Evolving Security for 6G: Integrating Software-Defined Networking and Network Function Virtualization into Next-Generation Architectures

JAADOUNI Hatim[1], CHAOUI Habiba[2], SAADI Chaimae[3]
Science and Engineering Laboratory of the National School of Applied Sciences of Kénitra, Ibn Tofail, Kenitra, Morroco[1, 2]
Laboratory of Systems Analysis, Information Processing and Industrial Management (LASTIMI) of EST Salé. Sale, Morroco[3]

***Abstract*—As technology continues to advance, the emergence of 6G networks is imminent, promising unprecedented levels of connectivity and innovation. A critical aspect of designing the security architecture for 6G networks revolves around the utilization of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies. By harnessing the capabilities of SDN and NFV, the security infrastructure of 6G networks stands to gain significant advantages in terms of flexibility, scalability, and agility. SDN facilitates the decoupling of the network control plane from the data plane, enabling centralized management and control of network resources. This article examines the synergistic relationship between SDN and NFV in enhancing the resilience and adaptability of 6G security architectures, offering insights into key challenges, emerging trends, and future directions in securing the next generation of wireless networks.**

Keywords*—*6G Network; network function virtualization; software defined network; security; architecture

I. Introduction

With the advancement of technology, the development of 6G networks is already on the horizon [1]. One of the key considerations in designing the security architecture for 6G is the use of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies. By leveraging SDN and NFV, the security architecture of 6G can benefit from enhanced flexibility, scalability, and agility. SDN enables the separation of the network control plane from the data plane, allowing for centralized management and control of network resources [2]. This centralized management and control can greatly improve the security of the network by enabling real-time threat detection and response, as well as efficient provisioning of security services such as firewalls, intrusion detection systems, and virtual private networks [3]. NFV, on the other hand, virtualizes network functions such as firewalls and encryption, allowing them to be deployed and scaled more easily [4]. This virtualization of network functions enables dynamic allocation of security resources based on the specific needs and demands of the network, ensuring that resources are utilized efficiently. In addition to flexibility and scalability, SDN and NFV can also enhance the security architecture of 6G by providing comprehensive visibility and control over network traffic [5]. This increased visibility enables security administrators to monitor and analyze network traffic in real-time, identify potential threats, and apply appropriate security measures.

In addition to the advancements in technology, the development of 6G networks represents a significant leap forward in wireless communications. As we approach the era of 6G, it becomes increasingly imperative to reevaluate and enhance the security architecture of these networks to mitigate emerging cyber threats and ensure the integrity of critical network resources.

The primary research problem addressed in this study is the lack of a comprehensive and flexible security architecture for 6G networks that can effectively mitigate emerging cyber threats while ensuring the integrity and reliability of network resources.

The objectives of this research are to first investigate the integration of SDN and NFV technologies into the 6G security architecture, second is to identify and address the security challenges specific to 6G networks and last is to develop strategies for the dynamic allocation and efficient utilization of security resources using SDN and NFV.

The significance of this research lies in its potential to revolutionize the security architecture of 6G networks. By leveraging SDN and NFV, this study aims to provide a flexible, scalable, and agile security framework that can adapt to the evolving landscape of cyber threats. This research will contribute to the development of more secure 6G networks, ensuring the protection of critical network resources and the overall reliability of next-generation wireless communications.

The work presented in this paper will be organized as follows: Section II will present why we will need to level up the level of the 6G security network. Section III is mainly to understand the concept of SDN and NFV. Section IV discusses briefly the integration compatibility of SDN/NFV to the 6G architecture. Section V will discuss the proposed 6G architecture including NFV and SDN and its details. Section VI and VII gives detail about the integrating SDN and NFV and provides discussion respectively. Section VIII and IX concludes the work and gives future scopes and areas for potential directions.

II. Related Work

In recent years, substantial research has focused on enhancing network security and efficiency using Software-Defined Networking (SDN) and Network Function Virtualization (NFV), especially with the anticipated arrival of

6G networks. Here, we review relevant studies that inform and position our research within the broader academic and industry context.

Siriwardhana et al. [6] emphasized the potential of AI in 6G security, addressing opportunities and challenges in integrating AI with SDN and NFV to enhance network protection mechanisms. Zhu et al. [7] provided a comprehensive analysis and performance evaluation of SDN controllers, crucial for understanding how SDN can be optimized for security in 6G networks. Akyildiz et al. [8] discussed the foundational concepts of wireless SDNs and NFV, laying the groundwork for subsequent innovations in 5G and beyond.

