

PAPER

IoT Challenges and Issues: A Comprehensive Review of Software Defined Networking and Network Function Virtualization Solutions

Manare Zerifi()
Abdellatif Ezzouhairi,
Abdelhak Boulaalam,
Mohamed Baghrous

National School of Applied
Sciences, Sidi Mohammed
ben Abdellah University,
Fez, Morocco

manare.zerifi@usmba.ac.ma

ABSTRACT

The idea behind the Internet of Things (IoT) is to connect everything, including laptops, smartphones, sensors, and other devices, to the Internet. To build an autonomous environment without human intervention. This novel network was used in several industries, including smart homes, smart cities, healthcare, etc. For this reason, IoT networks are growing in infrastructure. As a result, the administration of this vast array of linked devices and produced data becomes more complicated. Thus, a new elastic mechanism is required for this dynamic and rapid evolution in configuration, control, management, etc. Network Function Virtualization (NFV) and Software Defined Networking (SDN) have become essential points in scientific research to overcome IoT challenges such as security, heterogeneity, energy efficiency, interoperability, and more. These two approaches have proven their efficiency in adapting to dynamic and evolving networks. SDN reduces network latency by up to 30% and increases device scalability by 40%. At the same time, NFV optimizes resource allocation, achieving up to a 35% reduction in energy consumption and a 20% decrease in operational costs through virtualized infrastructure. In this review, we systematically analyze solutions designed for IoT systems by developing a state-of-the-art for NFV and SDN and thoroughly researching the various problems that IoT will face. Thus, we compare SDN- and NFV-based IoT solutions to overcome these challenges. Lastly, we will discuss the different obstacles that can lower the performance of SDN/NFV applications on the IoT. The contribution of this review lies in its systematic evaluation and comparison of current NFV and SDN approaches, providing valuable insights and paving the way for future research to enhance the integration and management of IoT systems.

KEYWORDS

Software Defined Networking (SDN), Internet of Things (IoT), Network Function Virtualization (NFV)

Zerifi, M., Ezzouhairi, A., Boulaalam, A., Baghrous, M. (2025). IoT Challenges and Issues: A Comprehensive Review of Software Defined Networking and Network Function Virtualization Solutions. *International Journal of Interactive Mobile Technologies (ijim)*, 19(3), pp. 209–226. <https://doi.org/10.3991/ijim.v19i03.49791>

Article submitted 2024-04-23. Revision uploaded 2024-10-29. Final acceptance 2024-10-29.

© 2025 by the authors of this article. Published under CC-BY.

1 INTRODUCTION

In the world, the global adoption of the Internet of Things (IoT) is expanding quickly every day. It enables billions of devices to connect. As a result, it is being utilized in many fields, such as industry, healthcare, agriculture, transport, and many others [1], [2], [3], [70]. Consequently, the most important objective of the IoT is to make life easier and facilitate processes in different fields. However, the vast amount of heterogeneous data generated by this evolution requires processing, storage, and computation. For this reason, managing this infrastructure is becoming more complicated. This calls for a new flexible mechanism adapted to the ever-changing nature of this smart network.

The proliferation of IoT applications requires the development of this network to find solutions to challenges such as confidentiality, reliability, interoperability, heterogeneity, energy efficiency, scalability, and so on [67], [69]. Unfortunately, these challenges can degrade the performance of the IoT in many areas.

However, traditional networking approaches often fail to meet these demands due to inherent limitations. Traditional networks lack the flexibility and programmability required to handle the dynamic and heterogeneous nature of IoT environments, leading to scalability, security, and interoperability constraints. Unlike traditional networks, Software Defined Networking (SDN's) programmability provides greater flexibility and adaptability to changing network demands, which is essential in IoT environments that need rapid responses to data flow adjustments. By decoupling the control and data planes, SDN centralizes control and allows dynamic adjustments to the network configuration, which is difficult to achieve in conventional networks.

Therefore, the problem is how to effectively oversee the quickly expanding IoT infrastructure while overcoming complex challenges such as confidentiality, reliability, and interoperability and ensuring optimal performance through SDN and network function virtualization (NFV) solutions.

However, here is the relevant role of SDN and NFV. Many researchers have studied these two concepts because of their importance.

Software-Defined Networking introduces the concepts of data plane and control plane separation to create a centralized network within a single entity. What's more, the network becomes easily programmable and manageable. In this way, it offers vendor independence, which is highly appreciated in the context of heterogeneous devices. What's more, virtualizing network functions aims to minimize costs by using virtual hardware in preference to physical hardware while retaining the network's elasticity, robustness, and flexibility. Unlike limited traditional networks, virtualization and programmability can bring flexibility and manageability to IoT by dissociating the hardware plane from the software plane, transforming decision-making and packet transfer to the control plane. Furthermore, this abstraction can be effective in addressing IoT challenges. As a result, network upgrades will be easy. On the one hand, SDN centralizes control functions via an SDN controller using OpenFlow as the essential protocol for data plane and control plane connections. On the other hand, NFV is known as an abstraction mechanism aimed at replacing hardware with virtual services to make the system robust, agile, and cost-effective [4].

The complementary properties of SDN and NFV, when combined, result in more powerful performance. NFV can improve SDN through the virtualization of the SDN controller in the cloud. In addition, SDN's programmable features enable it to implement the traffic selection decisions made by NFV [4]. An excellent job has

been done to combine the capabilities provided by SDN and NFV. To deal with IoT-related concerns. Therefore, it is necessary to thoroughly analyze various existing works to get a better understanding and propose a preliminary study for future researchers.

For this reason, the current literature based on SDN and NFV will be examined in depth in this survey to overcome the intensity of IoT challenges. Unlike previous surveys, our work uniquely emphasizes the synergistic potential of combining SDN and NFV in addressing these challenges, offering a comprehensive analysis that has not been extensively covered in prior studies. This is how the remainder of the document is structured. Section 2 provides general information and a state of the art of SDN and NFV. Section 3 highlights the most critical IoT challenges that will benefit from SDN and NFV features. Section 4 discusses related work and existing solutions provided by SDN. Section 5 presents the existing solutions offered by NFV. Section 6 details the different solutions provided by the combination and fusion of SDN and NFV to benefit from the complementary services provided by the two approaches. Section 7 ranks the most important challenges of SDN/NFV-based IoT. Finally, Section 8 concludes the paper and describes our next steps. In this section, we present a prioritized roadmap for future research, offering unique insights into unresolved challenges.

2 STATE OF ART OF SDN AND NFV

Software Defined Networking and NFV prove currently their efficiency in underestimating the extent of IoT challenges, especially in the security part. Let us make an in-depth study of these two mechanisms.

