SECURE LIGHTWEIGHT NFV ARCHITECTURE ANALYSIS FOR IOT EDGE COMPUTING

Shyam Raveenthiran[1,2]

[1]Sri Lanka Institute of Information Technology
[2]Department of ICT, Faculty of Technological Studies University of Vavuniya

Abstract

The IoT is a massive trend within an industry. Its exponential expansion in cloud computing creates new problems. NFV has solutions enabling service providers to scale the networks, integrate intelligence into those networks, and figure out how to monetize all these IoT devices. New threats and concerns about security breaches in the network are multilayered and dynamic. It's no longer about the transport layer, and it's about delivering services to users profitably. As a result, service providers are looking at NFV to help them build services, customize them, spin them up faster, and deliver a broader array of services to users. Due to the low processing capability of IoT devices, offering a lightweight NFV architecture for Edge Cloud Computing in IoT is critical for mitigating cyber assaults in this developing cyber domain.

Keywords*: Cloud Computing, IoT, NFV, SDN, Vulnerabilities.*

1 INTRODUCTION

The software-defined networking (SDN) sector was hailed as the networking industry's next major advancement. SDN has evolved from a single-use situation to being utilized in a variety of networking settings. SDN, or software-defined networking, was touted as the next big thing in the networking business. Software-defined networking is ascribed to academics from Stanford who invented the notion of bringing virtualization principles to networking. Data is routed through routers and switches utilizing integrated hardware and software in conventional networking. The first use of SDN was to virtualize networks by dividing the control plane and the data plane that carries the traffic. A smart controller running specialized software and a set of routers and switches that forward packets of traffic manage the network traffic of a data center. Virtualization provides various advantages, including the ability to dynamically scale networks, fine-tune them for specific application use cases, and apply security standards to each network. Today, the SDN industry has reached maturity and is breaking out of the data center. SDN governs how organizations connect to branch offices through the WAN. SD-WAN is a use case in which software is employed to aggregate several network connections, such as broadband, MPLS, and wireless, to create resilient and cost-effective connections. Utilizing micro-segmentation, which is the notion of segmenting network traffic for security purposes, SDN has been used for network security. Alternatively, certain networks might be exceedingly secure and transport important data. Other networks may be publicly accessible. Therefore, if a hacker obtains access to the data center, their harm is restricted to a specific area of the network. Moreover, SDN is used in the industry known as Network Function Virtualization (NFV). This is the notion of replacing specialized hardware firewalls and load balancers with software-based firewalls and load balancers. Certain companies are utilizing SDN to connect server farms to public cloud providers, hence enabling the development of a hybrid cloud platform with micro-segmentation and dynamic scaling features. By segmenting internet traffic and aiding with data organization, more SDNs might be utilized to aid in the management of the Internet of Things' massive traffic surge. SDN has evolved from a single-use case to a wide range of networking applications inside the data center, the cloud, and the growing domain of the Internet of Things. The network becomes more flexible, controllable, and adaptable to new use cases when software is applied to operate it. Service providers require a new view on how the business network operations should be structured due to the rise of IoT devices [1]. Virtualization creates exciting opportunities by substituting flexible functions implemented in software for expensive physical resources. Harnessing the benefits of virtualization requires a comprehensive type of NFV orchestration. Its governance capabilities enforce rules for the efficient assignment, use, and optimization of virtual resources, while its intelligent automation orchestrates activation management. NFV architecture enhances these capabilities with security accounting and data analytics tools. Virtual network services may be automatically balanced among scales or dynamically shifted throughout the network in real-time. Resources are no longer tied to a single data center. Still, they are distributed across the network to improve internal operational efficiency, resulting in better financial performance and optimal operating margins. Service providers may ensure that network operations are performed at the lowest possible cost while adhering to service level agreements. Customers are not satisfied with their service providers' NFV architecture to eliminate the physical constraints associated with network operation. Proper NFV enables businesses to maximize revenue and service quality by providing flexible infrastructures and digital service ecosystems.[2] It cannot convert passive value chains into active value constellations without the help of NFV architecture for virtual networks. In recent days IoT devices have represented several security risks for various reasons.

