A conceptual architecture for integrating software defined network and network virtualization with internet of things

Ali Haider Shamsan, Arman Rasool Faridi
Department of Computer Science, Faculty of Science, Aligarh Muslim University, Aligarh, India

Article Info

Article history:

Received Oct 28, 2021
Revised Jun 18, 2022
Accepted Jul 10, 2022

Keywords:

Internet of things
Network function virtualization
Network virtualization
Software defined network
Softwarization

ABSTRACT

Software defined network (SDN) and network function virtualization (NFV) are new paradigms and technologies of the network which support the best experience of providing functions and services, managing network traffic, and a new way of control. They support virtualization and separating data from control in network devices, as well as provide services in a software-based environment. Internet of things (IoT) is a heterogeneous network with a massive number of connected devices and objects. IoT should be integrated with such technologies for the purpose of providing the capabilities of dynamic reconfiguration with a high level of integration. This paper proposes a conceptual architecture for integrating SDN and NFV with IoT. The proposed work combines the three technologies together in one architecture. It also presents the previous works in this area and takes a look at the theoretical background of those technologies in order to give a complete view of proposed work.

Corresponding Author:

Ali Haider Shamsan
Department of Computer Science, Faculty of Science, Aligarh Muslim University
Aligarh, 202002, India
Email: ahtshamsan@myamu.ac.in

1. INTRODUCTION

The heterogeneity of internet of things (IoT) networks and devices standalone weakly because its components are designed to consume less power, no processing, and bits of data transmissions. IoT networks and devices with multiple protocols are utilized on a large scale with various ways of communication and data formats to connect addressable devices of IoT, either physical or virtual, in order to achieve various purposes through specific applications [1]. There is a difficulty of addressing IoT devices in traditional ways of legacy networks due to the heterogeneity of devices and various purposes. To solve this issue, IoT networks should integrate with other technologies to support flexibility, centralization, and dynamic configuration. The only technologies that support those features are network functions virtualization (NFV) and software defined network (SDN). So, the integration of IoT networks with SDN and NFV can guarantee these features and solve the addressing issues. The combination of SDN and NFV is called Softwarization which transforms the traditional ways of commutations and processing to the software-based environment with common-off-the-self (COTS) devices [2] by running various network services and functions on general-purpose hardware as a virtual machine (VM) instead of network hardware itself by decoupling hardware from functions, which is done by NFV [3]. Also, separating data and control planes, and centralize the controllers as part of SDN.

The network softwarization is integration of NFV and SDN to transform the components of the system and the process of telecommunications from traditional and legacy devices to general purposes devices. For a wide variety of services and activities through programmable network and virtualization [4],

[5] in a sufficient way with low cost of capital expenses (CAPEX) and operational expenses (OPEX) [6]. A new approach of networking which decouples controlling from data devices as separated planes and layers is called SDN. It centralizes the controller to facilitate managing, configuring, and controlling the network in a dynamic and softwareable environment [7]. It provides more flexibility and simplicity in deploying configuration and policies and managing the network through the controller which is centralized in control plane [8].

When dealing with the rapid expansion of networks, virtualization technology enables virtual infrastructure components which might be utilized and shared at a lower cost [9]. In order to supply network functions and services through general purpose devices [10], NFV virtualizes the infrastructure, and it enables the management of resources and the provision of network functions (NF), and also the function's ability to scale up and down on demand [3], [11]. In leverage of installing functions and services in a software-based and virtual environment, the time of creating services is reduced [12], and the network flexibility is improved [13].

Due to the characteristics of IoT, network needs to be more interoperable, flexible, and reliable. So, the best technological solution to achieve that is to integrate with SDN and NFV. IoT devices can be managed using virtualization and central controllers, and services and functionalities may be provided for IoT by integrating with the SDN and NFV frameworks [4], [14]. IoT sensors have low capabilities of configuration and less flexibility. A wireless sensor networks (WSN) is a vast network that needs to be operated, managed, and configured in high experienced technologies. Integrating IoT with SDN and NFV will improve the interoperability of protocols and IoT technologies. Moreover, providing network functions to facilitate controlling and managing of IoT with reduced effective cost as a result of using virtualization technologies [15], [16].