Du et al. [3] explored machine learning techniques to enhance bandwidth, massive access, and ultra-reliable low latency in 6G networks, which is relevant for SDN/NFV-based security improvements. Chkirbene et al. [9] introduced a dynamic intrusion detection and classification system using feature selection, highlighting advanced threat detection approaches applicable to SDN/NFV. Miranda et al. [10] proposed a collaborative security framework for software-defined wireless sensor networks, stressing the importance of cross-sector cooperation in addressing multifaceted security challenges.

Barakabitze and Walshe [11] discussed SDN and NFV for Quality of Experience (QoE)-driven multimedia services, providing insights into the integration process and its benefits for 6G networks. Zhang et al. [12] evaluated software switches' performance in SDN-NFV integration, offering valuable information on selecting appropriate switches for various tasks and understanding performance trade-offs.

This review of related works illustrates the significant efforts already made towards improving network security and efficiency through SDN and NFV. Our research contributes to this ongoing conversation by specifically focusing on the integration of these technologies within the 6G framework, addressing both the opportunities and the challenges posed by this next-generation network.

III. The Need for Enhanced Security in 6G Networks

6G networks are expected to introduce unprecedented levels of connectivity, enabling billions of devices to communicate seamlessly. While this connectivity offers tremendous opportunities for innovation, it also introduces new security risks [13]. Here are some of the security risks that we can face:

A. Quantum-Resistant Encryption

With the advent of quantum computing, traditional encryption methods become susceptible to brute-force attacks. Implementing quantum-resistant encryption algorithms [14] is crucial to protect sensitive data transmitted over 6G networks from potential future threats posed by quantum computing.

B. Dynamic Threat Detection and Response

Given the dynamic nature of cyber threats, 6G networks require advanced threat detection mechanisms capable of identifying and mitigating evolving threats in real-time [15]. Machine learning algorithms and AI-driven security solutions can play a pivotal role in continuously monitoring network traffic patterns and behavior anomalies to detect potential security breaches promptly.

C. Collaborative Security Frameworks

Enhancing security in 6G networks necessitates a collaborative approach involving network operators, device manufacturers, regulatory bodies, and cybersecurity experts [16]. Establishing comprehensive security standards, sharing threat intelligence, and fostering cross-sector cooperation are essential to address the multifaceted security challenges posed by 6G networks effectively.

IV. Understanding Software-Defined Networking (SDN) and Network Function Virtualization (NFV)

SDN and NFV are two key technologies that have emerged as critical enablers of next-generation networking architectures.

A. SDN

Software-Defined Networking (SDN) is a paradigm shift in network architecture that separates the control plane from the data plane, enabling centralized control and programmability of network devices through software-based controllers. In traditional networking, the control plane, responsible for making routing decisions, is tightly integrated with the data plane, which forwards traffic [17]. However, in SDN, the control plane is abstracted and centralized, allowing network administrators to manage and configure the network dynamically through software applications rather than relying on manual configuration of individual devices [18]. This separation of control and data planes enhances network agility, scalability, and flexibility, enabling organizations to adapt their networks quickly to changing traffic patterns and application requirements. SDN also facilitates automation, simplifying network management tasks and reducing operational overheads [19]. Overall, SDN revolutionizes network management by providing a more flexible, efficient, and programmable approach to configuring and controlling network infrastructure. The framework and architecture of SDN is shown on Fig. 1.

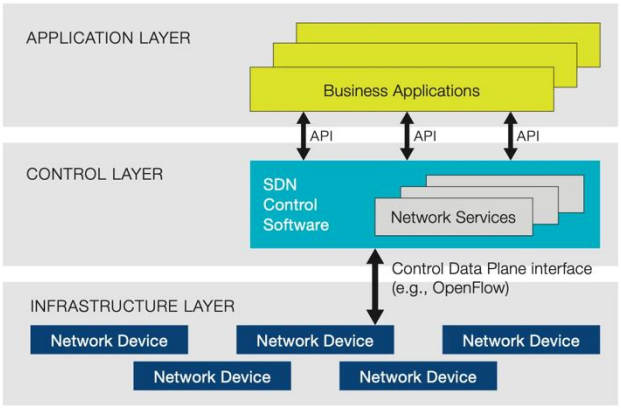

Fig. 1. SDN Architecture.