A highly scalable network-based platform for IoT security and visibility deployed at the ISP level IoT is implemented as an off-path virtual network function on the ISP network that analyzes the traffic of several residential and small business customers concurrently. These endpoints are either the homeowner's mobile device or the cloud based IoT service [2]. IoT critical framework provides a dashboard for the network operation center (NOC) and the homeowner to monitor and manage IoT traffic. Network - personal networks are monitored. The network operator has an up-to-date inventory of all connected devices and their state. Each device's attributes are specified, including its profile or safelist, retrieved from its data when an IoT device begins interacting with an unauthorized destination. When a new device is added to the home network, the network function notifies both the homeowner and the network operator. The same mud profile is used for all devices of the same type across multiple homes. The home networks are connected to the ISP network via the NAT, the home router [3]. As a result, all devices in the home use the same IP address outside the home. A client-server protocol connects home routers to an autoconfiguration server (ACS). Configure the home router to label outgoing IoT traffic using DHCP bits in the IP packet. Each IoT device is assigned a unique mark coordinated by the virtual network function.

2 Related Works

Software-Defined Network is beginning to be utilized as a framework to manage potential threats because it offers numerous benefits such as dynamic flow control, IoT traffic, and device isolation, network monitoring to identify attacks (such as botnets), and flexibility to support depth payment if virtual network security functions. Software-Defined Network is beginning to be utilized as a mechanism because it offers numerous benefits such as dynamic flow control, IoT traffic, device isolation, and network monitoring to identify attacks (such as botnets),

In this sense, Farris et al.,[4]. propose a variety of security threats and attacks, in addition to strategies for minimizing the effects of these threats using countermeasures based on software-defined networks. To improve the functionality of the Internet of Things, Mouradian et al. [5] present a Software Defined Network design. It plans to protect communications via the Internet of Things by relying on the centralized controller of the software-defined network to improve system administration and provide secure routing services. IoT traffic is monitored by a Software-Defined-Network gateway in the research carried out by Shih et al. [6] to identify inappropriate behavior on a network and then respond by blocking or forwarding the data. Shih et al, [7] have created a Software-Defined-Network (SDN) security solution for Internet of Things wireless networks. The goal of this approach is to avoid compromising a security domain by dispersing security rules over multiple security controllers. Pan and Yang,[8]. presented a software-defined security framework for the Internet of Things that enables the supply of security appliances like access control or channel protection; however, they do not make use of NFV. This framework enables the delivery of security appliances.

In contrast, NFV has the potential to realize security as a service model by divorcing security software from hardware. This would allow virtual network security services to function more effectively. Lightweight virtualization creates the conditions for the deployment of Virtual Network Functions (VNF) at the edge of Internet of Things (IoT) networks. For instance, provides a solution that helps improve network administration in 6LoWPAN Internet of Things networks [9]. This solution is based on Software Defined Networks, Network Function Virtualization, and cloud computing. IPsec is an Internet of Things security architecture that was developed by Shu et al. [10]. It enables the delivery of micro middleboxes source lightweight IoT devices on demand. NFV makes it easier to scale the security VNFs that are located at the edge of the network, such as Firewalls dvIDS, according to the current state of the network and the system. The combination of Software Defined Network with Network Function Virtualization (NFV) has the potential to boost resource utilization, optimize the chaining of virtualized middleboxes, and steer traffic towards virtual network functions (VNFs).

The challenges, potential benefits, and potential dangers that are related to NFV are discussed by Fu et al. [11]. Other recent publications do the same thing, summarizing the major benefits of using software-defined networks and network function virtualization to improve the security of IoT networks. The studies, in contrast to our study, do not give a comprehensive cyber-security framework that is dependent on Software Defined Network and NFV to strengthen the security of IoT devices. The framework can dynamically identify cyber-security risks and respond based on the present status of Internet of Things (IoT) networks, systems, and security regulations that have been established [12], [13].

