International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 322-331
Published Online July 2019 in IJEAST (http://www.ijeast.com)

VIRTUALIZING THE IOT ECOSYSTEM: A BRIEF REVIEW, ADDRESSING NFV STRATEGIES

Francis Aidan Ruambo
Department of Computer Science and Technology
Huazhong University of Science and Technology (HUST), Wuhan,430074, China
Department of Information and Communication Technology (ICT)
Mbeya University of Science and Technology (MUST), Mbeya,131, Tanzania

Justin Alipoki Mwakatobe
Department of Information and Communication Technology (ICT)
Mbeya University of Science and Technology (MUST), Mbeya,131, Tanzania

***Abstract*— Pervasiveness in computing, connectivity, and use of Internet Protocol (IP) contributes highly to the rapid growth of the Internet of things (IoT). The deployment of IoT and its applications range not only from smart cities to ubiquitous healthcare but also to the internet itself, thus resulting in a complex physical infrastructure of diversified network systems. The complicated IoT ecosystem infrastructure poses several challenges in effectively controlling and monitoring the system network functions and services. This triggers the need for dynamic and efficient solutions for management and configuration. The emerging strategy that promises to address the aforementioned challenges is by orchestrating the system network functions and services automatically. In the recent past, automating management and configuration processes to deliver system network functions and services has been an interesting research topic and extensively researched. It is achievable through virtualization technologies namely Network Function Virtualization (NFV) and Software Defined Networks (SDN). In this article, a brief overview of the NFV strategies towards virtualizing the IoT ecosystem is addressed. In addition, challenges and insights upon adopting NFV to virtualize the IoT ecosystem are highlighted. The review reveals that, in order to virtualize IoT ecosystem efficiently, there is a need for building an integrated IoT-NFV based framework with in-built automation capabilities by incorporating appropriate virtualization technologies whilst embracing the best design, performance and security principles and practices.**

Keywords— **Network Function Virtualization, Internet of Things, Network Management, Software Defined Network**

I. INTRODUCTION

The term "Internet of Things" refers to "scenarios whereby connectivity of the network and computation capability aspects are extended to sensors and commonplace items which are not computers per se, allowing them to create, transmit, receive and consume data with the least human involvement." IoT comprises consumer products, long-lasting goods, industrial and utility components, sensors, cars and trucks, and many more[1]. It allows users to interact with the network in a new way, using more devices than the existing traditional computers, laptops, and smartphones. IoT brings several opportunities which are novel within industrial applications and critical infrastructure, but worth mentioning challenges as well. The increasing reliance on the use of the network-connected technologies in our daily activities has grown faster, this accelerates the increase in a number of IoT devices within the IoT ecosystem. Although the wide range of IoT elements is designed to offer numerous benefits in the areas of automation and efficiency, at the same time it brings together new challenges, such as scaling the huge number of devices and quantity of data that must be processed [2]. Hence, the need for installing new network access and core devices is increasing. To manage the network devices and resources efficiently, the network functions and services can be virtualized.

Virtualization refers to the logical abstraction of the underlying hardware devices within a network, through software implementation which is also termed as softwarization [3]. The abstraction decouples the control from hardware, and simplifies modifying, managing, and upgrading tasks. The deployment of virtual infrastructure or virtualization technologies is non-disruptive, as the user experiences are generally unchanged. Nevertheless, virtual infrastructure provides the benefit in managing efficiently pooled resources transversely the enterprise, permitting IT administrators and managers to be more reactive to dynamic

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 322-331
Published Online July 2019 in IJEAST (http://www.ijeast.com)

administrative needs and to use infrastructure investments efficiently. Recently, the abstraction has not been restricted to hardware only, but rather software embedded into hardware has also been virtualized as independent elements. For instance, in the IoT ecosystem, NFV and SDN are two emerging paradigms that promise to enable effective management of the network functions and services through softwarization.

NFV exemplifies a decoupling of the network functions implemented as software from the underlying hardware through leveraging virtualization techniques. As a result of the network functions being separated from hardware, NFV can significantly reduce the OPEX and CAPEX. NFV provides a range of network elements and functions, comprising routing, network address translation, content delivery networks, intrusion detection and prevention systems (IDPS), load balancing, virtual private networks (VPNs), and firewalls [4]. Myriad network functions can be alma gated into the same hardware. By using NFV, both network users and operators benefit in terms of service cost and deployment as on-demand network functions and services can be easily executed and provisioned on commodity hardware at a reasonable price. NFV and SDN do not depend on each other and each can be implemented solely and work independently. Nevertheless, SDN can increase performance and support a rich functionality known as Dynamic Virtual Network Function Service Chaining. This capability makes things easier and speeds up the deployment of network functions based on NFV. Additionally, upon integrating SDN and IoT makes it possible to automatically configure smart devices for different physical locations in a simple way using centralized management where smart nodes leave and join the network freely. This mechanism promotes network resource utilization and the agility of network service provision [5].

Principally, as illustrated in Fig. 1 by ITU-T Y.2060 [6]. all network functions and other network elements can be considered for virtualization. These virtualized instances are Operations and Management which in the context of NFV termed as Virtual Network Functions (VNFs), which provide the same functionalities as the corresponding physical instances. Therefore, virtualization of the network functions and services [7] within the IoT ecosystem is possible whilst achieving its benefits such as being more agile, robust, and cost-effective. This will reduce the number of physical devices needed, easily segment networks, and enforce security policies on physical devices. This review paper provides a brief overview of NFV strategies and challenges towards virtualizing the IoT functions and services with the emphasis on systematic and efficient management of the IoT devices and resource utilization within the intricate IoT ecosystem.