2.1 Software defined networking

The concept of SDN is well-known and relies on dividing the network's control from the data to allow for greater flexibility and programmability. SDN achieves enhanced flexibility and scalability by decoupling the control plane from the data plane, allowing dynamic and centralized management over network resources. SDN operates in this way by utilizing a centralized SDN controller that has a global perspective over the entire network. This centralized controller not only enables efficient resource allocation but also supports real-time adjustments to meet diverse network demands. As a result, it can manage the control and data components independently.

The data, control, and application planes are the three parts of the SDN architecture (see Figure 1). In this layered structure, each plane performs specific functions while interacting seamlessly through standardized APIs, ensuring a modular and interoperable framework. The data plane, which is linked to the control plane via the southbound APIs, oversees data flow. In particular, southbound APIs such as OpenFlow facilitate communication between SDN controllers and network devices, enabling programmable control over data flow. The network's brain is shown by the SDN controller. Similarly, the northbound APIs connect the SDN controller to the application plane [5], [6], [7]. Northbound APIs, on the other hand, allow applications and services to interact with the control plane, supporting advanced functionalities such as security, monitoring, and traffic management essential in IoT environments.

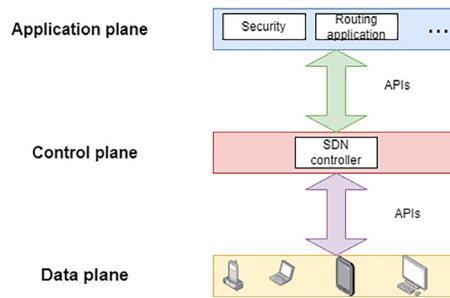


Fig. 1. SDN architecture

By examining these articles [20], [28], [30], we can identify numerous advantages of SDN. The most significant benefits include:

- **Dynamic management:** the split of the control functionalities towards the data part
- **Centralized management:** the use of an SDN controller
- **Automated configuration:** easy configuration of the network by the administrators

2.2 Comparison between SDN and traditional networks

The comparison table underscores the significant advantages of SDN over traditional networks. According to these studies [64], [65], [66], SDN offers superior scalability and enhanced security through centralized control and monitoring, along with other benefits detailed in Table 1.

Table 1. Contrast between SDN and traditional networks

Properties	SDN	Traditional Networks	Use Cases
Programmability	✓	✗	Smart grid networks: adaptive energy distribution and load balancing.
Easy configuration	✓	✗	Telecom networks: Dynamic network slicing for 5G.
Complex control	✗	✓	Network traffic management in a data center.
Manageability	✓	✗	Campus network: centralized management for multiple departments.
Centralization	✓	✗	Data centers: centralized traffic routing and resource allocation.
Cost-effective	✓	✗	Cloud networks: cost saving through efficient resource management.
Automation configuration	✓	✗	Automated warehousing: streamlined inventory tracking and control.

2.3 Network function virtualization

However, by substituting virtual resources for actual ones, NFV offers a significant way to lower the cost of physical resources. The common NFV architecture [6], as specified by the European Telecommunications Standards Institute (ETSI), is divided into three sections (see Figure 2): These components are:

- **Interface for network function virtualization (NFVI):** comprises a virtualization layer, a hardware interface, and an interface
- **Network function virtualization (VNF):** is a group of virtualized network functions
- **Network function virtualization management and orchestration (NFV MANO):** is in charge of the administration of the lifecycle of hardware and software services and manages the NFVI resources; capabilities, as well as other features that allow seamless integration among enterprise applications

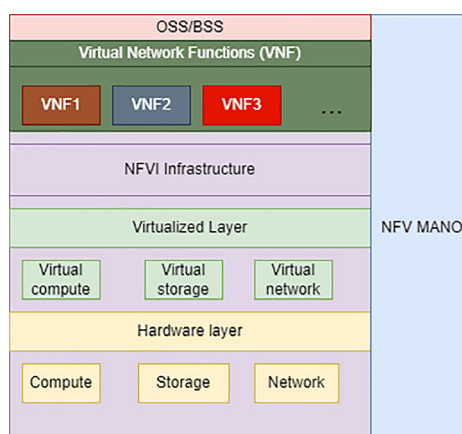


Fig. 2. NFV architecture

By studying these works [23], [11], [2], we can obtain numerous advantages of NFV. The most significant benefits are outlined below:

- **Easy network upgrade:** Network functions are deployed as software applications. For telecom providers, NFV enables them to deploy new services and updates rapidly, such as 5G upgrades, without needing to replace physical hardware.
- **Reduction in the cost of equipment:** The use of multiple functions in one physical server, such as in data centers allows for consolidation of hardware.
- **Reduction in the cost of maintenance:** It reduces the need for physical, maintenance. In cloud service providers, NFV minimizes on-site maintenance needs.
- **Reduction in the space of physical equipment:** Running of numerous functions in one single physical such as in smart city infrastructure when NFV enables the deployment of virtualized network functions in smaller, space-constrained environments.

3 THE MOST CRITICAL IOT CHALLENGES

The evolution of IoT applications in numerous fields poses different issues such as scalability, security, reliability, authenticity, interoperability, massive data, energy efficiency, and much more. That can degrade the potential of its performance in several fields. Specific IoT applications facing these challenges include smart cities, healthcare IoT, and industrial IoT, each of which encounters unique issues tied to scalability, data privacy, and energy consumption. We will analyze the existing works that study IoT challenges in more detail (refer to Table 2).

To provide practical relevance, Table 2 includes specific case studies for each challenge area. For example, in healthcare IoT, scalability issues arise with the rapid expansion of connected devices in hospitals, where traditional networks struggle

to support the high device density needed for patient monitoring and data sharing. Similarly, in smart city infrastructure, security challenges are critical due to the potential for cyber-attacks on traffic systems and surveillance networks.