Therefore, functions are implemented as software in softwarization, which can respond to the changes smoothly and fulfill the requirement of services in the way of a software update. In softwarization, hardware becomes more independent by decoupling functionalities from it and providing functions as software [4], [17]. The IoT softwarization integrates NFV and SDN to manage IoT devices agilely. For that, SDN orchestrates the flow of IoT network centrally, while NFV supports delivering on-demand IoT network services [4]. Network softwarization empowered by SDN and NFV increases the storage and performance with cost saving. In that, IoT systems are impacted by softwarization that reshapes and creates new opportunities to eliminate limits and maintain borderlessness between the Internet and its elements. So, IoT devices act as an edge node of the network, which can store data and execute services and functions of the system locally [18].

This paper explores the possibilities of integrating NFV and SDN as a network softwarization with IoT. An architecture of integrating NFV and SDN with IoT is proposed conceptually as an extended version of our previous work [19]. The proposed architecture is designed by combining the architecture of three technologies. The proposed architecture is software-based IoT to enable various technologies and provide multiple functions that are not possible to be supplied in IoT networks without leveraging of other technologies. The architecture with its layers is defined and discussed in this work conceptually. This work is unique in merging NFV and SDN with IoT, irrespective of the architecture’s purpose, that could be used for numerous services in order to accomplish various tasks such as orchestration, management, security, and controlling. The terms "integration of SDN and NFV" and "network softwarization" are interchangeably used within the context of this paper. The rest of this paper is organized as follows: section 2 explores the related works in this field. Section 3 covers the proposed framework architecture that integrates SDN and NFV with IoT. Section 4 explain the research method is used in this work, while section 5 discusses the importance of the proposed architecture as compared to other works. Section 6 includes conclusion and future works.

2. RELATED WORKS

SDN and NFV have been combined with IoT in some previous works. Cerroni *et al.* [20] proposed a reference architecture for IoT concerning the standard framework European Telecommunications Standards Institute management and orchestration (ETSI MANO) for the purpose of managing and orchestrating IoT networks of heterogeneous devices. This architecture has separate virtual infrastructure managers (VIMs) for each SDN and IoT.

Salahuddin *et al.* [16] proposed an IoT healthcare system based on softwarization. The proposed architecture aimed to secure and agile the smart healthcare system. It uses blockchain and Tor along with SDN and NFV. This work emphasizes the healthcare system and how to be secure and benefited from softwarization and blockchain. This work is considered as conceptual, which has no implementation or simulation to validate the results. Both wireless sensor networks (WSNs) and unmanned aerial vehicles (UAVs), both of which are examples of applications that are included under the umbrella of the internet of things, use the architecture that is described in [18]. This work constructs an architecture of software virtualization using NFV and SDN in order to circumvent the limitations imposed by conventional networks and make full use of the general resource pool offered by virtualization as well as cloud computing services. The goal of this work is to circumvent the limitations imposed by conventional networks and make full use of the general resource pool offered by virtualization and cloud computing services.

Caraguay *et al.* [21] proposed using SDN/NFV for IoT networks to customize switch behavior in SDN networks. Their proposed architecture just combines both NFV and SDN technologies without including IoT network architecture. This work experiments quality of service (QoS) in SDN network through video streaming between hosts using Mininet SDN simulation and Floodlight controller.

The architecture proposed by Acharyya and Al-Anbuky [22] adopts the requirements of demand services by interacting between physical and virtual sensors network. This IoT architecture is intended to be managed remotely by cloud or servers. Ojo *et al.* [23] proposed an SDN-IoT architecture with NFV implementation, which can increase the efficiency and agility of the IoT network, as well as scalability and mobility. Its proposed architecture is built based on SD-IoT architecture concerning the virtualization of IoT framework.

Distributed IoT gateways with leveraging of NVF and SDN is proposed by Mouradian *et al.* [24] as an architecture of IoT for provisioning disaster management. This architecture supports the reuse of gateways and handling traffics between them. Alenezi *et al.* [25] coupled the two architectures of SDN and NFV in order to address IoT network issues. The proposed architecture supports COTS devices to be used to provide a variety of services and functions. This work analyzes the cost of using different ways of network whether traditional 4G network and softwarization network.