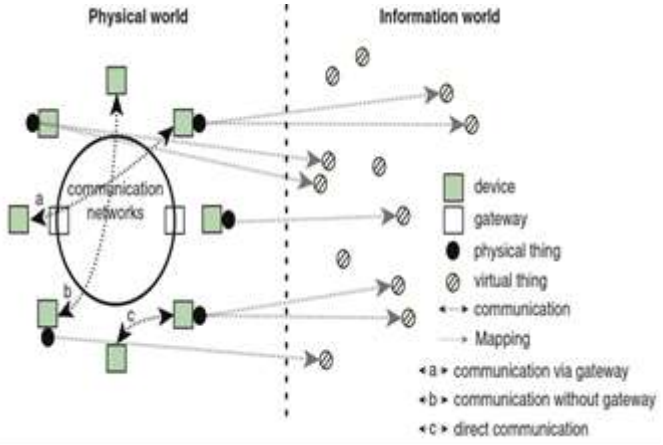

Fig. 1. Technical overview of the Internet of Things (IoT) (Y.2060) [6].

The organization of this review paper is as follows. Firstly, the IoT use cases and related management challenges are presented in Section II, then the network virtualization strategies are overviewed in section III, Section IV describes management and security NFV based solutions for IoT ecosystem, summary, and discussion of the reviewed paper is given in Section V and lastly, in Section VI the paper is concluded.

II. INTERNET OF THINGS (IOT)

Internet of Things is a collection of sensors, actuators, and smart objects, interconnected through the Internet applying embedded technology to interact and communicate with the exterior environment [8]. IoT deployment faces two major challenges namely connectivity and management. Usually, IoT systems are developed with a specific target and technology. It incorporates everything from a small object to big machines, appliances to building and industries, body sensors to cloud computing. In essence, it has infiltrated every aspect of our lives. It is estimated that the potential market value of IoT devices and associated technologies will exceed $14 trillion in the next 10 years [9]. Likewise, major hardware developers such as. Apple, Cisco, Samsung, et cetera have made huge investments in different IoT fields [9]. The following two subsections explain briefly about the common IoT use cases and IoT ecosystem management requirements and challenges.

A. IoT Use Cases

IoT is playing an important role in several use cases. Fig. 2 shows some applications within the IoT ecosystem. The benefits of IoT vary from small to large scale. Below are some of the use cases briefly introduced and highlighted their benefits within different industries.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 322-331
Published Online July 2019 in IJEAST (http://www.ijeast.com)

1) Hospitals and Healthcare: Application of IoT in both hospital premises and E-health systems is not limited to remote monitoring, but also provides a complete automated healthcare ecosystem. In accomplishing this process, several IoT devices are used, such as monitoring cameras, connected inhalers, ingestible sensors, smart insulin delivery devices, wearable sensors/data collectors, connected ambulance, etc.

2) Intelligent Transportation Systems: There are various uses of IoT applications in this domain. Sensors are used to retrieve information related to available parking spots for efficient parking management solutions. Smart signboard connected to the Internet can disseminate emergency information alongside roads. Asset tracking allows enterprises to easily locate and monitor vehicular fleets and other mobile assets. Fleet management helps transport companies reduce investment risks associated with vehicles. It improves efficiency and productivity, at the same time minimizing the overall transportation and management costs. Shipping service uses real-time traffic feeds to deliver more packages using efficient algorithms, with a lower burden on drivers and vehicles.

Connected vehicles can better automate many normal driving tasks. Benefits of self-driving cars include accident avoidance, lesser traffic congestion, and other economical efficiencies. Driverless taxis and buses are also a major use case for IoT applications. Application of IoT technology in transportation eventually reduces traffic congestion, enhances safety, productivity, and mobility.

3) Industrial Automation and Supply Chain: Industrial automation uses artificial intelligence with IoT technology, to automate the supply chain process. Supply chain along with asset tracking optimizes logistics, maintains levels of inventory, circumvent quality issues, and detect theft. Industry 4.0 production lines are greatly influenced by intelligent manufacturing system, such as smart machines (e.g. multiple smart robots used in car assembling works collaboratively) powered by IoT devices. By reducing the errors made by a human during the production process, this improves the speed of the production process and consequentially the quality of the finished products.

4) Smart Homes: IoT in such applications provides a complete intelligent ecosystem for connected devices, ranging from lighting control to security and safety. Usually, a smart central hub or gateway is used for human interaction, which in turn controls device automation. These devices can be linked to heating systems, lighting control, appliance monitoring, and control, utility usage and optimization, security system, support systems for elderly/disabled, etc.

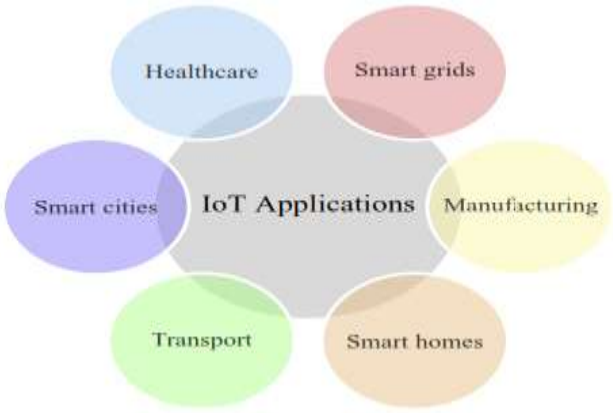

Fig. 2. Applications in the IoT ecosystem [2].

B. IoT Ecosystem Management Requirements and Challenges

IoT poses a critical and big challenge to network design that has been anticipated by network architects for a long time. To appropriately manage the huge number of devices, their bandwidth consumption, and harmonic connections, the appropriate network infrastructure must be established to suffice the need. Thus, introducing the necessity for a holistic and integrated management and orchestration system whereby visibility and automation of the processes is the panacea. Hereafter are management requirements and challenges within the IoT ecosystem.