B. NFV

Network Function Virtualization (NFV) is a technology paradigm that aims to virtualize and consolidate traditional

network functions, such as firewalls, load balancers, and intrusion detection systems, into software-based instances that can run on standard servers, virtual machines, or cloud infrastructure [20]. NFV seeks to abstract network functions from proprietary hardware appliances and deploy them as virtualized software instances, decoupling network functions from dedicated hardware. By doing so, NFV enables greater flexibility, agility, and scalability in deploying and managing network services. It allows service providers and enterprises to leverage virtualization technologies to dynamically instantiate, scale, and orchestrate network functions based on changing demand and traffic patterns. NFV also offers significant cost savings by reducing the need for specialized hardware appliances and simplifying network infrastructure management [21]. Overall, NFV represents a fundamental shift in how network services are deployed, managed, and scaled, providing organizations with greater efficiency and innovation in delivering network services. The architecture of NFV is shown on Fig. 2.

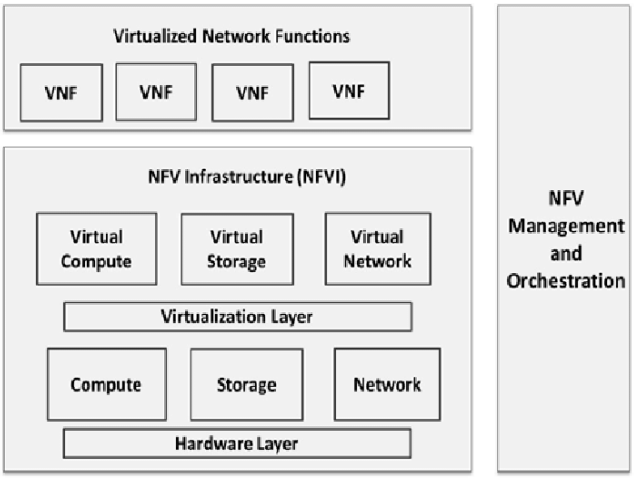

Fig. 2. NFV Architecture [22].

SDN provides the centralized control and programmability necessary to dynamically configure and optimize network resources, while NFV virtualizes and consolidates network functions, enabling them to run as software-based instances on standard hardware. By combining SDN and NFV, organizations can achieve unprecedented levels of agility, scalability, and efficiency in delivering network services. SDN's centralized control enables dynamic orchestration and management of NFV-based network functions, while NFV's virtualized network functions can leverage SDN's programmability to adapt and respond to changing network conditions [23]. Together, SDN and NFV form a powerful combination that transforms traditional networking paradigms, offering greater flexibility, automation, and innovation in network deployment and management.

V. SDN AND NFV COMPABILITY FOR 6G TECHNOLOGY

In pursuit of merging Software-Defined Networking (SDN) and Network Function Virtualization (NFV), Barakabitze A. & Walshe R. introduced a Software-Defined Networking Virtualization (SDNV) architecture, offering an extensive insight into the integration process [11]. They proposed two potential designs: NFV under a controller (NFV-C) and NFV beside the controller (NFV-AC), while discussing the advantages of amalgamating SDN and NFV.

Meanwhile, Zhang et al. conducted a study on the integration of SDN-NFV by evaluating software switches' performance across four hypothetical scenarios [24]. Their findings revealed that no single software switch excelled in all situations, emphasizing the importance of selecting the most suitable switch for each task. They also identified potential performance issues in software switches, contributing to a better understanding of design compromises. Notably, the article highlighting the merger's operational convenience stands out among related works on merging. Additionally, a comparison between SDN-NFV and SDN alone is provided [25].

VI. INTEGRATING SDN AND NFV INTO 6G ARCHITECTURE

Integrating Software-Defined Networking (SDN) and Network Function Virtualization (NFV) into 6G security architectures represents a sophisticated and comprehensive approach to addressing the evolving cyber threat landscape while maximizing the potential of next-generation networks. In such architectures, SDN serves as the backbone for centralized control and management, providing a unified platform for orchestrating security policies and resources across the entire network infrastructure as shown in Fig. 3. Through SDN's programmable interface, security administrators can dynamically configure and enforce security measures such as access control, traffic segmentation, and quality of service (QoS) prioritization to adapt to changing network conditions and security requirements in real-time.