The work proposed by Farris *et al.* [26] copes the features of SDN and NFV to eliminate security threats in IoT. The security protection mechanisms are supposed to be provided by the proposed framework as integration between current security mechanisms of IoT and softwarized services of NFV and SDN. It supports interacting with various security technologies through the orchestration layer [27].

Islam *et al.* [28] proposed DistBlackNet which is an architecture of secure NFV and Black SDN-IoT for smart cities. This architecture is built on the basis of SDN-IoT architecture with an improvement of adding NFV. It is more effective in building clusters in helping of distributed controllers, which leads to get some benefits such as confidentiality, integrity, and energy saving.

Mukherjee *et al.* [29] proposed architecture of SDN-IoT with the implementation of NFV to support smart city applications of IoT. In order to manage the IoT network efficiently, this work introduces clustering as a practical approach with less power consumption. The proposed architecture increases the efficiency and flexibility of the network, and it supports the distribution of controllers.

The concept of “smart device-as-a-service” (SDaaS) is proposed by Atzori *et al.* [30] in order to replace the physical IoT devices to be as virtual. SDaaS is supposed to improve the virtualization services of physical devices such as scalability, flexibility, and reusability. For reducing the number of network hops in Fog, this work suggested that NFV infrastructure be deployed in the environment of Fog.

Zarca *et al.* [6], [31] proposed an architecture of IoT, which is based on SDN/NFV. The proposed architecture framework is used for the security management of IoT networks. It reacts dynamically against the security attacks and threats of IoT [32].

Omnes *et al.* [33] proposed an architecture of IoT, which is multi-layered with SDN and NFV. The proposed architecture, according to the authors is able to eliminate and cope with the challenges of IoT network. For that, NFV provides virtual network functions (VNF) services which are handled by virtualization infrastructure, and it provides a virtualized framework and orchestration. While SDN is used for addressing the service infrastructure as well as establishing the connectivity between virtualized functions.

Setiawan *et al.* [34] examine the 6LoWPAN performance of IoT device using the SDN paradigm. Mininet-IoT emulator is used along with the open network operating system (ONOS) controller (IoT) to examine the QoS. The performance of several topologies involving a host, switch, and cluster were evaluated. This work examines how to evaluate QoS performance in a sophisticated environment of IoT with complicated topologies with large number of hosts [35].

3. PROPOSED FRAMEWORK

The integration of technologies with IoT is the most crucial step to cope with the vast requirements of the smart environment. In this work, we propose a conceptual architecture of integrating SDN and NFV with IoT. The proposed architecture is composed of four main layers, and each layer of those main layers has sub-layers of the three technologies and the connections between them, as shown in Figure 1. In this particular piece of work, we are going to focus our attention exclusively on the structure of the building. On the other hand, a proof of concept of this conceptual architecture and the protocol stack will be presented in the upcoming version of this work, which may be the extended version. This version of the work is expected to be published soon. This functionality will eventually be added in the version that has not yet been released.