Management Requirements

Within the IoT ecosystem, there must be a full understanding of the different components in the architecture, preferably through analytics. Furthermore, there must be heuristic intelligence capabilities to analyze the data from a broad ecosystem perception and orchestrate the environment by using policies. Lastly, it is necessary to possess the capability of enacting changes automatically in order to fine-tune for dynamic conditions. Hereafter, the requirements for managing the IoT ecosystem are briefly described.

Analytics

The system must possess the capability of collecting information from dissimilar technologies and several vendors. Data from numerous network components and elements such as application health metrics, routing topologies, DNS information must be collected. Additionally, the system responsible for management and orchestration must comprehend the inter-relationships between the virtualized infrastructure configurations and the different data points as per specific architecture.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 322-331
Published Online July 2019 in IJEAST (http://www.ijeast.com)

Heuristics

After data collection, there is a need for the existence of an intelligent entity that recognizes the inter-relationships between the data points and in what manner it relates to the business applications delivery and, sequentially, realize how the real-time analytical data has an impact to the applications. In order for the heuristics engine to present holistic and meaningful information, different application-based policies must be set into the system to get the full functional understanding that the engine can leverage.

Orchestration

Upon the architecture and functioning of the application delivery infrastructure is well understood by the system for intelligent management and orchestration, it can give recommendations and provide awareness to enact changes to the existing environment to fine-tune the cloud ecosystem to enhance delivery of the application based on different application with different levels of Service Level Assurance (SLA). Not all functions and applications are developed identically. For instance, the resilience and performance requirements for assembly line automation infrastructure differ from the Heating, Ventilation, and Air Conditioning (HVAC) automation system, likewise, possess not the same requirements as the devices for monitoring personal health.

Automation

Eventually, it is necessary to automate the management and orchestration system processes as it is not realistic to meet SLA requirements 24/7/365 for each application if the detection, analytics, and prescriptive processes are carried out manually. Eliminating the human element eliminates the loophole for human error and lessens the operational requirements to upkeep the infrastructure that may encompass thousands if not billions of devices with applications run on them.

Challenges

There are many technological challenges for deploying IoT systems so they can function smoothly. These include security, connectivity, compatibility and longevity, standards, and intelligent analysis and actions. IoT networks are usually large, mobile, and dynamically change their topology and connectivity. They also composed of heterogeneous devices which support a variety of applications. Hence, challenges like IoT device detection, low power consumption, bandwidth, access control, and data privacy become major concerns for large scale deployment.

In this section, the challenges in the management of network functions and services within the IoT ecosystem are highlighted as illustrated in Fig. 3 and thereafter are explained with the emphasis on security implementation in the management perspective.

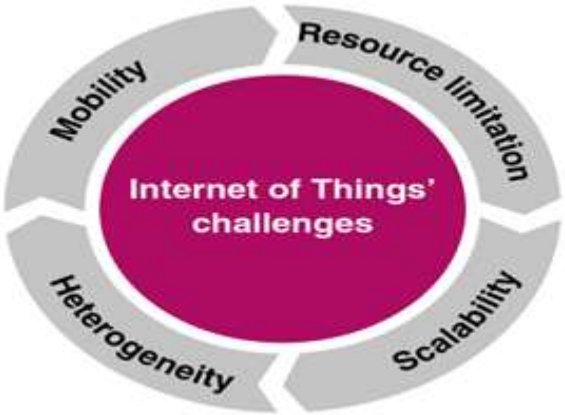

Fig. 3. Challenges in the IoT ecosystem [2].

Heterogeneity

Heterogeneity of communication standards and information system technologies in a distributed networked ecosystem is a critical issue in securing the ecosystem. For instance, the communication among sensor nodes and servers or CPU units from various applications (which are heterogeneous in terms of units of measurements and delivery frequencies) generally are carried out over Internet where networks, communication mediums, and protocols are also heterogeneous and have different security configurations. The diversity of the entities involved in IoT networks provides a wide-ranging surface for attacks from any of those entities (e.g. Attacks such as Distributed Denial of Service are inevitable) [10]. Thus, developing an adaptive solution to manage security that works in heterogeneous environments is very challenging.

Scalability

As population and reliance on using of the network-connected technologies steadily increase, it also accelerates the growth in the number of smart devices hence posing serious scalability challenge on managing security within the IoT ecosystem.

Resources limitations

Most of the devices participating in IoT networks such as embedded sensors and wearable have restricted resources in terms of memory, computation, and battery. As most of the cryptographic strategies are expensive in terms of computation, fine-tuning them to guarantee a high-security level whilst reducing consumption of energy is a serious and hard challenge in the management of the IoT ecosystem.

High mobility

From embedded sensors and actuators in human bodies to smart vehicles, reliably managing security is a critical challenge. Taking in concern about mobility within highly dynamic environments, where the topology of the network changes regularly is a serious challenging for security solutions deployment and management.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 322-331
Published Online July 2019 in IJEAST (http://www.ijeast.com)

III. OVERVIEW OF NETWORK VIRTUALIZATION STRATEGIES

Network virtualization is the mechanism of combining both software and hardware resources and network functionality into a logically configured single software-based administrative entity [11]. The terminology of virtual network denotes to the resulting software network entity. In other words, successful network virtualization would require platform virtualization along with resource virtualization. This is accomplished through the Virtualization Layer, which is an extra abstraction layer between network and storage hardware, and the running applications on it. It can be classified as either external virtualization, consisting of many networks into a virtual unit, or internal virtualization serving network-like functionality to containers of software on a standalone network server. In network virtualization generally, multiple virtual networks are run on a physical network with an illusion that each of the virtual networks is running on a physical network [12]. The following subsections elaborate each part of a virtualized network.