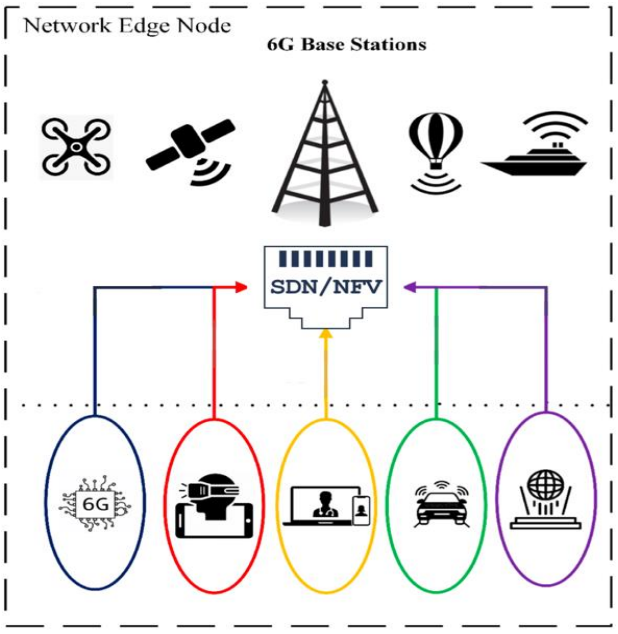

Fig. 3. The placement of SDN / NFV in 6G architecture.

In tandem with SDN, NFV plays a pivotal role in virtualizing and consolidating a diverse range of security functions into software-based instances that can be dynamically instantiated, scaled, and orchestrated as needed. This virtualization of security functions allows for greater

flexibility and agility in deploying and managing security services within 6G networks. For instance, here are some services that can all be provisioned as virtual network functions (VNFs) that will jump up the security level of communication between sensors and base stations:

- Virtualized Firewalls: NFV enables the deployment of virtualized firewall instances on-demand, managed and orchestrated by the SDN controller. These firewalls can inspect and filter network traffic, enforce security policies, and protect against unauthorized access and malicious activities.
- Intrusion Detection/Prevention Systems (IDPS): NFV allows for the virtualization of IDPS functions, which can be instantiated as virtual network functions (VNFs) on SDN controllers. These IDPS VNFs analyze network traffic for suspicious behavior and patterns, detecting and preventing potential security breaches in real-time.
- Virtual Private Network (VPN) Gateways: NFV enables the creation of virtualized VPN gateways that can be centrally managed by the SDN controller. These VPN gateways provide secure communication channels for remote users or branch offices, encrypting data traffic over the 6G network to ensure confidentiality and integrity.
- Security Analytics: NFV facilitates the deployment of security analytics functions as virtualized instances on SDN controllers. These analytics functions analyze network telemetry data, logs, and security events to identify and correlate potential security threats, providing actionable insights for threat detection and response.
- Encryption/Decryption Services: NFV enables the virtualization of encryption/decryption services, which can be deployed as VNFs on SDN controllers to encrypt sensitive data transmissions over the 6G network. These services ensure end-to-end encryption of data traffic, protecting it from unauthorized access and interception.
- Virtualized Network Access Control (NAC): NFV allows for the deployment of virtualized NAC functions on SDN controllers, enabling centralized management and enforcement of access control policies. These virtualized NAC functions authenticate and authorize devices and users accessing the network, ensuring compliance with security policies and preventing unauthorized access.

Moreover, the integration of SDN and NFV both as their working theory is shown in Fig. 4 enables advanced security orchestration capabilities, where security policies and functions can be dynamically coordinated and adapted in response to detected threats or changing network conditions. Through automated workflows and policy-driven mechanisms, security orchestration streamlines incident response processes, accelerates threat mitigation, and optimizes resource allocation to effectively counteract cyber threats in real-time.

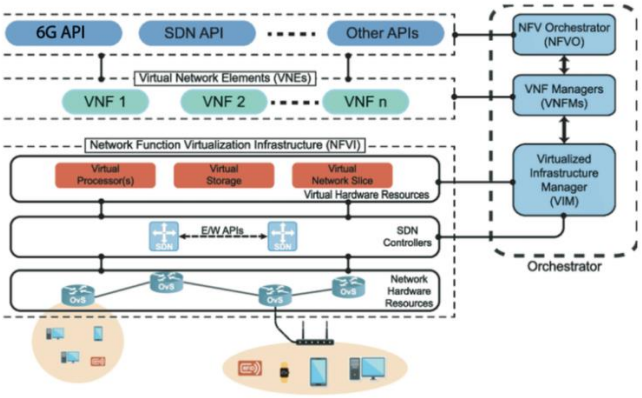

Fig. 4. The working theory of SDN / NFV between sensors and base towers.