Thanh,[14] provides a framework for policy-based frameworks that is aroused on an expanded model of Event-Condition-Action (ECA) rules. These rules incorporate post conditions to validate the successful fulfillment of policy actions. Rensing et al. [15] provide a policy-based architecture and framework that is tailored specifically for AAA. Bonfim et al. [16] use policy-based network management with context awareness for Mobile Ad hoc Networks (MANETs), whereas Lv and Xiu, [17] offer-based framework management for securely deploying and configuring network traffic-processing components. Both management approaches are used for Mobile Ad hoc Networks (MANETs).

An initial overview of the Anastacia project was provided at the beginning of the project in the form of a conference presentation. This paper focused on the key aims, issues, and foundations of the project. In the same vein, a rudimentary knowledge of how security features based on software-defined networks and network function virtualization might be used for Internet of Things applications as outlined. Zarca et al [18]. only just described the mechanism that would be used to implement the Anastacia policy. In contrast to the current study, however, preceding articles did not offer the whole final architecture and did not address the complete autonomic loop for self-protection and self-healing of the Internet of Things controlled system. In addition, neither the monitoring, detection nor reaction tactics against cyberattacks were addressed nor assessed. This was disappointing.

2.1 IoT Edge Outline

According to this Google trend chart, public interest in the edge has increased, and the edge has become increasingly popular. Especially in the last three and a half years, we've found several factors that we believe are driving this trend toward precision, and we've addressed these 10 themes in detail. If it wasn't already clear that edge is a trending issue, there is quantifiable evidence to demonstrate its popularity. The phrase edge computing refers to intelligent computational resources situated near the price of data consumption or creation. From the standpoint of IoT analytics, edge computing refers to intelligent computational resources positioned near the source of data consumption or creation. The industrial context edge has existed for many years. You have industrial controllers and centers and robots and all sorts of things that are running on the edge and executing automated chores and stuff, but from our perspective, these edge devices are undergoing a sea change. We do not consider them clever because they frequently run on proprietary operating systems before running proprietary applications, and the hardware is tightly connected to the software. When we speak of the intelligent edge, we are referring to edge computing devices that can execute numerous sorts of apps and often run the Linux operating system.

2.1.1 Types of IoT Edge

The many sorts of computational resources up into the cloud and the edge, with an emphasis on the cloud. Most objects running in the cloud are data centers, which are geographically structured. National or regional data centers and local data centers are the three forms of cloud that we have identified. There are six distinct types of computing resources available at the edge, as well as a few more in-depth options. From the cell tower data centers at the highest level or closest to the cloud down to the sensors and devices, we divide these edges compute resources into three groups, beginning with the cell tower data centers. This relates to the computation capacity of the thick edge, thin edge, and micro edge. Depending on the type of edge and the user's use case, different computer resources are required to achieve the user's use case. It is somewhat quantitative to examine the usual computational characteristics at the various levels of the edge when defining the edge. The closer you are to the data source and the further you are from the data source, the shorter the latency between the compute resource and the device that is creating the data. Typically, the sensors and devices that require computing resources are the sensors themselves. They are millimeters distant from the equipment that generates computational output. Considering the cloud, on the other hand, cloud data centers may be located kilometers away from the device providing the data, resulting in a normal increase in latency. In the coming years, as private 5g and private LTE grow more popular, there may be a shift in the competitive advantage in the industrial sector as private 5g and private LTE become more prevalent. There are numerous industries in which edge computing can be placed anywhere, from your home's Alexa to an industrial facility. The focus of the market research we've been working on, and the industrial edge have some distinct qualities that deserve additional attention.

This report focuses on the industrial edge computing market as well as the intelligent industrial edge computing industry. The market for industrial edge computing reached $11.4 billion in 2019 and is predicted to grow at a CAGR of 70 percent throughout the forecast period [16]. Industrial edge computing underscores the notion that what we are examining does not contain quote or unquote ”dumb” field equipment that has been in the field for decades and runs proprietary software and hardware. The majority of DCS systems plc that utilize ladder logic are excluded from the intelligent edge. The industrial edge refers to compute resources deployed in industrial environments, and the term edge is also significant in this context. Cloud-hosted infrastructure software is becoming an increasingly vital component of the industrial automation industry, yet we are not considering it. The intelligent industrial edge market's share of the industrial automation market. 7% percent of the industrial automation market [16], according to those who believe intelligent industrial edge is the future. As the growth rate of the intelligent industrial edge outpaces that of industrial automation, we may assume that this sector of the market will continue to increase.