A. Control Plane Virtualization

Traditionally, a network consists of hardware devices for connectivity with an in-built dedicated controller. The controller is part of router architecture which gives instructions to switches where to forward packets. Hardware in the physical network devices is managed through the controller. In the existing communication network, there is a need for more flexible features from these controllers. An ideal controller can be managed anytime from geographically anywhere in the world. This has geared up the room for controller virtualization, which is implemented through Software Defined Networks (SDNs) [13]. The key idea is to isolate the control and data plane, i.e. the intelligence of the router/switch is placed in the control plane after being removed from the engine responsible for packet-forwarding. This may be implemented in a distributed or centralized manner. The controller in SDN supports programmability by permitting abstraction of the underlying infrastructure for network services and applications. Therefore, network programmability is the process of releasing the network's power in unique ways for more flexible, faster, and intelligent infrastructure that makes the network application-aware [14]. Incorporating programmability enhances network features by connecting the applications to it and thus permitting dynamic traffic flow change, providing Quality of Service (QoS) both at network and application-level.

SDN provides an architecture of the network that can be dynamic, manageable, adaptable, cost-effective, appropriate for high bandwidth requirements, and adapts to dynamic nature of today's applications. It is directly programmable, agile, and centrally manageable. It has the ability to prioritize, deprioritize or even block specific types of packets with a granular state of control while routing packets in a given network. This process may also be referred to as efficient traffic engineering allowing the administrator to use less expensive OpenFlow complaint commodity switches. OF is a communications protocol that allows access to the network switch data plane [15].

B. Function Virtualization

Function Virtualization is implemented through Network Function Virtualization (NFV) architecture. Fig. 4 shows an ETSI NFV reference architecture [16], which utilizes IT virtualization technologies to virtualize the complete network node functions into a series of building blocks to establish connectivity, and to facilitate communication services among them. Its architecture encompasses three main components: Virtual Network Function (VNF), Network Function Virtualization Infrastructure (NFVI), and Network Function Virtualization Management and Orchestration architectural framework (NFVMANO) [17]. NFV implements network functions through a piece of software that is configured under NFVI. These network functions tend to be in the form of VNF, which is responsible for handling specific network operations that run on top of the hardware infrastructure. NFVI consists of both physical and virtual storage, processing, and virtualization software. NFV-MANO architectural framework consists of interfaces and reference points to different VNFs and NFVI elements.

For example, network function such as firewall is an instance of plain software, installed inside voluminous switches, storage, and servers, to filter traffic and neutralize vulnerable packets. Further benefits include allowing the relocation and initiation of these nodes from geographically different network locations.

C. Device Virtualization

Device virtualization refers to the process whereby a switch in the data plane is virtualized using certain logical abstractions amongst its components or running only the functionality on different operating systems. Virtualization, in a computing platform, tends to hide the physical features from the users, and create an abstract computing platform to define unique rules for switches to fulfill, which may be regarded as VNFs. The control program also termed as the hypervisor is the software that controls virtualization [18]. Likewise, Sensor virtualization [19] offers software abstraction of several external IoT objects and permits applications to easily use several IoT resources via open APIs (e.g. Zeroconf [20]). Zeroconf or alike APIs permits the virtual sensor to transparently determine arbitrary sensor devices and regarding them as virtual switches. It can also communicate with different applications via a standard communication interface using UDP/TCP sockets or even HTTP [21]. In this way, there is no need for applications to deal with sensor specific details.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 322-331
Published Online July 2019 in IJEAST (http://www.ijeast.com)

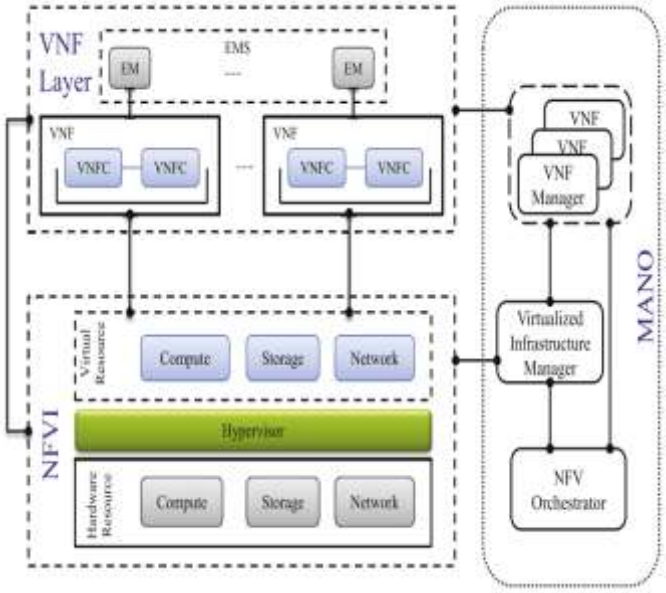

Fig. 4. A ETSI NFV reference architecture [16].

IV. NETWORK FUNCTION VIRTUALIZATION FOR IOT

Network Function Virtualization and SDN are complementary technologies. They do not require or are dependent on each other, but rather improve and facilitate each other's working. NFV provides a collection of virtual applications known as Virtual Network Functions. These can include processes for deep packet inspection (DPI), routing, security, and traffic management, which can be combined to provide network services specialized for IoT. A hybrid SDN/NFV architecture for IoT, given in Fig. 5, shows a general interaction of SDN and NFV to provide reliable communication and to facilitate IoT platforms. The architecture is composed of Network Function Virtualization Infrastructure (NFVI), Virtual Network Functions (VNFs), and Management and Orchestration (MANO) plane, leveraging each other to achieve sustainable network virtualization, with uninterrupted network connectivity and enforcing efficient packet flow rules by the SDN controller. Different components of this architecture are detailed below:

Network Function Virtualization Infrastructure: It consists of all of the networking hardware and software resources required for connecting and supporting the carrier network. These resources include operating systems, hypervisors, servers, virtual switches, Virtual Machines (VMs), Virtual Infrastructure Managers (VIMs), and any other virtual and physical assets enabling NFV.