Table 2. IoT challenges

Research	Contribution	Application	IoT Challenges Addressed
[9]	This survey has presented a new classification of program analysis (PA) that detects various malware applications.	General	Security: The research focuses on detecting malware, contributing to the security of IoT systems by enhancing their ability to detect malicious behavior in applications. Privacy: Ensures data privacy by detecting privacy-invasive malware. Interoperability: The system can adapt to various IoT platforms.
[10]	This work has proposed a survey of vulnerabilities inside IoT environments from the perspective of forensics.	General	Security: Focused on forensic methods to address security breaches in IoT systems, ensuring a better understanding of vulnerabilities. Interoperability: Forensic tools applicable across various platforms and systems.
[11]	This work provides a comprehensive survey of IoT issues such as security, and privacy, etc.	General	Security: Highlights IoT-specific security threats and their solutions. Privacy: Explores privacy concerns in data collection and transfer. Interoperability: Examines challenges in integrating heterogeneous devices. Massive Data: Discusses handling large data volumes in IoT environments.
[12]	This article has introduced a new IoT layered model with the Identification of privacy and security components and levels. The proposed model is implemented and evaluated.	IoT system	Security: New model secures data at different levels. Privacy: Layered structure ensures privacy at each stage of data processing. Interoperability: Designed for integration across different IoT environments. Massive Data: Manages large-scale data flows efficiently. Energy Efficiency: Reduces energy consumption by optimizing the use of each layer.
[13]	The paper has concluded IoT's current challenges and solutions related to the industrial field.	Industrial IoT	Interoperability: Focuses on industrial IoT where device diversity poses interoperability challenges. Massive Data: Discusses industrial data flow and management.
[14]	This survey described an overview of IoT technologies and applications, and thus it presented the most important confidentiality, integrity, and availability (CIA) as examples of security concerns.	General	Security: Focuses on the CIA triad as a key concern in IoT systems, aiming to ensure secure communications and data transfer.
[15]	This work presents a comprehensive study of critical security issues that IoT will encounter.	General	Security: Identifies upcoming security challenges in IoT systems, providing a roadmap for future security protocols and systems.
[16]	This paper has mentioned the major issues facing IoT systems. Thus, it has discussed the merging of blockchain with IoT to solve them by proposing an architecture design.	General	Security: Uses blockchain to secure IoT data and processes. Privacy: Blockchain improves user data privacy.
[3]	This article has emphasized the idea of the Internet of Things, its development, and various communication technologies. In addition, it has discussed the possible open issues and challenges of IoT	General	Security: Highlights security challenges arising from IoT's communication protocols. Privacy: Addresses privacy issues in IoT communication. Interoperability: Discusses challenges in integrating communication technologies across various devices. Massive Data: Focuses on the impact of IoT on big data management.

(Continued)

Table 2. IoT challenges (Continued)

Research	Contribution	Application	IoT Challenges Addressed
[17]	This work has talked about different IoT applications, and it analyzed the overall system's power consumption by the implementation of an IoT gadget with an Arduino platform and a LoRa radio module.	Agriculture IoT	Energy Efficiency: Focused on optimizing power consumption in IoT devices, particularly in agriculture.
[18]	This article has reviewed the major challenges especially the security issues in the context of smart grid networks based on IoT.	IoT based Smart grid networks	Security: Addresses vulnerabilities in smart grids, focusing on secure energy management systems
[19]	This review has discussed IoT technology and its applications like agriculture, smart cities, and so forth. Thus, it has made a comparison between IoT and M2M.	General	Security: The focus on CIA highlights the fundamental security requirements for IoT systems. Massive Data: The study acknowledges the issue of managing large data volumes generated by IoT devices, especially in sectors like smart cities where data traffic is massive. Energy Efficiency: The research briefly mentions how continuous security protocols may impact energy consumption, suggesting potential relevance for optimizing energy usage in IoT applications.

4 SOLUTIONS PROVIDED BY SDN BASED ON IoT

Software Defined Networking provides an important model for researchers looking for solutions to IoT challenges [68]. In the literature, several works have been done on the utilization of SDN in IoT domains to overcome its multiple issues (refer to Table 3). The main area of these studies is generally security solutions [20], [21], [22], [23], [24], [25], [26], [27]. The studies in [28] and [29] were according to the issues of heterogeneous information and the interoperability of IoT tools.

The work presented in [30] examines the complexity of real-time configuration and management in IoT environments. In addition, in [31], the work focuses on management, mobility, and the effectiveness of energy issues. Conversely, the study [32] discussed the scalability released by the Internet of Things.

Table 3. Research of SDN-based IoT

Ref.	IoT Challenges	Proposed Solutions	Limitations/Future Works
[20]	Security	This work has proposed a taxonomy of SDN-based solution attacks; thus, it has presented a quantitative evaluation of review works.	<ul style="list-style-type: none"> – No evaluation or implementation. – Limited to security challenges.
[21]	Security	This work proposed a FUPE a security-aware job scheduler used in IoT fog networks. That applies to SDN to counteract TCP SYN flood attacks, consider IoT fog networks. The assessment of the suggested method illustrates the effectiveness of denial of TCP SYN attacks.	<ul style="list-style-type: none"> – Few types of attacks addressed – Future research is developing this approach to tackle other types of attacks.
[22]	Security (ARP spoofing attacks)	This paper has proposed a secure SDN-based IoT architecture to overcome the extent of ARP spoofing attacks by using a near machine to the SDN controller to manage ARP traffic to examine address spoofing attacks.	<ul style="list-style-type: none"> – Limited to ARP spoofing attacks.

(Continued)

Table 3. Research of SDN-based IoT (Continued)

Ref.	IoT Challenges	Proposed Solutions	Limitations/Future Works
[23]	Security flows	This paper presented an ontological security architecture related to IoT environments and thus proposed a protocol to authenticate IoT systems.	– No Evaluation or experimentation is programmed as a future work.
[28]	Interoperability Heterogeneity	This article implemented a new IoT architecture using the SDN and MQTT protocols in tandem to address the problem of heterogeneity and interoperability.	– The work doesn't take into the QoS of MQTT in a wireless network with a mobile node.
[24]	Security (DDoS attack)	This article tested and analyzed the SECOND (SDN data plane and control security) algorithm to protect SDN-based IoT networks.	– Limited to DDOS attacks – Future work includes defining a threshold for various applications and using actual IoT devices to validate the output.
[30]	Configuration Management in real-time	This work has introduced SDN-based self-configuration parameters to improve the configuration and the management in real-time in IoT environments.	– The work is passed on fixed packet sizes and doesn't handle the changing packet sizes.
[25]	Security	This work is a thorough examination of the application of SDN strategies in IoT security environments, and thus it has presented a comprehensive study of Software Defined Security (SDCec) as a solution for IoT security challenges.	– No evaluation or implementation – Future work is IoT Security solutions considering SDN and machine learning approaches.
[26]	Security	To enforce security in IoT systems, this work has developed an automated, intelligent solution to intrusion detection and mitigation for SDN. The evaluation of the proposed security mechanism has demonstrated good results in attaining precise and timely attack detection and mitigation in SDN-managed Internet of Things networks.	– Few types of attacks addressed – The suggested model will be expanded upon in future studies to include other assault kinds.
[32]	Scalability Dynamic adaptability	This work has proposed a Software Defined IoT Reprogramming framework called (SD-IoTR) that emphasizes OTA programming for Internet of Things systems to address dynamic adaptability and scalability.	– The implementation is not achieved and doesn't complete all features presented in the proposed framework.
[27]	Security	This article has implemented and evaluated a model based on the use of SDN in Internet of Things systems to counteract man-in-the-middle attacks.	– Limited to the man-in-the-middle attacks.
[29]	Heterogeneous data	This work proposes that PrioDex is a cross-layer middleware solution that uses SDN techniques to impose configuration in the Internet of Things settings. The evaluation of the model has proved the ability of this approach to improve network performance.	– The prototype doesn't include the management of dynamic conditions like varying network bandwidth/error rates. etc. – Future work is the development of this work to include the management of dynamic conditions.
[31]	Management Mobility Energy efficiency	This article has presented the idea of the "Software Defines Internet of Things concept to address IoT challenges".	– No evaluation or implementation.