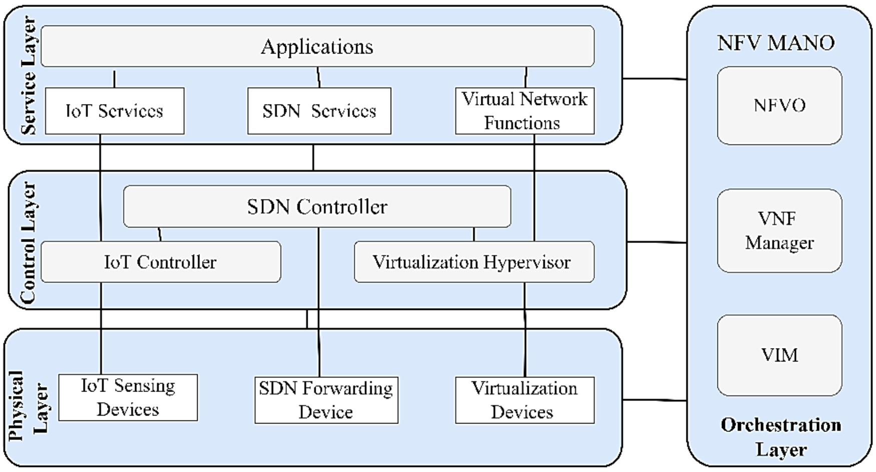

Figure 1. Conceptual architecture of integrating SDN & NFV with IoT

3.1. Physical layer

The internet of things, software-defined networking, and virtualization are a few examples of technologies that each include component types that are associated with hardware. These technologies are also good examples of technologies that include virtualization. These are just a few examples out of a much larger pool. Because it is the level that is the lowest in the network, the physical layer is where you will find each of these individual components.

3.1.1. IoT sensing devices

It contains the devices of IoT, such as sensing devices which sense the environment and collect the data and send it to the sink. The sink devices are the devices which are collecting data from various sensors through connected devices. A connection device may be built-in with sensors, or it may be attached to sensors and gateways.

3.1.2. SDN devices

In this layer, you will find the devices that belong to the data and forwarding planes of the SDN. It is the responsibility of these network devices, which include routers, switches, access points, and other similar devices, to build the flow table based on the dynamic rules and configurations that are made by controllers, and then to route and forward packets in accordance with the flow table that they have built. Examples of these network devices include routers, switches, and access points.

3.1.3. Virtualization hardware resources

This sub-layer is where the general-purpose devices, which are also known as COTS devices, that are considered to be virtualization's hardware resources are located. Also, this sub-layer is where the general-purpose devices are located. The networking, storage, and computing devices that are a part of the virtualization hardware infrastructure are the components that go into the construction of a resource pool for the virtualization infrastructure. This pool is one of the essential parts of the infrastructure.

3.2. Control layer

The control layer of our proposed architecture contains three sub-layers that are connected to each other, as well as connected to the physical layer. The sub-layers are responsible mainly for controlling their physical and data layer devices, and, secondly, they will integrate with each other and control the functions overly. Those layers are the SDN controller, IoT controller, and virtualization hypervisor.

3.2.1. IoT controller

IoT controllers are responsible for managing IoT devices whether they are for sensing or actuating. As mentioned earlier, IoT gateways may be considered as IoT controllers that may be installed on edge. The

IoT controllers can be a virtual controller in the leverage of NFV. The virtual controller may utilize the virtualized infrastructure to be fully functionalized with the capabilities of managing heterogeneous devices.

3.2.2. Virtualization hypervisor

The virtualization layer is considered as an interface between virtualization hardware devices and virtual service and functions. It is called virtualization hypervisor, which manages and controls the shared COTS and hardware resources to provide VNFs. It also offers controlling services for IoT as an IoT controller, and also it can provide a function to be used as an SDN controller.

3.2.3. SDN controller

SDN controller is responsible for controlling the whole network whether IoT devices controlled via IoT controllers, or virtualization through controlling Virtualization hypervisor as well as VNFs. It provides an abstract view of the devices in the physical layer, and the controllers in the control layer to the service layer. The controller is considered as the brain of the network. It has full permission authority of the network, so the configuration of all networks is done dynamically and remotely through controllers. Controllers can be distributed in different places, and they communicate each other through west/east-bound application programming interface (APIs) and communicate with data layers through southbound APIs. Northbound APIs are used to communicate with the service layer.

3.3. Service layer

The topmost layer of the architecture that we have proposed is called the service layer. It comprises IoT services, SDN services, and virtual network services and functions. In addition to the services, it provides the applications that correspond to each of these categories.

3.3.1. IoT services

The various services of IoT are provided and managed by this layer. Irrespective of the service, they are processed in this layer and data is sent to the cloud for storage. It communicates with the IoT controller to require specific functions performed by IoT devices that are needed by the user using applications. IoT applications are considered as an interface between IoT services and users.

3.3.2. SDN services

This layer is responsible for the management of a variety of services that are made accessible by the SDN. Load balancing, security, and a few other services are included in these offerings. Utilization of the northbound protocol is what enables communication to take place between these services and the SDN controller.