Furthermore, the incorporation of artificial intelligence (AI) and machine learning (ML) technologies into SDN-NFV-based security architectures enhances threat detection, anomaly identification, and predictive analysis capabilities. By leveraging AI-driven security analytics, 6G networks can proactively detect and mitigate security threats before they escalate, thereby bolstering the overall resilience and reliability of the network infrastructure.

In summary, the integration of SDN and NFV into 6G security architectures represents a sophisticated and multi-faceted approach to cybersecurity, combining centralized control, virtualized network functions, dynamic orchestration, and AI-driven analytics to create a robust and adaptive security framework capable of safeguarding next-generation networks against a myriad of cyber threats.

VII. Results and Discussion

The integration of SDN and NFV into 6G security architectures demonstrates significant potential for enhancing network flexibility, scalability, and operational efficiency. Our findings indicate that these technologies can provide a robust framework capable of adapting to the evolving cyber threat landscape.

Enhanced Security Capabilities:

- Dynamic Threat Detection and Response: Leveraging AI and machine learning, SDN and NFV enable real-time monitoring and response to cyber threats. This dynamic approach ensures that security measures can adapt to new and emerging threats promptly.
- Quantum-Resistant Encryption: As quantum computing evolves, traditional encryption methods become vulnerable. Implementing quantum-resistant algorithms within the SDN/NFV framework is crucial for protecting sensitive data in 6G networks.

Operational Efficiency and Flexibility:

- Centralized Control and Management: SDN facilitates centralized management of network resources, enhancing the ability to implement and enforce security policies across the network. This centralized approach simplifies network management and reduces operational overhead.

- Virtualization of Security Functions: NFV allows for the virtualization of essential security functions, such as firewalls and intrusion detection systems. This flexibility enables the dynamic allocation of security resources based on real-time network demands, improving overall resource utilization.

Challenges and Future Directions:

- Interoperability: Ensuring seamless interoperability between SDN and NFV components remains a critical challenge. Future research should focus on developing standardized protocols and frameworks to enhance compatibility.
- Security Concerns: Addressing inherent security challenges in SDN/NFV deployments is essential. Robust mechanisms for threat detection and mitigation, compliance with regulatory standards, and the incorporation of advanced encryption methods are necessary to safeguard network integrity.
- Scalability: As 6G networks scale, ensuring that SDN and NFV solutions can handle increased traffic and a higher number of connected devices is crucial. Optimizing network resource allocation and performance under varying conditions is a key area for further research.

Our study underscores the necessity of advancing SDN-NFV integration techniques to fully realize these benefits, highlighting the importance of continuous research and development efforts. By refining technical aspects and fostering collaboration among academia, industry, and policymakers, we can drive the evolution of network architectures towards more intelligent, responsive, and secure configurations.

VIII. Conclusion

In conclusion, this research has highlighted the significant potential of integrating Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) to revolutionize modern network infrastructures. By decoupling network functions from hardware and enabling programmable network control, SDN-NFV integration offers unparalleled benefits in terms of flexibility, scalability, and operational efficiency.

The findings of this study underscore the necessity of advancing SDN-NFV integration techniques to fully realize these benefits. Key improvements include enhancing the interoperability between SDN and NFV components, optimizing network resource allocation, and ensuring robust performance under varying network conditions.

Moreover, the study has identified critical security challenges inherent to SDN-NFV deployments. Addressing these challenges through innovative threat detection and mitigation strategies is paramount to safeguarding the integrity and reliability of future network systems. The research also emphasizes the importance of adhering to regulatory standards to maintain compliance and foster trust among users and stakeholders.

In essence, the successful deployment and adoption of SDN-NFV technology hinge on continuous research and development efforts. This includes refining technical aspects and fostering collaboration among academia, industry, and policymakers. By doing so, we can drive the evolution of network architectures towards more intelligent, responsive, and secure configurations, ultimately paving the way for next-generation networking solutions.

IX. Future Scope

The future scope of this research article encompasses several key areas of exploration and development. Firstly, there is a need for continued refinement and optimization of SDN-NFV integration techniques to enhance network efficiency, flexibility, and scalability. Research should focus on developing advanced algorithms and protocols that improve the coordination between SDN controllers and NFV orchestrators, thereby achieving seamless and efficient network management.