5 SOLUTIONS PROVIDED BY NFV BASED ON IoT

Network Function Virtualization is a promising mechanism that provides numerous advantages for IoT networks, such as flexibility, manageability, and much more. In the literature, numerous works have studied the potential of NFV in handling IoT challenges (refer to Table 4). In this section, most articles focused on the significance of NFV in the security part of smart networks. [34], [36], [37], [40].

Table 4. Research of NFV-based IoT

Ref	IoT Challenges	Proposed Solutions	Limitations/Future Works
[33]	QoS management	This work has proposed a new approach designed to address the issues of NFV-enabled IoT platforms, known as QoS4NIP (QoS for NFV-enabled IoT Platforms), which is built on a Genetic Algorithm (GA).	– The work requires more improvement to anticipate the associated QoS violations.
[34]	Security threats	This work has proposed a software-based architecture for identifying malware threats in networks using Internet of Things devices. This model utilizes NFV techniques that provide a distributed security architecture. The evaluation of the proposed model has demonstrated its effectiveness in increasing security in IoT networks.	– The simulation doesn't examine the model in terms of the scalability of monitoring zones and the rate at which various malware attacks that are observed in IoT networks die out, and is anticipated to be included in future studies.
[35]	Complexity of IoT networks	This paper has proposed a 5G network architecture founded on NFV to enable MC-IoT services. The simulation results have been proved the maximum achieved.	– Limited to 5G wireless communication networks.
[36]	Security	This paper has presented a system to provide IoT security through VNF. The system is based on the MUD specifications.	– No Implementation – Few types of addressed attacks, the work is limited to DDoS attacks
[37]	Interoperability Security	This article has proposed a novel approach called ClimBOS is a scalable NFV-based solution that fulfils the requirements of users of IoT devices.	– The model may need more use cases to prove its efficiency in satisfying the requirements of users of IoT devices.
[38]	Mobility Complexity	This article has simulated a proposed DRL-based SFC embedding Shema. The work is based on the composition of VNF into a set of VNFCs and an internal connection graph to form the VNF-FG in the NFV-enabled IoT framework. The simulation has shown that the proposed model has a better performance.	– Convolutional neural networks (CNNs) will used in the model's application in the Internet of Things as future works.
[39]	The management of massive data	This work has introduced a new framework that applies NFV technology to an edge computing platform for IoT applications. The evaluation of the framework has proved the practicability for IoT applications.	– Edge computing only.
[42]	Interoperability	This work has introduced a network translator in a virtualized environment to address interoperability challenges in IoT platforms.	– The translator adds latency to the system.
[40]	Security	This work has proposed a new framework called NETRA a lightweight Docker-based framework to make NFV conforming with IoT environments. The framework is tested by using IoT devices.	– Few types of attacks addressed. – Future works is the study of the proposed model in handling the Zero-day attacks.
[41]	Heterogeneous devices Scalability	This work has introduced a novel NFV-enabled IoT architecture to provide the required flexibility and scalability for IoT platforms.	– No Implementation. – Future research is the integration of other devices from different vendors in the proposed architecture

6 SOLUTIONS PROVIDED BY SDN/NFV BASED ON IoT NETWORKS

In this, different works have studied the fusion between SDN and NFV to address IoT challenges, and an analysis comparison between existing works has been done (refer to Table 5).

The analysis of works mentioned in Table 5 present the integration of SDN and NFV affirmed that the complementarity between the two technologies, offers a promising approach to enhance the flexibility, scalability, and manageability of IoT networks. Thus, we can say that the usage of these concepts is crucial for the evolution of IoT, as it provides a robust framework for dynamically adjusting network resources. This combination not only facilitates network management but also simplifies the way for innovative solutions to handle the complexity of IoT deployments.

Table 5. Research of SDN/NFV solution for IoT

Ref	IoT Challenges	Proposed Solutions	Limitations/Future Works
[43]	Security	This work has proposed an SDN-NFV framework by using a classification model depending on machine learning like LR, KNN, SVM, and IF. The proposed framework has been simulated and showed a promising result.	– Limited to HTTP flood, SiDDoS Flood, Smurf Flood, and UDP flood.
[44]	Security threats	This work has introduced a new approach called (D-ARPSpoof) which is q Denial of ARP Spoofing based on the integration of SDN and NFV-enabled cloud, fog, and edge platforms for IoT applications to prevent ARP Spoofing attacks.	– Limited to ARP Spoofing attacks.
[45]	Security Scalability Complexity Management	This paper has provided a new model that presents a decentralized Blockchain-Software Defined Networking (SDN) depending on energy-aware architecture for IoT in smart cities with the usage of NFV for saving energy and load balancing. The model has introduced a Cluster Head Selection (CHS) as an algorithm to reduce energy consumption.	– The model is dependent only on smart cities.
[63]	Security	This article has proposed a mechanism based on a pipelined multichannel cryptosystem integrated into NFVI servers to secure NFV/SDN IoT systems.	– It focuses only on the development of NFVI.
[46]	Security	This paper has introduced a novel mechanism leveraging the combination of SDN and NFV to enforce security in IoT honeynets. The proposed model has been implemented and tested, showing the efficiency in mitigating cyber-attacks.	– The work doesn't implement the cognitive approaches of ANASTACIA like AI but is envisioned as future works
[47]	Security	This article has presented A zero-touch, policy-driven, semantic-aware security orchestration framework for SDN/NFV-aware Internet of Things situations. The simulation has been showing the feasibility of detecting conflicts.	– The framework doesn't consider additional needs during the SFC chaining
[48]	Security	This work has proposed a Distributed Secure black SDN-Io architecture with the implementation of NFV for smart cities to enforce security in IoT platforms.	– No evaluation or implementation. – The proposed architecture may have an additional latency problem
[49]	Complexity Management Scalability	This work has been exploring SDN and NFV network architecture for enhancing IoT gateways. The architecture has been tested in a real NB-IoT gateway.	– The implementation is limited to NB-IoT gateway
[50]	Heterogeneity Routing problems	This paper has proposed an important H-STIN architecture based on the development trends of IoT integrating SDN and NFV technologies.	– No implementation or evaluation.
[51]	Security Privacy	This study has implemented and evaluated a comprehensive architectural design to empower IoT security through the usage of SDN and NFV.	– Few types of attacks addressed. – Limited to DDoS and IoT malware attacks.
[52]	Interoperability	This survey has presented a comprehensive study of the interoperability challenges in IoT platforms.	– This survey doesn't analyze all related IoT proposals for IoT interoperability.