3.3.3. Virtual network functions

The hypervisor of the general-purpose hardware that is used for virtualization is the component that is in charge of providing the various virtual services and network functions that are required. The IoT and SDN can be combined in order to perform these functions. To satisfy the requirements that have been outlined for the system as a whole, it is possible to incorporate these capabilities with IoT and SDN, and doing so will be of assistance if it is done.

3.3.4. Applications

All IoT, SDN, and NFV applications are located in this layer and are presented as one of the applications. These applications are considered to be the user interface because they enable the user to interact with the system and the various services that it provides. This layer can also be referred to as the application layer.

3.4. Orchestration management layer

The orchestration layer consists of three types of managers which are VNF manager, virtual infrastructure manager (VIM), and NFV orchestration. This layer is responsible for managing the virtualization processes. For example, (VNFManager) manages the services of VNFs, VIM manages the infrastructure, and (NFVO) manages the whole NFV system and VNF life cycle as well as allocates the resources infrastructure for the provided services.

4. RESEARCH METHOD

In this study, network function virtualization and software-defined networking are integrated with the internet of things irrespective of the architecture's purposes and may be used to accomplish a variety of functions, such as security, monitoring and orchestration. The terms "integration of SDN and NFV" and "network softwarization" are interchangeably used within the context of this paper. IoT-based softwarization articles that have been published and mentioned in the related works sections are focused on a single problem rather than a comprehensive solution. Based on past research, the problem is addressed. Then, the solutions and their drawbacks are discussed. According to previous research, the proposed architecture is compared with prior works, as shown in Table 1. The prior works are aimed toward certain objectives, such as management, security, or disaster management. However, our proposed architecture is a general-purpose architecture based on the NFV, SDN, and IoT standard architectures. It may be used to deliver a wide variety of services by using the SDN and NFV resources. Additionally, the proposed architecture might serve as a reference model for IoT softwarization architectures.

Table 1. Comparison of proposed solution

Work	IoT	NFV	SDN	Performance improvement	Application independent
[20]	✓		✓	X	X
[16]	✓	✓	✓	X	X
[17]	X	✓	✓	X	X
[21]	X	✓	✓	X	✓
[22]	✓	✓	X	X	X
[23]	✓	✓	✓	X	✓
[24]	✓	✓	X	X	X
[25]	X	✓	✓	X	X
[26], [27]	✓	✓	✓	X	X
[28]	✓	✓	✓	X	X
[29]	✓	✓	✓	X	X
[6], [31], [32]	✓	✓	✓	X	X
[34]	✓	X	✓	✓	X
Proposed Architecture	✓	✓	✓	✓	✓

5. RESULTS AND DISCUSSION

All three SDN, NFV, and IoT technologies are represented in the proposed architecture. As opposed to other related efforts, they focused on integrating specific SDN and NFV layers with IoT. With the help of Table 1, we were able to compare the proposed architecture with currently conducted ones, and we also determined if it relied on SDN, NFV, or IoT. In addition, it is important to know if the solutions presented are general solutions or just application-wise solutions. The comparison demonstrates that the proposed architecture approach is superior to prior research in performance enhancement. SDN, NFV, and IoT are all included in the architecture proposed in this study. As a matter of fact, they had previously only integrated specific layers of NFV and SDN technologies with IoT.

The proposed work is suitable for various purposes, for example, management, security, and data flow. While the previous works were focusing on one or more specific of those purposes, for example study [16] proposed to use softwarization along with blockchain to secure a healthcare system, the study [36] proposed the NFV framework generally in IoT with using SDR as part of SDN. Still, the layers of the proposed solutions were based on the NFV architecture, while architecture proposed in this paper combines both SDN and NFV with IoT architecture. The proposed architecture suggests one VIM for all devices where study [20] proposed a separate VIM for IoT and SDN. All devices of the system, whether those devices are IoT devices or SDN devices as well as NFV devices, are managed by one VIM.