Virtual Network Functions: VNF focuses on network service optimization. It facilitates the management of a specific network function that runs on single or multiple VMs. These VMs operate on top of physical hardware resources (i.e. router, switches, etc.). Virtual function for routing, firewall, load balancing, Intrusion Prevention System (IPS), etc. defining unified policy for virtualized hardware resources is adopted into a single VNF. In this way, multiple VNFs can be linked together to form a chain of services managed by the VNF manager and consequently the VIM.

Management and Orchestration Plane: MANO facilitates connection of services of different modules of NFVI, VNF, and APIs from the Management Plane, and coordinates with the respective subcomponents in MANO plane.

- NFV Orchestrator: NFVO works concurrently with VNFM and VIM, standardizing the of virtual networking functions and improving the interoperability of the IoT devices. It binds together different functions like service orchestration, coordinating, authorizing, releasing, and engaging NFVI resources, to build an end-to-end resource coordinated service in a distributed NFV environment.

- VNF Manager: All VNF instances are associated with VNFM. Its operations include initiation, scaling, updating and/or upgrading, and termination of VNFs.

- Virtual Infrastructure Manager: Network hardware resources like IoT gateways, SDN virtual Switches, routers, etc., are abstracted by the virtualization layer via VIM. It keeps allocation inventory of virtual and hardware resources and manages VNF forwarding graphs, security group policies, hardware resources in a multi-domain environment or optimize them for a specific NFVI environment.

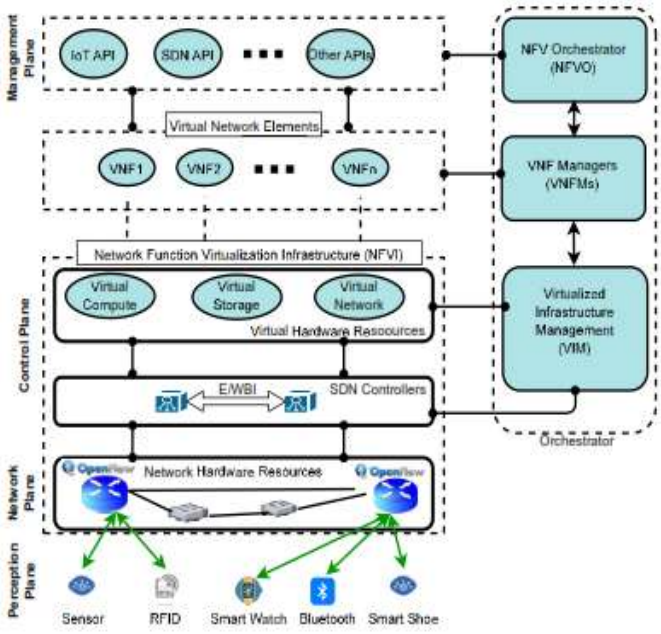

Fig. 5. A general interaction of SDN and NFV [22]

Network softwarization enabled by NFV and SDN is at present being speeded by numerous technical and economic factors such as improved performance of storage and processing at constantly decreasing expenses [23]. This drift will have a huge impact on reshaping existing IoT ecosystems and creating new opportunities because softwarization will steadily and inevitably remove the boundary between the Internet and the elements connected to it [24]. In such situation, more and more powerful IoT devices (e.g., robot, user terminal, machine, etc.) will accomplish tasks like network nodes that store data locally and even execute network functions and services [25]. Consequently, the implementation of softwarization at the edge network and IoT will constitute a borderless platform with logical resources, which is completely decoupled from the underlying physical infrastructure and spanned transversely devices, network nodes, as well as up to the cloud. Multiple services can be dynamically created and provided through this platform. From this perspective, network softwarization benefits not only IoT but also other technologies such as big data and digital money, hence creating a vast wave of modernization within all industries and fostering towards a digital society [26].

The rest of the section presents management and security solutions of NFV for IoT.

A. Management of IoT using NFV

This sub-section reviews management specific literature for function virtualization in IoT environments. Some of the solutions use SDN technology besides NFV. Batalle et al. [27] incorporate NFV and SDN in IoT to reduce cost, whereby the centralized controller facilitates the routing functionality with a global network view capability. This work presents a novel design of a virtualized routing protocol using NFV infrastructure. It basically manages and reduces signaling overhead, mainly when inter-domain routing is required. The implementation of NFV for the routing function virtualization is carried out over an OpenFlow network. It also targets to reduce the number of deployed and connected devices, therefore minimizing the cost too. Just like OpenFlow, a packet is inspected and if required, it is directed to the Floodlight controller which then takes a decision after inspecting whether the packet belongs to IPv4 or IPv6. The proposed solution is implemented using GEANT [28], that offers infrastructure to emulate OpenFlow-based SDN solutions. As the number of communication increases, the proposed solution is able to reduce the number of flow entries by 50%, which improves performance and scalability. But to enhance the virtualized function robustness, more evaluation is expected. The experiment leads to a number of open research questions, starting from implementation of dynamic routing protocols in the virtualized host, to different routing policy optimization.

Maksymyuk et al. [29] adopt an IoT-based network monitoring framework to manage the performance of 5G heterogeneous networks under different conditions. In this architecture, Radio Access Network functionalities are virtualized using NFV to simplify spectrum allocation and load balancing. Conversely, centralized intelligence in the SDN controller is used to implement spectrum allocation with interference awareness. This permits enhanced smaller cells load balancing and manages user's mobility. This proposed framework possesses two main advantages. Firstly, only relevant data will be subscribed by each network operator that can improve the existing monitoring system. It also supports multiple Mobile Network Operators (MNOs). Secondly, the small size of the transmittable data block generates less traffic overhead.