(Continued)

Table 5. Research of SDN/NFV solution for IoT (Continued)

Ref	IoT Challenges	Proposed Solutions	Limitations/Future Works
[53]	Security	This paper has presented a security approach named (SCORE) which is the Security Controls security-oriented reference for developing security in IoT and SDN/NFV platforms.	– No Implementation.
[54]	QoS Data analysis	This work has provided an architecture based on the integration between SDN and NFV focused on IoT environments to enhance the quality of services.	– Balancing and orchestration of virtual resources in IoT platforms is a challenge in this architecture.
[55]	Security Scalability Heterogeneity	This paper has evaluated a novel framework that exploits SDN/NFV-based security elements with current IoT security approaches in two realistic use case studies.	– Few use cases may not be sufficient to prove the maturity of the proposed architecture.

This comparison between IoT solutions focuses on how each proposal addresses specific challenges, utilizing distinct parameter values and architectural designs. For security solutions, most proposals rely on SDN or NFV to mitigate attacks such as DDoS, ARP spoofing, and man-in-the-middle. Solutions such as the SECOND algorithm and FUPE scheduler showcase strong security-focused architectures, using control algorithms tailored for real-time detection and mitigation of specific attacks. However, many are limited by the types of attacks they address or lack full implementation, highlighting the need for future expansion to cover a broader range of threats, and integration with machine learning is suggested to improve detection capabilities.

When it comes to interoperability, solutions such as SDN and MQTT-based architectures tackle the heterogeneity of IoT devices, ensuring seamless communication between different systems. These solutions leverage virtualization techniques and middleware to bridge compatibility gaps, though some suffer from added latency or lack robust QoS (quality of service) management. Scalability is addressed by frameworks such as SD-IoTR and blockchain-SDN-NFV architectures, which focus on dynamic adaptability and flexible over-the-air (OTA) updates. These architectures aim to support growing IoT networks efficiently but are often hindered by incomplete implementations, requiring further validation and feature integration.

In terms of energy efficiency, the use of algorithms such as cluster head selection (CHS) within decentralized Blockchain-SDN architectures highlights how certain frameworks prioritize reduced power consumption, particularly in smart city applications. While these energy-focused designs show potential, their narrow application scope limits their widespread adoption across diverse IoT environments. QoS management solutions, such as the QoS4NIP framework, use control algorithms such as genetic algorithms (GA) to enhance service quality in NFV-enabled IoT platforms. However, improvements are needed to fully anticipate and handle QoS violations in dynamic conditions.

The comparison reveals that while many solutions demonstrate strong architectural foundations, such as SDN-NFV hybrid models, their real-world applicability is often constrained by specific attack types, limited scalability, or incomplete implementations. The inclusion of adaptive control algorithms and further integration across varied IoT platforms will be crucial for these solutions to meet the evolving demands of IoT ecosystems comprehensively.

7 CHALLENGES OF APPLIED SDN AND NFV IN IoT SYSTEMS

On the one hand, we cannot ignore the pertinent role of SDN and NFV in the evolution of IoT performances. On the other hand, there are unique concerns and

obstacles associated with the deployment of these technologies. In IoT environments, NFV and SDN implementation necessitate large infrastructure and skill investments. For integration and operation to go well, concerns about security, interoperability, and standardization also need to be resolved.

Table 6. Challenges of SDN/NFV in IoT

Research	Technology	Challenge Types				
		Latency	Implementation	Budget Constraints	Security Performance	Flexibility
[56]	SDN		✓	✓		
[57]	SDN				✓	
[58]	SDN			✓		✓
[59]	SDN				✓	✓
[45]	SDN/NFV	✓				
[60]	NFV				✓	
[61]	NFV				✓	
[62]	NFV				✓	

Table 3 reveals several key advantages of SDN-based solutions in the IoT domain. These solutions enable centralized network management, ensuring more dynamic network configuration and better resource allocation. This centralization also allows for improved network visibility and control, facilitating the rapid detection and resolution of problems.

The NFV solutions in Table 4 illustrate how the virtualization of network functions reduces dependency on specific hardware, leading to cost reductions and increased network agility. It also indicates that NFV allows the rapid deployment of new network functions without requiring additional hardware. This is particularly beneficial in IoT environments where demand can fluctuate rapidly.

Table 5 shows that the integration of SDN and NFV technologies not only centralizes network management but also virtualizes network services, thereby increasing operational efficiency. This combination also facilitates the implementation of advanced functions such as dynamic resource orchestration and real-time analytics.

On the other hand, Table 6 highlights several significant challenges associated with the application of SDN and NFV in IoT environments. These challenges include security concerns, interoperability issues, and the complexity of managing virtualized environments, which need to be addressed to fully realize the potential of these technologies. Additional research and development efforts are necessary to overcome these obstacles and facilitate broader adoption.

In summary, the tables show that despite the challenges, the use of SDN and NFV, both individually and in combination, offers substantial improvements in network management, flexibility, and cost reduction in IoT environments.

In my view, after conducting this comprehensive study of solutions based on SDN and NFV, it is evident that these two technologies play a fundamental role in addressing a wide array of IoT challenges. However, the integration of SDN and NFV is not without its difficulties. To fully harness their potential in the IoT landscape, it is crucial to undertake extensive research and development efforts to overcome their inherent limitations and optimize their performance.

8 CONCLUSION

In this paper, we have reinforced the focus on the technical integration of SDN and NFV within IoT environments, providing an in-depth analysis of their contributions and performance metrics. By categorizing existing solutions based on the independent and combined applications of SDN and NFV, we have demonstrated how these technologies complement each other to effectively address key IoT challenges such as security, scalability, interoperability, and energy efficiency. Our analysis highlights that SDN provides centralized control and dynamic traffic management, while NFV enables flexible deployment of virtualized network functions, both of which are crucial for optimizing IoT networks.