2.1.2 *Trends and Challenges*

Trends and challenges related to the thick edge, beginning with computers, one of the factors driving this adoption is the decoupling and consolidation of automation workloads from the underlying hardware. Previously connected with hardware and proprietary software, control and visualization workloads are now being separated from this hardware. Containerized applications frequently run on more intelligent edge computing devices. Applications can run on top of a Linux operating system alongside non-real-time and real-time software applications and even third-party consumer applications [18]. Once you have decoupled the automation hardware from the software, you must be conscious of the usually short product life cycles associated with such equipment. As we all know, IoT gear can remain operational for decades, and these workloads are becoming detached from regular IoT hardware. When deploying more sophisticated computer resources, you must ensure that the industrial PCs and data centers on which these workloads will be deployed have the same support life that you as an end-user have come to anticipate from the IoT vendor.

The first trend we've observed here is custom-made solutions. By pre-configuring and pre-certifying these solutions, these providers hope to shorten the maintenance and integration time associated with these systems. The FTP server is pre-certified to operate the industrial software suite, and another trend on the edge of the industrial or on-premises data center is the provision of hardware as a service. Traditional IoT providers and cloud hyperscale are beginning to provide on-premises edge computing as a service. Vendors now provide their equipment as a service as opposed to requiring a huge capital expenditure to purchase an entire data center; hyperscale's are also adopting this model. Amazon and Azure are now selling their hardware as a service that can be deployed on-premises. Microsoft's new azure stack edge hardware is a rack-based server with a Windows logo that can be placed in your data center to expand the azure cloud on-premises. Use cases and architectures at the cutting edge of the industry. In a cost reduction analysis based on case studies for the industrialized computing report [19] with the use cases, cost reduction use cases were the largest group that we identified. There are many use cases for cost reduction, but only a few case studies were examined; this is because many edge computing case studies realize numerous use cases. The maintenance and quality at the end of a single case study are depicted with other sorts of use cases [20] to provide more granular information. The cost reduction category is related to many different types of use cases [21].

2.2 IoT Edge Architecture

The forms of architectures edge architectures that are utilized to realize these. The three sorts of edge architectures that we've identified in the research are deployed to realize the use cases specified in (figure1). The first sort of architecture is fledged architecture. These are architectures in which there is no cloud backhaul a lot of these systems are airdropped to incorporate at least one of the many types of edge compute resources in those systems.