Zhang et al. [30] propose an extension to OpenNetVM using Network Function (NF) management module that manages on-demand NFs in lightweight Docker containers. This is to facilitate various service providers, leveraging startup duration and memory consumption of CPUs. OpenNetVM supports flexible and high-performance NFV architecture for a smart IoT platform, supporting increased interoperability amongst NFs. NF management module is a scalable and efficient packet processing architecture that enables dynamic manipulation of packets using service chains. The simulation result shows a significantly high rate of throughput for packet transmission leveraging Data Development Kit (DPDK) [31] to improve performance I/O. This creates scope to render complex software-based services for deep analysis within the network and data centers. This work may also remove the limitation of managing large IoT devices number to some extent. However, the deployment of NF on-demand is restricted to CPU cores.

In all the efforts mentioned in this subsection, third party services are used to facilitate and manage the network topology. Usage of SDN controllers may also include management services from vendor specific organizations. Research community may work on developing SDN/NFV-based advanced real-time applications to manage and orchestrate IoT nodes in 5G mobile networks with knowledge context awareness.

B. NFV-based Security solutions for IoT

This sub-section presents different security solutions, which use NFV to implement security in IoT. Massonet et al. [32] proposes an extended federated cloud networking architecture for edge networks and connected IoT device security. The security solution utilizes lightweight virtual functions and Service Function Chaining (SFC). In the edge networks, the IoT gateways are responsible for implementing global security policy, by creating a chain of VFs for different purposes, such as firewall and intrusion detection. They monitor the IoT devices for vulnerabilities and attacks and isolate the device upon detection. SFC is also responsible for flow management within the IoT network and also with the federated cloud, which needs the cloud and IoT platforms to have appropriate infrastructure to support it. This is done through federation agent implementation at IoT controller or gateway level. The communication itself is done using REST API. The federated network manager sends configuration information to IoT network Controller, which is then forwarded to gateways for

implementation. Finally, the network controller exchanges information with the IoT proxy, which helps to manage the data plane using the OpenFlow protocol. To safeguard the network slices within the IoT-Cloud, a module is implemented inside the IoT network controller. Future work may incorporate enhancing scalability among IoT devices, and algorithms to maintain strong privacy and security in the edge IoT ecosystem.

Al-Shaboti et al. [33] propose novel IPv4 address resolution protocol (ARP) server providing NFV security service to defend against ARP spoofing attack, and network scanning. The work also proposes an architecture based on SDN for enforcing network static and dynamic access control of smart home IoT. All ARP requests pass through a virtualized trusted entity called ARP server. It is able to secure all ARP operations, eliminating the ARP broadcast messages, and easily legitimates ARP spoofing through ARP proxy by configuring the ARP server. The work resolves packet processing delay problem using high-speed packet processing technology. Such technologies include deep packet inspection (DPI), multi-core processor, a carrier-grade operating system with Linux, and virtualization enabling the sharing of cores between applications. Here, the emphasis is only on contribution related to NFV-IoT architecture. The design architecture includes local components like data plane, NFV dispatcher, and local security services. Security agent, as one of the remote components, takes input from the user control plane, IoT policy manager, security services, and configures the SDN (Ryu) controller to enforce the corresponding network access control rules. NFV dispatcher receives all mirrored packets relaying from mirror port. Then, it forwards them basing on the dispatcher list to the corresponding security service. Security agents extract related information to direct security services for each flow. Based on the examination, security decisions/alerts are generated. IPv4 ARP server validation shows that it can protect ARP spoofing, and corresponding data plane deployment kit (DPDK) implementation performs well enough within the smart home IoT network. Future work will extend incorporating intrusion detection and prevention system into this architecture, with the inclusion of IPv6 as a significant enabler for IoTs.

NFV or SDN domains have diverse elements, applications, orchestration managers, virtual functions, communication APIs, etc. A malicious or compromised element in any of them may have severe effects on the entire system. For instance, a malicious VNF by any of the elements such as a compromised vendor software, a compromised hypervisor, or MANO component, could damage the whole network domain. If these elements are well secured than availability, confidentiality, integrity, access control, and accountability can be well well-kept. Research work on packet inspection and access control mechanisms, requires further investigation, especially for resource-constrained IoT devices.

V. SUMMARY AND DISCUSSION

The initiative for virtualization started with cloud-enabled technologies and has advanced to include emerging technologies like NFV and SDN. The prerequisite that embraces the key to success for the cloud-enabled, virtualized architectures is the necessity of having a holistic and integrated management and orchestration system. The system must possess the capability to understand the different components within the architecture via analytics, possess the heuristics intelligence aspect for analyzing the data from a wide-ranging IoT ecosystem perception and orchestrate the environment using policies, along with having the capability to enact changes automatically to fine-tune for dynamic conditions. Virtualization offers the elasticity and agility for networks to provide the resources needed for IoT to do well, without the necessity of overbuilding network infrastructures. Also, it enables the allocation and de-allocation of network resources as needed by the IoT ecosystem-aware orchestration and management system.

IoT offers virtualization a perfect and focused reason to survive and, sequentially, the effective IoT evolution relies on virtualization for the flexible network framework that can deliver, establishing a precisely mutual relationship. It is an important fact that the devices and applications exist within the IoT ecosystem are based on different technologies and coming from a different vendor, and additionally, the virtualized cloud infrastructure will consist of multiple vendors and technologies. The management and orchestration system has to be flexible and extensible sufficient to integrate these different aspects to deliver a holistic and integrated view of the whole application delivery ecosystem. Independently both technologies provide potential advantages, however, they collaboratively work together to drive the network transformation more speedily and effectively to the future generation networks and applications.