Additionally, the paper delves into the performance of various SDN/NFV-based architectures, comparing them with existing solutions in terms of efficiency, control algorithms, and architectural designs. This comparison has provided deeper insights into the capabilities and limitations of SDN and NFV in real-world IoT applications, underscoring their potential to improve network management and security. By exploring these aspects, we have laid out clear directions for future research, particularly regarding developing SDN/NFV-based IoT frameworks capable of overcoming evolving IoT challenges.

9 REFERENCES

- [1] A. N. Rao, K. K. Kumar, and A. Balam, "Smart applications in IoT - A systematic review," *AIP Conf. Proc.*, vol. 2358, no. 1, p. 080011, 2021. <https://doi.org/10.1063/5.0061309>
- [2] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "IoT connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67646–67673, 2020. <https://doi.org/10.1109/ACCESS.2020.2985932>
- [3] A. Khanna and S. Kaur, "Internet of Things (IoT), applications and challenges: A comprehensive review," *Wirel. Pers. Commun.*, vol. 114, no. 2, pp. 1687–1762, 2020. <https://doi.org/10.1007/s11277-020-07446-4>
- [4] I. Alam *et al.*, "A survey of network virtualization techniques for Internet of Things using SDN and NFV," *ACM Comput. Surv. (CSUR)*, vol. 53, no. 2, pp. 1–40, 2020. <https://doi.org/10.1145/3379444>
- [5] M. Zerifi, A. Ezzouhairi, and A. Boulaalam, "Overview on SDN and NFV based architectures for IoT environments: Challenges and solutions," in *2020 Fourth International Conference on Intelligent Computing in Data Sciences (ICDS)*, 2020, pp. 1–5. <https://doi.org/10.1109/ICDS50568.2020.9268779>
- [6] H. Hantouti, N. Benamar, T. Taleb, and A. Laghrissi, "Traffic steering for service function chaining," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 487–507, 2019. <https://doi.org/10.1109/COMST.2018.2862404>
- [7] E. Haleplidis *et al.*, "Network programmability with ForCES," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 3, pp. 1423–1440, 2015. <https://doi.org/10.1109/COMST.2015.2439033>
- [8] S. H. Haji *et al.*, "Comparison of software defined networking with traditional networking," *Asian J. Res. Comput. Sci.*, vol. 9, no. 2, pp. 1–18, 2021. <https://doi.org/10.9734/ajrcos/2021/v9i230216>
- [9] A. A. Hamza, I. T. Abdel-Halim, M. A. Sobh, and A. M. Bahaa-Eldin, "A survey and taxonomy of program analysis for IoT platforms," *Ain Shams Eng. J.*, vol. 12, no. 4, pp. 3725–3736, 2021. <https://doi.org/10.1016/j.asej.2021.03.026>





- [10] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1191–1221, 2020. <https://doi.org/10.1109/COMST.2019.2962586>
- [11] C. C. Sobin, "A survey on architecture, protocols, and challenges in IoT," *Wirel. Pers. Commun.*, vol. 112, pp. 1383–1429, 2020. <https://doi.org/10.1007/s11277-020-07108-5>
- [12] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, 2020. <https://doi.org/10.3390/app10124102>
- [13] P. Varga et al., "5G support for industrial IoT applications—Challenges, solutions, and research gaps," *Sensors*, vol. 20, no. 3, p. 828, 2020. <https://doi.org/10.3390/s20030828>
- [14] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence, and blockchain technology," *Internet Things*, vol. 11, p. 100227, 2020. <https://doi.org/10.1016/j.iot.2020.100227>
- [15] S. Panchiwala and M. Shah, "A comprehensive study on critical security issues and challenges of the IoT world," *J. of Data Inf. Manag.*, vol. 2, pp. 257–278, 2020. <https://doi.org/10.1007/s42488-020-00030-2>
- [16] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021. <https://doi.org/10.1109/ACCESS.2021.3070555>
- [17] T. Perković, S. Damjanović, P. Šolić, L. Patrono, and J. J. P. C. Rodrigues, "Meeting Challenges in IoT: Sensing, Energy Efficiency, and the Implementation," in *Fourth International Congress on Information and Communication Technology, Advances in Intelligent Systems and Computing*, X.-S. Yang, S. Sherratt, N. Dey, and A. Joshi, Eds., Springer, Singapore, vol. 1041, 2020, pp. 419–430. https://doi.org/10.1007/978-981-15-0637-6_36
- [18] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, 2019. <https://doi.org/10.1016/j.ijcip.2019.01.001>
- [19] S. Balaji, K. Nathani, and R. Santhakumar, "IoT technology, applications, and challenges: A contemporary survey," *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 363–388, 2019. <https://doi.org/10.1007/s11277-019-06407-w>
- [20] O. Yurekten and M. Demirci, "SDN-based cyber defence: A survey," *Future Gener. Comput. Syst.*, vol. 115, pp. 126–149, 2021. <https://doi.org/10.1016/j.future.2020.09.006>
- [21] S. Javanmardi, M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, and A. Pescapè, "FUPE: A security-driven task scheduling approach for SDN-based IoT–Fog networks," *J. Inf. Secure. Appl.*, vol. 60, p. 102853, 2021. <https://doi.org/10.1016/j.jisa.2021.102853>
- [22] H. Aldabbas and R. Amin, "A novel mechanism to handle address spoofing attacks in SDN based IoT," *Clust. Comput.*, vol. 24, pp. 3011–3026, 2021. <https://doi.org/10.1007/s10586-021-03309-0>
- [23] Nazmul Hossain, Md. Zobayer Hossain, and Md. Alam Hossain, "An ontological security framework to secure the SDN based IoT networks," *American Journal of Agricultural Science, Engineering, and Technology*, vol. 5, no. 1, pp. 4–18, 2021. <https://doi.org/10.54536/ajaset.v5i1.55>
- [24] S. Wang, K. Gomez, K. Sithampanathan, M. R. Asghar, G. Russello, and P. Zanna, "Mitigating DDoS attacks in SDN-based IoT networks leveraging secure control and data plane algorithm," *Appl. Sci.*, vol. 11, no. 3, p. 929, 2021. <https://doi.org/10.3390/app11030929>
- [25] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, 2020. <https://doi.org/10.1109/JIOT.2020.2997651>