Additionally, research efforts should concentrate on addressing security concerns and vulnerabilities associated with SDN-NFV deployments. This includes developing robust mechanisms for threat detection and mitigation, as well as ensuring compliance with regulatory standards. Enhancing the security of SDN-NFV environments is critical to protect against evolving cyber threats and maintain the trust of users and stakeholders.

Furthermore, exploring novel applications of SDN-NFV technology in emerging fields such as edge computing, the Internet of Things (IoT), and 6G networks holds great promise. By leveraging the capabilities of SDN-NFV, organizations can unlock new opportunities for innovation and digital transformation. Research in these areas should aim to design and implement use cases that demonstrate the practical benefits and scalability of SDN-NFV solutions in real-world scenarios.

Collaboration between academia, industry, and policymakers will be crucial for advancing research in this field and driving the adoption of SDN-NFV technology in real-world deployments. By fostering interdisciplinary partnerships and knowledge exchange, we can collectively contribute to the continued evolution of network architectures and the realization of the full potential of SDN-NFV technology.

In summary, future research should aim to:

- Refine and optimize SDN-NFV integration techniques.
- Address security concerns and ensure regulatory compliance.
- Explore applications in edge computing, IoT, and 5G networks.
- Foster collaboration between academia, industry, and policymakers.

By focusing on these areas, we can enhance the capabilities and adoption of SDN-NFV technology, driving innovation and efficiency in network management and operations.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to SAADI Chaimae & CHAOUI Habiba for their guidance and support throughout this research endeavor. Special thanks to University Ibn Tofail for providing resources. Lastly, I appreciate the encouragement from my friends and family.

REFERENCES

[1] Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 616-621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503. keywords: {6G mobile communication;Privacy;Intelligent networks;Automation;5G mobile communication;Security;Artificial intelligence;6G;6G Security;Artificial Intelligence;Machine Learning;Intelligent Security}.

[2] Liehuang Zhu, Md M. Karim, Kashif Sharif, Chang Xu, Fan Li, Xiaojiang Du, and Mohsen Guizani. 2020. SDN Controllers: A Comprehensive Analysis and Performance Evaluation Study. ACM Comput. Surv. 53, 6, Article 133 (November 2021), 40 pages. https://doi.org/10.1145/3421764.

[3] Du, Jun & Jiang, Chunxiao & Wang, Jian & Ren, Yong & Debbah, mérouane. (2020). Machine Learning for 6G Wireless Networks: Carry-Forward-Enhanced Bandwidth, Massive Access, and Ultrareliable/Low Latency. IEEE Vehicular Technology Magazine. PP. 10.1109/MVT.2020.3019650.

[4] Ian F. Akyildiz, Shih-Chun Lin, Pu Wang, Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation, Computer Networks,Volume 93, Part 1,2015, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2015.10.013.

[5] Huang, Huiyue & Yang, Lei & Wang, Yuanbin & Xu, Xun & Lu, Yuqian. (2021). Digital Twin-driven online anomaly detection for an automation system based on edge intelligence. Journal of Manufacturing Systems. 59. 138-150. 10.1016/j.jmsy.2021.02.010.

[6] Siriwardhana, Yushan & Porambage, Pawani & Liyanage, Madhusanka & Ylianttila, Mika. (2021). AI and 6G Security: Opportunities and Challenges. 10.1109/EuCNC/6GSummit51104.2021.9482503.

[7] Zhu, Liehuang & Karim, Md Monjurul & Sharif, Kashif & Xu, Chang & Li, Fan & Du, Xiaojiang & Guizani, Mohsen. (2020). SDN Controllers: A Comprehensive Analysis and Performance Evaluation Study. ACM Computing Surveys. 53. 1-40. 10.1145/3421764.

[8] Ian F. Akyildiz, Shih-Chun Lin, and Pu Wang. 2015. Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems. Comput. Netw. 93, P1 (December 2015), 66–79. https://doi.org/10.1016/j.comnet.2015.10.013.

[9] Chkirbene, Zina & Erbad, Aiman & Ridha, Hamila & Mohamed, Amr & Guizani, Mohsen & Hamdi, Mounir. (2020). TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2994931.

[10] Miranda, Christian & Kaddoum, Georges & Bou-Harb, Elias & Garg, Sahil & Kaur, Kuljeet. (2020). A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security. PP. 10.1109/TIFS.2020.2973875.