In virtualizing the IoT ecosystem, the management and deployment of NFV processes are enabled through software defined networking SDN. Using SDN, network traffic is steered between the network functions [38], and the service chain can be easily added or modified just by creating other virtual machines instances and update the forwarding decisions for such traffic using SDN. SDN ensures reliable connectivity at any given time, based on pre-defined policies. SDN supports customized device configuration enabling efficient packet flows and optimized routing. It is also a vendor-independent platform supporting widely used OF protocol, which mitigates the compatibility standardizing challenges. SDN facilitates device-to-device communication without the intervention of base stations. Heterogeneity is a major concern, especially when billions of mobile IoT devices are connected in a network. NFV plays a significant role in connecting and managing heterogeneous IoT elements. Function virtualization and service chaining mechanisms are the core components to mitigate heterogeneity limitation.

Furthermore, NFV presents the service orchestration concept, which facilitates the creation of network applications via the network functions composition using a predefined recipe. Service orchestration is a significant aspect of NFV though it introduces new challenges in security for access control. The new security challenges arise as in building new network applications, service orchestration uses high-level recipes. For this reason, access control policies must have the same level of abstraction as these recipes. Also, it is projected that network applications within SDN/NFV are made up of heterogeneous resources, given the diversity of network functions, possibly running on top of different implementation technologies. In this sense, various enforcement mechanisms have to apply the high-level security policies defined during orchestration. Since those different use cases have different security requirements, no one size fits all. As long as no silver bullet solution to the aforesaid challenges, a flexible and adaptable framework to IoT use cases is needed. Security within IoT systems and services requires automated visibility from end to endpoints, equipped with innovative detection capabilities, driven by the threat intelligence permitting orchestration of responses to alleviate threats at machine speed. What is required is an integrated and distributed, framework-based security approach that can cover the whole networked ecosystem, increase and guarantee resilience, and protect computing resources. This strategy can effectively enable monitoring legitimate traffic, checking authentication and credentialing, and imposing access management across the distributed ecosystem through a security architecture that is integrated, synchronized, and automated. Combination of NFV and SDN supports network programmability, which can improve access control and bandwidth, data encryption, IoT device detection, low power consumption, etc. for large scale IoT ecosystem deployment.

VI. CONCLUSION

Network functions virtualization has widespread deployment in core networks and data centers, where it plays a significant role in reducing the OPEX and CAPEX through promoting network resource utilization and the agility of network service provisioning. The recent development in the Internet of Things has drawn a strong interest within the research community as well as industry to integrate virtualization in the IoT ecosystem. In this review paper, network virtualization strategies for IoT ecosystem have been addressed. For efficient virtualization of the IoT ecosystem, management requirements and security challenges were highlighted, and their respective NFV solutions were reviewed and insights for future research issues were given. The review finds that heterogeneity is a major concern, especially when billions of mobile IoT devices are connected in a network. NFV plays a significant role in connecting and managing heterogeneous IoT elements. Function virtualization and service chaining mechanisms are the core components for NFV to mitigate heterogeneity limitation within the IoT ecosystem. Combination of NFV and SDN supports network programmability, which can improve access control and bandwidth, data privacy, IoT device detection and low power consumption for large scale deployment of IoT. Additionally, different IoT use cases have different management and security requirements, thus there is such a special or universal solution towards virtualizing IoT ecosystem perfectly. For efficient IoT virtualization, there is the need for building an integrated flexible and adaptable IoT ecosystem framework with in-built automation capabilities by incorporating appropriate virtualization technologies whilst embracing the best design, performance and security principles and practices.

VII. REFERENCE

[1] Rose, K. Eldridge, S. and Chapin, L. (2015). "The Internet of Things: An Overview - Understanding the Issues and Challenges of a More Connected World," *Internet Soc.*, no. October, p. 80.

[2] Kouicem, D.E. Bouabdallah, A. Lakhlef, H. (2018). Internet of things security: A top-down survey, *Computer Networks*,141199221.doi.org/10.1016/j.comnet.2018.03.012

[3] Blenk, A. Basta, A. Zerwas, J. and Kellerer, W. (2015). "Pairing sdn with network virtualization: The network hypervisor placement problem," *in Proc. of IEEE Conf. on Network Function Virtualization and Software Defined Network*, pp. 198–204.

[4] Cloud Security Alliance "Security Position Paper Network Function Virtualization" [Accessed 05- May, 2019].[Online].Available:https://cloudsecurityalliance.org/download/security-position-paper-network-function-virtualization/.

[5] Wang, P. Lan, J. Zhang, X. Hu, Y. Chen, S. (2015). "Dynamic function composition for network service chain: model and optimization, *Elsevier Comput. Netw.* 92 (2) 408–418, doi: 10.1016/j.comnet.2015.07.020.

[6] ITU-T, Overview of the Internet of Things. Y.2060, June 2012.

[7] Bijwe, S. Machida, F. Ishida, S.and Koizumi, S. (2017). "End-to-end reliability assurance of service chain embedding for network function virtualization," *in Proc. of IEEE Conf. on Network Function Virtualization and Software Defined Networks*, pp. 1–4.

[8] Fan, Y. J. Yin, Y. H. Xu, L. D. Zeng, Y. and Wu, F. (2014). "Iot-based smart rehabilitation system," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1568–1577.

[9] Bradley, J. (2013), "The internet of everything: Creating better experiences in unimaginable ways." [Accessed 16-January2019].[Online].Available:https://blogs.cisco.com/digital#more-131793.