- [26] A. K. Sarica and P. Angin, "Explainable security in SDN-based IoT networks," *Sensors*, vol. 20, no. 24, p. 7326, 2020. <https://doi.org/10.3390/s20247326>
- [27] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, p. 8, 2020. <https://doi.org/10.3390/computers9010008>
- [28] R. Tamri *et al.*, "The MI-SDN system to manage MQTT data in an interoperable IoT wireless network," *Turk. J. Comput. Math. Educ. (TURCOMAT)*, vol. 12, no. 5, pp. 1031–1036, 2021. <https://doi.org/10.17762/turcomat.v12i5.1747>
- [29] G. Bouloukakis *et al.*, "PrioDeX: A data exchange middleware for efficient event prioritization in SDN-based IoT systems," *ACM Trans. Internet Things*, vol. 2, no. 3, pp. 1–32, 2021. <https://doi.org/10.1145/3456301>
- [30] N. S. Bülbül, D. Ergenç, and M. Fischer, "SDN-based self-configuration for time-sensitive IoT networks," in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, Edmonton, AB, Canada, 2021, pp. 73–80. <https://doi.org/10.1109/LCN52139.2021.9524979>
- [31] H. Zembrane, Y. Baddi, and A. Hasbi, "SDN-based solutions to improve IoT: Survey," in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, 2018, pp. 588–593. <https://doi.org/10.1109/CIST.2018.8596577>
- [32] D. Huynh-Van and Q. Le-Trung, "SD-IoTR: An SDN-based Internet of Things reprogramming framework," *IET Netw.*, vol. 9, pp. 305–314, 2020. <https://doi.org/10.1049/iet-net.2019.0223>
- [33] C. A. Ouedraogo, S. Medjiah, C. Chassot, K. Drira, and J. Aguilar, "A cost-effective approach for end-to-end QoS management in NFV-enabled IoT platforms," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3885–3903, 2021. <https://doi.org/10.1109/JIOT.2020.3025500>
- [34] N. Guizani and A. Ghafoor, "A network function virtualization system for detecting Malware in large IoT based networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1218–1228, 2020. <https://doi.org/10.1109/JSAC.2020.2986618>
- [35] X. Ge, R. Zhou, and Q. Li, "5G NFV-based tactile internet for mission-critical IoT services," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6150–6163, 2020. <https://doi.org/10.1109/JIOT.2019.2958063>
- [36] Y. Afek *et al.*, "NFV-based IoT security for home networks using MUD," in *NOMS 2020 – 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020, pp. 1–9. <https://doi.org/10.1109/NOMS47738.2020.9110409>
- [37] M. Gallo, S. Ghamri-Doudane, and F. Pianese, "CliMBOS: A modular NFV cloud backend for the Internet of Things," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5. <https://doi.org/10.1109/NTMS.2018.8328684>
- [38] X. Fu, F. R. Yu, J. Wang, Q. Qi, and J. Liao, "Dynamic service function chain embedding for NFV-enabled IoT: A deep reinforcement learning approach," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 1, pp. 507–519, 2020. <https://doi.org/10.1109/TWC.2019.2946797>
- [39] Y.-Y. Shih, H.-P. Lin, A.-C. Pang, C.-C. Chuang, and C.-T. Chou, "An NFV-based service framework for IoT applications in edge computing environments," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 4, pp. 1419–1434, 2019. <https://doi.org/10.1109/TNSM.2019.2948764>
- [40] R. Sairam, S. S. Bhunia, V. Thangavelu, and M. Gurusamy, "NETRA: Enhancing IoT security using NFV-based edge traffic analysis," *IEEE Sens. J.*, vol. 19, no. 12, pp. 4660–4671, 2019. <https://doi.org/10.1109/JSEN.2019.2900097>
- [41] I. Miladinovic and S. Schefer-Wenzl, "NFV enabled IoT architecture for an operating room environment," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 2018, pp. 98–102. <https://doi.org/10.1109/WF-IoT.2018.8355128>
- [42] S. T. Arzo, F. Zambotto, F. Granelli, R. Bassoli, M. Devetsikiotis, and F. H. P. Fitzek, "A translator as virtual network function for network level interoperability of different IoT technologies," in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, 2021, pp. 416–422. <https://doi.org/10.1109/NetSoft51509.2021.9492677>

- [43] S. Shahzadi *et al.*, “Machine learning empowered security management and quality of service provision in SDN-NFV environment,” *Comput. Mater. Contin.*, vol. 66, no. 3, pp. 2723–2749, 2021. <https://doi.org/10.32604/cmc.2021.014594>
- [44] A. K. Rangiseti, R. Dwivedi, and P. Singh, “Denial of ARP spoofing in SDN and NFV enabled cloud-fog-edge platforms,” *Clust. Comput.*, vol. 24, pp. 3147–3172, 2021. <https://doi.org/10.1007/s10586-021-03328-x>
- [45] Md. J. Islam *et al.*, “Blockchain-SDN based energy-aware and distributed secure architecture for IoT in smart cities,” *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3850–3864, 2021. <https://doi.org/10.1109/JIOT.2021.3100797>
- [46] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. Alcaraz Calero, “Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1262–1277, 2020. <https://doi.org/10.1109/JSAC.2020.2986621>
- [47] A. Molina Zarca, M. Bagaa, J. Bernal Bernabe, T. Taleb, and A. F. Skarmeta, “Semantic-aware security orchestration in SDN/NFV-enabled IoT systems,” *Sensors*, vol. 20, no. 13, p. 3622, 2020. <https://doi.org/10.3390/s20133622>
- [48] Md. J. Islam, Md. Mahin, S. Roy, B. C. Debnath, and A. Khatun, “DistBlackNet: A distributed secure black SDN-IoT architecture with NFV implementation for smart cities,” in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2019, pp. 1–6. <https://doi.org/10.1109/ECACE.2019.8679167>
- [49] S. Do, L.-V. Le, B.-S. P. Lin, and L.-P. Tung, “SDN/NFV-based network infrastructure for enhancing IoT gateways,” in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Atlanta, GA, USA, 2019, pp. 1135–1142. <https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00192>
- [50] W.-C. Chien, C.-F. Lai, M. S. Hossain, and G. Muhammad, “Heterogeneous space and terrestrial integrated networks for IoT: Architecture and challenges,” *IEEE Netw.*, vol. 33, no. 1, pp. 15–21, 2019. <https://doi.org/10.1109/MNET.2018.1800182>
- [51] A. Molina Zarca *et al.*, “Security management architecture for NFV/SDN-Aware IoT systems,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8005–8020, 2019. <https://doi.org/10.1109/JIOT.2019.2904123>
- [52] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and open challenges,” *Mob. Netw. Appl.*, vol. 24, pp. 796–809, 2019. <https://doi.org/10.1007/s11036-018-1089-9>
- [53] T. Dimitrakos, “How to develop a security controls oriented reference architecture for Cloud, IoT, and SDN/NFV platforms,” in *Trust Management XII, IFIPTM 2018, IFIP Advances in Information and Communication Technology*, N. Gal-Oz and P. Lewis, Eds., Springer, Cham, vol. 528, 2018, pp. 1–14. https://doi.org/10.1007/978-3-319-95276-5_1
- [54] Á. L. V. Paraguay, P. J. Ludeña-González, R. V. T. Tandazo, and L. I. B. López, “SDN/NFV architecture for IoT networks,” in *Proceedings of the 14th International Conference on Web Information Systems and Technologies – ITSCO*, 2018, pp. 425–429. <https://doi.org/10.5220/0007234804250429>
- [55] I. Farris *et al.*, “Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems,” in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017, pp. 169–174. <https://doi.org/10.1109/CSCN.2017.8088617>
- [56] B. Sokappadu, A. Hardin, A. Mungur, and S. Armoogum, “Software defined networks: Issues and challenges,” in *2019 Conference on Next Generation Computing Applications (NextComp)*, 2019, pp. 1–5. <https://doi.org/10.1109/NEXTCOMP.2019.8883558>
- [57] D. S. Rana, S. A. Dhondiyal, and S. K. Chamoli, “Software defined networking (SDN) challenges, issues and solution,” *Int. J. Comput. Sci. Eng.*, vol. 7, no. 1, pp. 884–889, 2019. <https://doi.org/10.26438/ijcse/v7i1.884889>