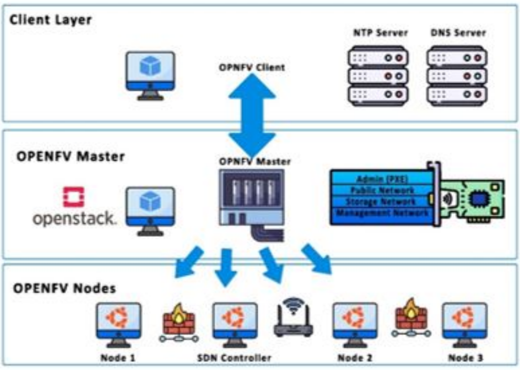


Figure 1. NFV OpenStack Deployment Layers

The second form of edge architecture is a thick edge plus the cloud. This is when you have an on-premises data center and some form of backhaul to a cloud-based or off-premises-based edge computing resource. Edge computing devices to be classified as a thick edge plus cloud to have an on-premises data center and an off-premises cloud. The third type of edge architecture identified was the thin or micro-edge plus the cloud [22]. These edge architectures do not have an on-premises data center, but they have one or more of some of these lighter-weight computational resources running on the edge and then sending data back up to the cloud for analytics or other types of use cases. An investigation of the case studies revealed that there is no ideal architecture for every use case. There were a few case studies that reduced downtime using full edges, but there were also many case studies that used different designs, and the same holds for most use cases that we found in the research. The answer to this question relies on the exact problem you are attempting to solve and the context in which you are attempting to deploy your edge computing resources [23]. A. Virtual Machine Architecture Open Platform for Network Function Virtualization (OPNFV) is essentially an OpenStack environment for deploying VNFs utilizing VMs. OPNFV offers multiple installers, such as Compass and Fuel, for deploying the technology. Its usability and 5 VMs are established to set up the infrastructure. The top-level perspective of the environment based on the OPNFV architecture is depicted in Figure 1. describing each of the three architectural layers. B. Container-based Architecture We've talked about the difficulties OPNFV faces, and it's clear that we need a solid architecture to make it easier to install VNFs at the network's edge. VNFs can be developed and deployed on low-computing devices using the proposed architecture. ISPs function as intermediaries between the cloud servers and Internet service providers (ISPs). A D-Link device communicates with the D-Link cloud when it is activated at the lowest level of the IoT stack. All our Docker images may be found in this layer, which includes the Docker Hub. It is possible to deploy Docker images using the docker pull command from this layer. If a new VNF is needed, Docker VNFs can be built and deployed in a few minutes. The IoT Gateway layer represents the actual network edge in an IoT scenario. Many

Dockers VNFs are hosted on a Raspberry Pi 3 as the IoT gateway. The Wireless Access Point (WAP) VNF defined in Section II-C is used to connect IoT devices to the network. Using this layer, devices connected to the Internet of Things can communicate with the rest of the world. As a result, this layer is capable of detecting and neutralizing threats. Our IoT gateway, the Raspberry Pi, is connected to a network of VNFs, as shown in Figure 3. The VNFs in this collection work together. VNFs such as firewalls, intrusion detection, software-defined networking (SDN) switches, edge analytics, etc., are deployed in Section II-C, as indicated. Devices connected to the Internet, or ”smart objects,” are part of the IoT environment. Smart light bulbs, IP cameras, smart remote controls, and smart plugs are among the gadgets we use in the lab. Using an SDN controller, the IoT gateway’s OpenV Switch may be managed as a VNF. It has already been demonstrated that containers may be used to run any application with minimum overhead and faster deployment times. There are at least three edge nodes required to implement OPNFVs. All VNFs are kept separate on this machine. An efficient way to implement NFV at the network edge may be seen in the comparisons of performance between two different configurations.

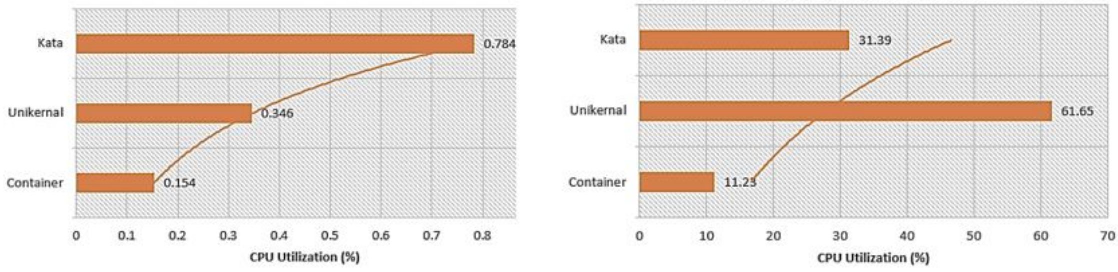
3 Methodology

The express-performance evaluation is being conducted here. Kata Containers, Unikernels, and Container-based, are the three distinct server platforms that HTTP offers. The major purpose is to define the effect of the deployed virtualization technologies on the service’s performance and to assess the benefits and drawbacks of these technologies on each platform. Express is an asynchronous server for NodeJS that does not stop requests. It is a simple building that may be modified easily. This provides access to a vast array of functionalities. This study aims to analyze emerging trends in technology for NFV adoption, specifically virtualization. Experiments and research typically test not just the platforms’ limitations but also the services’ actual performance. Comparative to Apache a tool that can transmit requests and evaluate performance can be installed on the operating system that is hosting the application.