[10] Ruambo, F.A. (2019)."Network Security: A Brief Overview of Evolving Strategies and Challenges", *IJSR*,https://www.ijsr.net/archive/v8i2/show_abstract.php ? id=ART20194980, Volume 8 Issue 2, 834 - 841

[11] Hwang I. and Shin, D. (2018). "Application level network virtualization using the selective connection," *in Proc. of Int. Conf. on Consumer Electronics (ICCE)*, pp. 1–2.

[12] ETSI, (2012). Network function virtualization-white paper1, SDN, and openflow world congress, Darmstadt, Germany, [Online]. Available: http://portal.etsi. org/NFV/NFV _ White _ Paper.pdf.

[13] Banchuen, T. Kawila, K. and Rojviboonchai, K. (2018). "An sdn framework for a video conference in inter-domain network," *in Proc. of Int. Conf. on Advanced Communication Technology*.

[14] Shu, Z. Wan, J. Lin, J. Wang, S. Li, D. Rho, S. and Yang, C. (2016). "Traffic engineering in software-defined networking: Measurement and management," *IEEE Access*, vol. 4, pp. 3246–3256.

[15] Raghavan, B. et al., (2012). ''Software-defined internet architecture: Decoupling architecture from infrastructure,'' *in Proc. 11th ACM Workshop Hot Topics Netw.*, pp. 43–48.

[16] ETSI, NFV: Architecture framework, 2014, [Accessed 05-May,2019].[Online].Available:http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf.

[17] Park, C. and Shin, D. (2017). "VNF management method using vnf group table in network function virtualization," *in Proc. of Int. Conf. on Advanced Communication Technology*, pp. 210–212.

[18] Demral, Y. and Demrc, M. (May 2018). "An investigation of hypervisor effect on virtual networks performance," *in Proc. of Signal Processing and Comm. Applications Conference (SIU)*, pp. 1–4.

[19] Ko, J. Lee, B.-B. Lee, K. Hong, S. G. Kim, N. and Paek, J. (2015). "Sensor virtualization module: Virtualizing IoT devices on mobile smartphones for effective sensor data management," *Int. Journal of Distributed Sensor Networks*, vol. 11, no. 10, p. 730762.

[20] Chesire S. and Steinberg, D. (2006). "Zero Configuration Network-The Definitive Guide", [Accessed 30-January-2019].

[21] Evensen P. and Meling, H. (2009). "Sensewrap: A service oriented middleware with sensor virtualization and self-configuration," *in Proc. of Int. Conf. on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 261–266.

[22] Alam, I. et al., (2019). "IoT Virtualization: A Survey of Software Definition and Function Virtualization Techniques for the Internet of Things," pp. 1–30. [Accessed05-May,2019].[Online].Available https://arxiv.org/abs/1902.10910v1

[23] Marino, F. et al., (2017). "Towards softwarization in the iot: integration and evaluation of t-res in the onem2m architecture", *in Proceedings of the 2017 IEEE Conference on Network Softwarization (NetSoft)*, Bologna,Italy,pp.1–5,doi: 10.1109/NETSOFT.2017.8004202.

[24] Fichera, S. Gharbaoui, M. Castoldi, P. Martini, B. Manzalini, A. (2017). "On experimenting 5g: testbed set-up for SDN orchestration across network cloud and iot domains", *in: Proceedings of the 2017 IEEE Conference on Network Softwarization (NetSoft)*, Bologna, Italy, pp. 1–6, doi: 10.1109/NETSOFT.2017. 8004245.

[25] Khazaei, H. Bannazadeh, H. Garcia, A.L. (2017). "End-to-end management of iot applications", *in Proceedings of the 2017 IEEE Conference on Network Softwarization (NetSoft)*, Bologna, Italy, pp. 1–3, doi: 10.1109/NETSOFT.2017. 8004252.

[26] Xiao, B.et al., (2016). "Intelligent data-intensive iot: A survey", *in Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, China, pp. 2362–2368, doi: 10.1109/CompComm.2016. 7925122.

[27] Batalle, J. Riera, J. F. Escalona, E.and Garcia-Espin, J. A. (2013). "On the implementation of nfv over an openflow infrastructure: Routing function virtualization," *in Future Networks and Services (SDN4FNS), IEEE SDN for. IEEE*, pp. 1–6.

[28] "Geant project: Software defined networking." 2017, [Accessed 05- May, 2019]. [Online]. Available: https://geant3plus.archive.geant.net/opencall/SDN/Pages/Home.aspx

[29] Maksymyuk, T. Dumych, S. Brych, M. Satria, D. and Jo, M. (2017). "An iot based monitoring framework for software defined 5g mobile networks," in Proc. of Int. Conf. on Ubiquitous Information Management and Communication. ACM, pp. 105:1–105:4.

[30] Zhang, W. Liu, G. Zhang, W. Shah, N. Lopreiato, P. Todeschi, G. Ramakrishnan, K. and Wood, T. (2016). "Opennetvm: A platform for high performance network service chains," in Proc. of Int. Conf. Workshop on Hot Topics in Middleboxes and Network Function Virtualization. ACM, pp. 26–31.

[31] "Data plane development kit." [Accessed 05-May, 2019]. [Online]. Available: http://www.dpdk.org/

[32] Massonet, P. Deru, L. Achour, A. Dupont, S. Croisez, L. M. Levin, A. and Villari, M. (2017). "Security in lightweight network function virtualization for federated cloud and iot," *in Proc. of Int. Conf. on Future Internet of Things and Cloud (FiCloud)*, pp. 148–154.

[33] Al-Shaboti, M. Welch, I. Chen, A. and Mahmood, M. A. (2018). "Towards secure smart home IoT: Manufacturer and user network access control framework," *in Proc. of Int. Conf. on Advanced Information Networking and Applications*, pp. 892–899.