The proposed architecture has been built concerning the three technologies, while previous works were developed based on the architecture of one or two technologies. In [23], [28], [29], the architectures are built depending on SDN architecture or, more specifically, SDN-IoT architecture, while our architecture combined the three technologies architectures. The architecture of [25] is built in the form of NFV architecture, which shows that SDN devices are replaced with VM and the service with VNF. In [26], [27], the architecture is built depending on NFV architecture. The control plane of SDN is attached in management of NFV, while IoT devices mentioned in parallel with VM infrastructure. Moreover, the proposed architecture of work [21] just contained SDN and NFV, while it was mentioned that architecture as an IoT SDN/NFV. Also, in the experiment, IoT was not involved. On the other hand, our proposed architecture combines the three technologies in various layers. The proposed architecture of the is supposed to be more agile and flexible as this design is more general that can be applied anywhere in various applications and services for different purposes. It thereby solves the scalability issues of IoT networks. Nodes and new devices can be added easily, configured dynamically, and managed virtually.

6. CONCLUSION AND FUTURE WORKS

When it comes to providing functions and services in a manner that is both cost-effective and agile, the network softwarization that arises as a result of combining SDN and NFV is regarded as the best networking practice there. This is because it brings about the creation of network virtualization. The power of these technologies lies in their capacity to control the network as well as their ability to provide high-quality services on devices designed for general purposes by utilizing technologies related to virtualization. Both of these capabilities contribute to the power of these technologies.

To cope with the rapid evolution in technology fields, integrating technologies is the best idea that can help to overcome the insufficiency of one technology. In this regard, this work suggested the integration between SDN and NFV with IoT to cope with the insufficiency of the IoT network that has been designed with low capabilities. It proposed conceptually integrating the architecture of the three technologies which are SDN, NFV, and IoT. In other words, it can be referred to combining SDN and NFV to softwarization or network softwarization. So, this work can be clearly considered as integrating the softwarization with IoT.

This paper covered the theoretical background of the softwarization of SDN and NVF, and IoT, and the previous related works of integrating with IoT. Finally, we proposed our conceptual architecture of integrating softwarization with IoT. In this work the conceptual architecture has been discussed. This work seems promising and to prove that a proof of concept will be presented as an extended version of the paper. Also, the protocol stack of each technology will be presented as future work.

REFERENCES

[1] C. Mouradian, S. Kianpisheh, M. Abu-Lebdeh, F. Ebrahimnezhad, N. T. Jahromi, and R. H. Glitho, "Application component placement in NFV-based hybrid cloud/fog systems with mobile fog nodes," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 5, pp. 1130–1143, May 2019, doi: 10.1109/JSAC.2019.2906790.

[2] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: state-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, 2016, doi: 10.1109/COMST.2015.2477041.

[3] Y. T. Woldeyohannes, A. Mohammadkhan, K. K. Ramakrishnan, and Y. Jiang, "ClusPR: Balancing multiple objectives at scale for NFV resource allocation," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1307–1321, Dec. 2018, doi: 10.1109/TNSM.2018.2870733.

[4] B. Yi, X. Wang, K. Li, S. k. Das, and M. Huang, "A comprehensive survey of network function virtualization," *Computer Networks*, vol. 133, pp. 212–262, Mar. 2018, doi: 10.1016/j.comnet.2018.01.021.

[5] F. Marino, L. Maggiani, L. Nao, P. Pagano, and M. Petracca, "Towards softwarization in the IoT: Integration and evaluation of t-res in the oneM2M architecture," in *2017 IEEE Conference on Network Softwarization (NetSoft)*, Jul. 2017, pp. 1–5, doi: 10.1109/NETSOFT.2017.8004202.

[6] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, "Enhancing IoT security through network softwarization and virtual security appliances," *International Journal of Network Management*, vol. 28, no. 5, Sep. 2018, doi: 10.1002/nem.2038.

[7] E. Haleplidis, S. Denazis, J. H. Salim, O. Koufopavlou, D. Meyer, and K. Pentikousis, "SDN layers and architecture terminology," vol. RFC7426. pp. 1–35, 2015. Accessed: Oct. 15, 2021. [Online]. Available: http://tools.ietf.org/html/draft-haleplidis-sdnrg-layer-terminology-04.