The deployment of VNFs is accomplished using virtualization technologies, and web servers are required for network communication. Consequently, the evaluation performance considerations were considered throughout the rollout. The size of the image on each platform is what defines how much storage space is needed before the host. The scalability of a server is directly proportional to how much its CPU and memory are being utilized. Image size and the amount of RAM that was used were both measured in the first two studies. Comparisons are made between different instances of the service being performed. The next step is to evaluate the CPU’s use in both its idle and active stages. On each platform, a total of ten customers that together transmit ten thousand queries have been developed for testing the service. For traffic generation, Apache-benchmark is utilized. instances that include many threads and several clients. Docker stats is the tool that is used to get information about docker’s performance.

4 Results and Discussions

This section presents the results of the tests done. Initially, the size of images for installed services is analyzed across supported mediums. Considering the techniques of architecture, the unikernels storage is considerably less. Based on the Solution, traced back to the center which comprises just OS dependencies and system codes. The plugins are needed to program execution. In contrast to unikernels images, the regular Linux Operating System, and containers, increases in size due to the addition of unnecessary libraries and binaries. VM size comparison is illogical because it employs GPUs and reaches around 10GB with a basic installation.



(a)

(b)

Figure 2. CPU Utilization (a) on inactive state (b) on 1000 requests

5 Conclusion

This study provided an in-depth review of three virtualization technologies, kata containers, unikernels and Containers suggested an architectural solution using Figures 2 and 3. For assessment purposes, the Server is implemented on all mediums. Unikernels are consuming less memory and light to execute operations. The only necessary Operating System library operations minimize the threat surface but maximize the poor virtual allocation of memory and overhead. Due to the single address space of unikernels, applications that frequency of both mode operations executed best at unikernels implementation. Furthermore, containers are light and efficient with memory and CPU. Reduced isolation between host and kernel (shared kernel) increases security vulnerabilities. Kata containers provide light virtual machines that can execute containers utilizing their runtime. When considering Kata, it is not efficient in memory management or as speedy as Docker, but it offers a secure framework for operating containers in multi-tenant environments. The development of Kata-containers and unikernels is a major threat to the container environment. Future development for unikernels and kata-containers will be based on 5G use cases and edge device use cases .

References

[1] Clovis Anicet Ouedraogo, Samir Medjiah, Christophe Chassot, et al. “A cost-effective approach for end-to-end QoS management in NFV-enabled IoT platforms”. In: *IEEE internet of things journal* 8.5 (2020), pp. 3885–3903.

[2] Yicen Liu, Hao Lu, Xi Li, et al. “A novel approach for service function chain dynamic orchestration in edge clouds”. In: *IEEE Communications Letters* 24.10 (2020), pp. 2231–2235.

[3] Meng Wang, Bo Cheng, Xuan Liu, et al. “A sdn/nfv-based iot network slicing creation system”. In: *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. 2018, pp. 666–668.

[4] Ivan Farris, Tarik Taleb, Yacine Khettab, et al. “A survey on emerging SDN and NFV security mechanisms for IoT systems”. In: *IEEE Communications Surveys & Tutorials* 21.1 (2018), pp. 812–837.

[5] Carla Mouradian, Fereshteh Ebrahimnezhad, Yassine Jebbar, et al. “An IoT platform-as-a-service for NFV-based hybrid cloud/fog systems”. In: *IEEE Internet of Things Journal* 7.7 (2020), pp. 6102–6115.

[6] Yuan-Yao Shih, Hsin-Peng Lin, Ai-Chun Pang, et al. “An NFV-based service framework for IoT applications in edge computing environments”. In: *IEEE Transactions on Network and Service Management* 16.4 (2019), pp. 1419–1434.