- [58] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, "Challenges and solutions in software defined networking: A survey," *J. Netw. Comput. Appl.*, vol. 141, pp. 23–58, 2019. <https://doi.org/10.1016/j.jnca.2019.04.020>
- [59] A. O. Jefia, S. I. Popoola, and A. A. Atayero, "Software-defined networking: Current trends, challenges, and future directions," in *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 2018, pp. 1677–1685.
- [60] M. Sandeep Kumar and J. Prabhu, "Analysis of network function virtualization and software defined virtualization," *JOIV: International Journal on Informatics Visualization*, vol. 1, no 4, pp. 122–126, 2017.
- [61] M. Daghmehchi Firoozjaei, J. (Paul) Jeong, H. Ko, and H. Kim, "Security challenges with network functions virtualization," *Future Gener. Comput. Syst.*, vol. 67, pp. 315–324, 2017. <https://doi.org/10.1016/j.future.2016.07.002>
- [62] X. Tao, Y. Han, X. Xu, P. Zhang, and V. C. M. Leung, "Recent advances and future challenges for mobile network virtualization," *Sci. China Inf. Sci.*, vol. 60, p. 040301, 2017. <https://doi.org/10.1007/s11432-017-9045-1>
- [63] W.-L. Chin, H.-A. Ko, N.-W. Chen, P.-W. Chen, and T. Jiang, "Securing NFV/SDN IoT using Vnfs over a compute-intensive hardware resource in NFVI," *IEEE Network*, vol. 37, no. 6, pp. 248–254, 2023. <https://doi.org/10.1109/MNET.135.2200558>
- [64] T. Jackisch, "SDN vs Traditional Network," Glyndwr University, WrexhamFigure, 2022. <https://doi.org/10.13140/RG.2.2.17889.38246>
- [65] B. S. E. Zoraida and G. Indumathi, "A comparative study on software-defined network with traditional networks," *TEM Journal*, vol. 13, no. 1, pp. 167–176, 2024. <https://doi.org/10.18421/TEM131-17>
- [66] I. Bedhief, M. Kassar, and T. Aguilii, "From evaluating to enabling SDN for the Internet of Things," in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, 2018, pp. 1–8. <https://doi.org/10.1109/AICCSA.2018.8612841>
- [67] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A survey on security, privacy, trust, and architectural challenges in IoT systems," *IEEE Access*, vol. 12, pp. 57128–57149, 2024. <https://doi.org/10.1109/ACCESS.2024.3382709>
- [68] S. W. Turner, M. Karakus, E. Guler, and S. Uludag, "A promising integration of SDN and blockchain for IoT networks: A survey," *IEEE Access*, vol. 11, pp. 29800–29822, 2023. <https://doi.org/10.1109/ACCESS.2023.3260777>
- [69] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "IoT connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67646–67673, 2020. <https://doi.org/10.1109/ACCESS.2020.2985932>
- [70] K. Fizza, P. P. Jayaraman, A. Banerjee, N. Auluck, and R. Ranjan, "IoT-QWatch: A novel framework to support the development of quality-aware autonomic IoT applications," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 17666–17679, 2023. <https://doi.org/10.1109/JIOT.2023.3278411>





10 AUTHORS

Manare Zerifi     received her M.S. degree in Internet of things and mobile systems from ENSA-Fez, the University of Sidi Mohamed Ben Abdellah Fez, Morocco, in 2019. She is currently a Ph.D. candidate at the University of Sidi Mohamed Ben Abdellah Fez, Morocco. Her research interests include: IoT, SDN, NFV, fog computing. She can be contacted at email: manare.zerifi@usmba.ac.ma.

Prof. Dr. Abdellatif Ezzouhairi     received Ph.D. and M.Sc. degrees in Mobile Computing from Ecole Polytechnique, Montreal, Canada, and Engineering degree in Computer Sciences from ENSIAS, Rabat, Morocco. He worked as an

associated researcher at the Mobile Computing and Networking Research Laboratory, Chair Ericsson Canada. He is now a Full Professor at USBMA-ENSA University, Morocco. His research interests cover Mobile Network Integration and the Internet of Things. He can be contacted at email: abdellatif.ezzouhairi@usmba.ac.ma.

Prof. Abdelhak Boulaalam     is a Professor in Dept. of Electrical and Computer Engineering at the National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, and Fez, Morocco. He received a Ph.D. degree in computer science from Sidi Med Ben Abdellah University. He holds M.Sc. (USMBA University, Morocco) degrees in computer sciences. He has published some journal and conference articles and book chapters in the areas of IoT, Intelligent Products, IMS, Product Data Management, and PLM. He also serves as a reviewer for various journals and conferences. He can be contacted at email: abdelhak.boulaalam@usmba.ac.ma.

Mohamed Baghrous     received his M.S. degree in Internet of Things and mobile systems from ENSA, the University of Sid Mohamed Ben Abdellah, and Fez, Morocco. He is currently a Ph.D. candidate at the University of Sid Mohamed Ben Abdellah Fez, Morocco. His research interests include IoT, Fog computing, and smart farming. He can be contacted at email: mohamed.baghrous@usmba.ac.ma.