & Engineering 47.2 (2023).

[45] Alnaim, Abdulrahman K. "Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security." International Journal of Information Security (2024): 1-21.

[46] Allaw, Zeina, Ola Zein, and Abdel-Mehsen Ahmad. "Cross-Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework." Sensors 25.11 (2025): 3335.

[47] Heidarikohol, Niloofar, Shuvalaxmi Dass, and Akbar Siami Namin. "Evolutionary Defense: Advancing Moving Target Strategies with Bio-Inspired Reinforcement Learning to Secure Misconfigured Software Applications." arXiv preprint arXiv:2504.09465 (2025).

[48] García, Carlos Rubio, et al. "Enhancing the security of software defined networks via quantum key distribution and post-quantum cryptography." International Symposium on Distributed Computing and Artificial Intelligence. Cham: Springer Nature Switzerland, 2023.