[7] Carla Mouradian, Somayeh Kianpisheh, Mohammad Abu-Lebdeh, et al. “Application component placement in NFV-based hybrid cloud/fog systems with mobile fog nodes”. In: *IEEE Journal on Selected Areas in Communications* 37.5 (2019), pp. 1130–1143.

[8] Jianli Pan and Zhicheng Yang. “Cybersecurity challenges and opportunities in the new” edge computing+ IoT” world”. In: *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. 2018, pp. 29–32.

[9] Aman Kumar Singh and Raj K Jaiswal. “DDoSify: Server Workload Migration During DDOS Attack In NFV”. In: *Proceedings of the 2020 9th International Conference on Software and Computer Applications*. 2020, pp. 364–369.

[10] Chang Shu, Zhiwei Zhao, Geyong Min, et al. “Deploying network functions for multiaccess edge-IoT with deep reinforcement learning”. In: *IEEE Internet of Things Journal* 7.10 (2020), pp. 9507–9516.

[11] Xiaoyuan Fu, F Richard Yu, Jingyu Wang, et al. “Dynamic service function chain embedding for NFV-enabled IoT: A deep reinforcement learning approach”. In: *IEEE Transactions on Wireless Communications* 19.1 (2019), pp. 507–519.

[12] Yugen Qin, Qiufen Xia, Zichuan Xu, et al. “Enabling multicast slices in edge networks”. In: *IEEE Internet of Things Journal* 7.9 (2020), pp. 8485–8501.

[13] Bilal R Al-Kaseem, Yousif Al-Dunainawi, and Hamed S Al-Raweshidy. “End-to-end delay enhancement in 6LoWPAN testbed using programmable network concepts”. In: *IEEE Internet of Things Journal* 6.2 (2018), pp. 3070–3086.

[14] Nguyen Huu Thanh, Nguyen Trung Kien, Ngo Van Hoa, et al. “Energy-Aware Service Function Chain Embedding in Edge–Cloud Environments for IoT Applications”. In: *IEEE Internet of Things Journal* 8.17 (2021), pp. 13465–13486.

[15] Mohammed Ketel. “Fog-cloud services for iot”. In: *Proceedings of the SouthEast Conference*. 2017, pp. 262–264.

[16] Michel S Bonfim, Kelvin L Dias, and Stenio FL Fernandes. “Integrated NFV/SDN architectures: A systematic literature review”. In: *ACM Computing Surveys (CSUR)* 51.6 (2019), pp. 1–39.

[17] Zhihan Lv and Wenqun Xiu. “Interaction of edge-cloud computing based on SDN and NFV for next generation IoT”. In: *IEEE Internet of Things Journal* 7.7 (2019), pp. 5706–5712.

[18] Tuan-Minh Pham et al. “Optimization of resource management for nfv-enabled iot systems in edge cloud computing”. In: *IEEE Access* 8 (2020), pp. 178217–178229.

[19] Duong Tuan Nguyen, Chuan Pham, Kim Khoa Nguyen, et al. “Placement and chaining for runtime IoT service deployment in edge-cloud”. In: *IEEE Transactions on Network and Service Management* 17.1 (2019), pp. 459–472.

[20] Alejandro Molina Zarca, Jorge Bernal Bernabe, Ruben Trapero, et al. “Security management architecture for NFV/SDN-aware IoT systems”. In: *IEEE Internet of Things Journal* 6.5 (2019), pp. 8005–8020.

[21] Talal Alharbi, Ahamed Aljuhani, Hang Liu, et al. “Smart and lightweight DDoS detection using NFV”. In: *Proceedings of the International Conference on Compute and Data Analysis*. 2017, pp. 220–227.

[22] Rishi Sairam, Suman Sankar Bhunia, Vijayanand Thangavelu, et al. “NETRA: Enhancing IoT security using NFV-based edge traffic analysis”. In: *IEEE Sensors Journal* 19.12 (2019), pp. 4660–4671.

[23] Alejandro Molina Zarca, Jorge Bernal Bernabe, Antonio Skarmeta, et al. “Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks”. In: *IEEE Journal on Selected Areas in Communications* 38.6 (2020), pp. 1262–1277.