[8] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, "Integrated NFV/SDN architectures: A systematic literature review," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–39, Nov. 2019, doi: 10.1145/3172866.

[9] A. J. Gonzalez, G. Nencioni, A. Kamisinski, B. E. Helvik, and P. E. Heegaard, "Dependability of the NFV orchestrator: State of the art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3307–3329, 2018, doi: 10.1109/COMST.2018.2830648.

[10] S. Il Kim and H. S. Kim, "Semantic ontology-based NFV service modeling," in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, Jul. 2018, pp. 674–678, doi: 10.1109/ICUFN.2018.8436738.

[11] B. Zhang, P. Zhang, Y. Zhao, Y. Wang, X. Luo, and Y. Jin, "Co-Scaler: Cooperative scaling of software-defined NFV service function chain," in *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Nov. 2016, pp. 33–38, doi: 10.1109/NFV-SDN.2016.7919472.

[12] M. Xie, C. Banino-Rokkones, P. Gronsund, and A. J. Gonzalez, "Service assurance architecture in NFV," in *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Nov. 2017, pp. 229–235, doi: 10.1109/NFV-SDN.2017.8169881.

[13] Y. Cheng, L. Yang, and H. Zhu, "Deployment of service function chain for NFV-enabled network with delay constraint," in *2018 International Conference on Electronics Technology (ICET)*, May 2018, pp. 383–386, doi: 10.1109/ELTECH.2018.8401407.

[14] S. Chen, H Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 349–359, Aug. 2014, doi: 10.1109/JIOT.2014.2337336.

[15] Á. L. V. Caraguay, A. B. Peral, L. I. B. López, and L. J. G. Villalba, "SDN: Evolution and opportunities in the development IoT applications," *International Journal of Distributed Sensor Networks*, vol. 10, no. 5, May 2014, doi: 10.1155/2014/735142.

[16] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of internet of things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, May 2017, doi: 10.1109/MC.2017.195.

[17] S. Mahmoud, I. Jawhar, N. Mohamed, and Jie Wu, "UAV and WSN softwarization and collaboration using cloud computing," in *2016 3rd Smart Cloud Networks & Systems (SCNS)*, Dec. 2016, pp. 1–8, doi: 10.1109/SCNS.2016.7870554.

[18] H. Khazaei, H. Bannazadeh, and A. Leon-Garcia, "End-to-end management of IoT applications," in *2017 IEEE Conference on Network Softwarization (NetSoft)*, Jul. 2017, pp. 1–3, doi: 10.1109/NETSOFT.2017.8004252.

[19] A. H. Shamsan and A. R. Faridi, "Network softwarization for IoT: A survey," in *Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development, INDIACom 2019*, 2019, pp. 1163–1168.

[20] W. Cerroni *et al.*, "Intent-based management and orchestration of heterogeneous openflow/IoT SDN domains," in *2017 IEEE*

Conference on Network Softwarization (NetSoft), Jul. 2017, pp. 1–9, doi: 10.1109/NETSOFT.2017.8004109.

[21] Á. L. V. Caraguay, 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*, 2018, pp. 425–429, doi: 10.5220/0007234804250429.

[22] I. S. Acharyya and A. Al-Anbuky, “Towards wireless sensor network softwarization,” in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, Jun. 2016, pp. 378–383, doi: 10.1109/NETSOFT.2016.7502470.

[23] M. Ojo, D. Adami, and S. Giordano, “A SDN-IoT architecture with NFV implementation,” in *2016 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6, doi: 10.1109/GLOCOMW.2016.7848825.

[24] C. Mouradian, N. T. Jahromi, and R. H. Glitho, “NFV and SDN-based distributed IoT gateway for large-scale disaster management,” *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 4119–4131, Oct. 2018, doi: 10.1109/JIOT.2018.2867255.

[25] M. Alenezi, K. Almustafa, and K. A. Meerja, “Cloud based SDN and NFV architectures for IoT infrastructure,” *Egyptian Informatics Journal*, vol. 20, no. 1, pp. 1–10, Mar. 2019, doi: 10.1016/j.eij.2018.03.004.

[26] 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)*, Sep. 2017, pp. 169–174, doi: 10.1109/CSCN.2017.8088617.