[11] Alcardo Alex Barakabitze, Ray Walshe, SDN and NFV for QoE-driven multimedia services delivery: The road towards 6G and beyond networks,Computer Networks, Volume 214,2022,109133,ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2022.109133.

[12] Rashid, Salar & Alkababji, Ahmed & Khidhir, Abdulsattar. (2023). Performance evaluation of software-defined networking controllers in wired and wireless networks. TELKOMNIKA (Telecommunication Computing Electronics and Control). 21. 49-59. 10.12928/TELKOMNIKA.v21i1.23468.

[13] M. Mitev, A. Chorti, H. V. Poor and G. P. Fettweis, "What Physical Layer Security Can Do for 6G Security," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 375-388, 2023, doi: 10.1109/OJVT.2023.3245071. (fisical).

[14] Diksha Chawla, Pawan Singh Mehra, A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions, Internet of Things, Volume 24, 2023, ISSN 2542-6605,https://doi.org/10.1016/j.iot.2023.100950.

[15] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani and M. Hamdi, "TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection," in IEEE Access, vol. 8, pp. 95864-95877, 2020, doi: 10.1109/ACCESS.2020.2994931.

[16] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg and K. Kaur, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2602-2615, 2020, doi: 10.1109/TIFS.2020.2973875.

[17] Juan Camilo Correa Chica, Jenny Cuatindioy Imbachi, Juan Felipe Botero Vega,Security in SDN: A comprehensive survey, Journal of Network and Computer Applications, Volume 159, 2020, 102595, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102595.

[18] Hatim, J., Chaimae, S., Habiba, C. (2022). Improved IOT/SDN Architecture with the Concept of NFV. In: Motahhir, S., Bossoufi, B. (eds) Digital Technologies and Applications. ICDTA 2022. Lecture Notes in Networks and Systems, vol 454. Springer, Cham. https://doi.org/10.1007/978-3-031-01942-5_29.

[19] Noe M. Yungaicela-Naula, Cesar Vargas-Rosales, Jesús Arturo Pérez-Díaz, Mahdi Zareei,Towards security automation in Software Defined Networks,Computer Communications,Volume 183,2022,Pages 64-82,ISSN 0140-3664,https://doi.org/10.1016/j.comcom.2021.11.014.

[20] J. Hatim, S. Chaimae and C. Habiba, "SDN/NFV Security Challenges and Proposed Architecture," 2023 7th IEEE Congress on Information Science and Technology (CiSt), Agadir - Essaouira, Morocco, 2023, pp. 145-149, doi: 10.1109/CiSt56084.2023.10409955. keywords: {Information science; Organizations;Network function virtualization;Security;Software defined networking; Resilience; sdn;nfv;security}.

[21] Issam Abdeldjalil Ikhelef. Optimization of VNF placement and chaining according to NFV/SDN paradigms. Performance [cs.PF]. Université Paris-Nord - Paris XIII, 2024. English. ⟨NNT : 2024PA131002⟩. ⟨tel-04509177⟩.

[22] Bh, Deval & Samaka, Mohammed & Erbad, Aiman & Jain, Raj & Gupta, Lav & Chan, H Anthony. (2017). Optimal Virtual Network Function Placement in Multi-Cloud Service Function Chaining Architecture. Computer Communications. 102. 10.1016/j.comcom.2017.02.011.

[23] Alshammari, N., Shahzadi, S., Alanazi, S. A., Naseem, S., Anwar, M., Alruwaili, M., Abid, M. R., Alruwaili, O., Alsayat, A., & Ahmad, F. (2024). Security monitoring and management for the network services in the orchestration of SDN-NFV environment using machine learning techniques. Computer Systems Science and Engineering, 48(2), 363-394. https://doi.org/10.32604/csse.2023.040721.

[24] J. Zhang, Z. Wang, N. Ma, T. Huang and Y. Liu, "Enabling Efficient Service Function Chaining by Integrating NFV and SDN: Architecture, Challenges and Opportunities," in *IEEE Network*, vol. 32, no. 6, pp. 152-159, November/December 2018, doi: 10.1109/MNET.2018.1700467.

[25] Jaadouni, Hatim & Chaimae, Saadi & Chaoui, Habiba. (2022). SDN/NFV architectures for edge-cloud oriented IoT. ITM Web of Conferences. 46. 02004. 10.1051/itmconf/20224602004.