[27] I. Farris, T. Taleb, Y. Khettab, and J. Song, “A survey on emerging SDN and NFV security mechanisms for IoT systems,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 812–837, 2019, doi: 10.1109/COMST.2018.2862350.

[28] M. J. Islam, M. 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)*, Feb. 2019, pp. 1–6, doi: 10.1109/ECACE.2019.8679167.

[29] B. K. Mukherjee, S. I. Pappu, M. J. Islam, and U. K. Acharjee, “An SDN based distributed IoT network with NFV implementation for smart cities,” in *2nd International Conference on Cyber Security and Computer Science (ICONCS 2020)At: Daffodil International University, Dhaka*, 2020, pp. 539–552.

[30] L. Atzori *et al.*, “SDN & NFV contribution to IoT objects virtualization,” *Computer Networks*, vol. 149, pp. 200–212, Feb. 2019, doi: 10.1016/j.comnet.2018.11.030.

[31] A. Molina Zarca *et al.*, “Security management architecture for NFV/SDN-aware IoT systems,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8005–8020, Oct. 2019, doi: 10.1109/JIOT.2019.2904123.

[32] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, “Managing AAA in NFV/SDN-enabled IoT scenarios,” in *2018 Global Internet of Things Summit (GIoTS)*, Jun. 2018, pp. 1–7, doi: 10.1109/GIOTS.2018.8534551.

[33] N. Omnes, M. Bouillon, G. Fromentoux, and O. Grand, “A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges,” in *2015 18th International Conference on Intelligence in Next Generation Networks*, 2015, pp. 64–69, doi: 10.1109/ICIN.2015.7073808.

[34] D. Y. Setiawan, S. Naning Hertiana, and R. M. Negara, “6LoWPAN performance analysis of IoT software-defined-network-based using mininet-Io,” in *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, Jan. 2021, pp. 60–65, doi: 10.1109/IoTaIS50849.2021.9359714.

[35] A. H. Shamsan and A. R. Faridi, “A Novel SDNFV IoT Architecture Leveraging Softwarization Technology Services to Alleviate IoT Network Resource Restrictions,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 2, pp. 1–10, Feb. 2022, doi: 10.14445/22315381/IJETT-V70I2P201.

[36] T. Ahmed, A. Alleg, and N. Marie-Magdelaine, “An architecture framework for virtualization of IoT network,” in *2019 IEEE Conference on Network Softwarization (NetSoft)*, Jun. 2019, pp. 183–187, doi: 10.1109/NETSOFT.2019.8806650.

BIOGRAPHIES OF AUTHORS

Ali Haider Shamsan iD 8 SC ◐ pursed Bachelor of Computer Network Technology Engineering (CNET) from Sana’a Community College SCC, Sana’a, Yemen in 2012 and Master of Computer Science from Kakatiya University in year 2017. He is currently pursuing Ph.D. in Department of Computer Sciences, Faculty of Science, Aligarh Muslim University, Aligarh, India since 2018. His main research work focuses on internet of things, software defined network, network virtualization, and computer network. He has 2 years of teaching experience and 1 year of research experience. He can be contacted at email: ahtshamsan@myamu.ac.in.

Arman Rasool Faridi iD 8 SC ◐ was born in Gaya, Bihar, India, in 1971. He received the Master in Computer Science and Application degree in 1996 and a Ph.D. degree in 2017 from Aligarh Muslim University (AMU), Uttar Pradesh, India. From 1998 to 2005, he was Lecturer in the Department of Computer Science, AMU, Aligarh Uttar Pradesh, India. Since 2006 he has been working as an Assistant Professor of Computer Science. He is Deputy Director of Online Courses, Centre for Distance Education, AMU. He has contributed six chapters in a book published by CDE, AMU. He has published more than twenty articles in various journals and conferences. His research interests include E-Learning, information retrieval, IoT, Blockchain Technology, and Soft Computing. Dr. Faridi was a recipient of the prestigious President of India, Dr. Shankar Dayal Sharma Gold Medal. He can be contacted at email: ar.faridi.cs@amu.ac.in.