Computer Communications 169 (2021) 129–153

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

SDN/NFV architectures for edge-cloud oriented IoT: A systematic review

Partha Pratim Ray [a], Neeraj Kumar [b,c,*]

[a] Department of Computer Applications, Sikkim University, India
[b] School of Computing, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India
[c] Thapar Institute of Engineering and Technology, Patiala, India

ARTICLE INFO

Keywords:
SDN
NFV
IoT
Edge
Cloud
Architecture

ABSTRACT

Software-defined network (SDN) and network function virtualization (NFV) have entirely changed the way internetwork backhaul should be utilized and behaved for virtualized service provisioning. Several benefits have been observed in multiple domains of applications that has used SDN and NFV in integrated way. Thus, SDN/NFV paradigm has been investigated to seek whether network services could be efficiently delivered, managed, and disseminated to the end users. Internet of Things (IoT) is justifiably associated with the SDN/NFV augmentation to make this task enriched. However, factors related to edge-cloud communication and network services have not been effectively mitigated until now. In this paper, we present an in-depth, qualitative, and comprehensive systematic review to find the answers of following research questions, such as, (i) how does state-of-the-art SDN/NFV architecture look like, (ii) how to solve next generation cellular services via architecture involvement, (iii) what type of application/test-bed need to be studied, and (iv) security framework should be catered. We further, elaborate various key issues and challenges in the existing architecture mitigation for SDN/NFV integration to the IoT-based edge-cloud oriented network service provisioning. Future directions are also prescribed to support fellow researchers to improve existing virtualized service scenario. Lessons learned after performing comparative study with other survey articles dictates that our work presents timely contribution in terms of novel knowledge toward understanding of formulating SDN/NFV virtualization services under the aegis of IoT-centric edge-cloud scenario.

Contents

* Corresponding author at: Thapar Institute of Engineering and Technology, Patiala, India.
E-mail addresses: ppray@cus.ac.in (P.P. Ray), neeraj.kumar@thapar.edu (N. Kumar).

https://doi.org/10.1016/j.comcom.2021.01.018
Received 30 January 2020; Received in revised form 8 June 2020; Accepted 3 January 2021
Available online 28 January 2021

1. Introduction

1.1. Background

Edge-cloud interplay has become an utmost requirement now-a-days for facilitation of low-time consuming processing of any network related activities, thus a holistic improvement of current users' experience level [1,2]. SDN and NFV are such technologies which can closely work together to enhance the edge-cloud interplay scenario [3,4]. Myriad of studies and investigations have been performed to seek how SDN/NFV combination could be efficiently utilized for betterment of edge-cloud communication and service ecosystem [5,6].

SDN refers to the process of separation of the network control functions apart from the available network forwarding functions. NFV deals with the method of abstract of network functions on top of the hardware that act as the key elements of running the network operations. Main difference between SDN and NFV is that SDN performs over the NFV infrastructure in the network. SDN helps to transmit packets from one network device to other [7]. The background tasks of SDN are controlled by a remote virtual machine placed anywhere in the network. SDN provides facilities to run network policy functions and routing related jobs, whereas NFV orchestrate network functions rather than just controlling those. Programmatic behavior mitigation and run time configuration are achieved by the SDN itself. Most of the times, both the SDN and NFV leverage network architectures to be more flexible and dynamic in nature. They differ in the way how the network architectures are defined and to be supported on. Moreover, SDN deals with the process of abstraction of the physical elements responsible for networking. Overall decision making is served by the

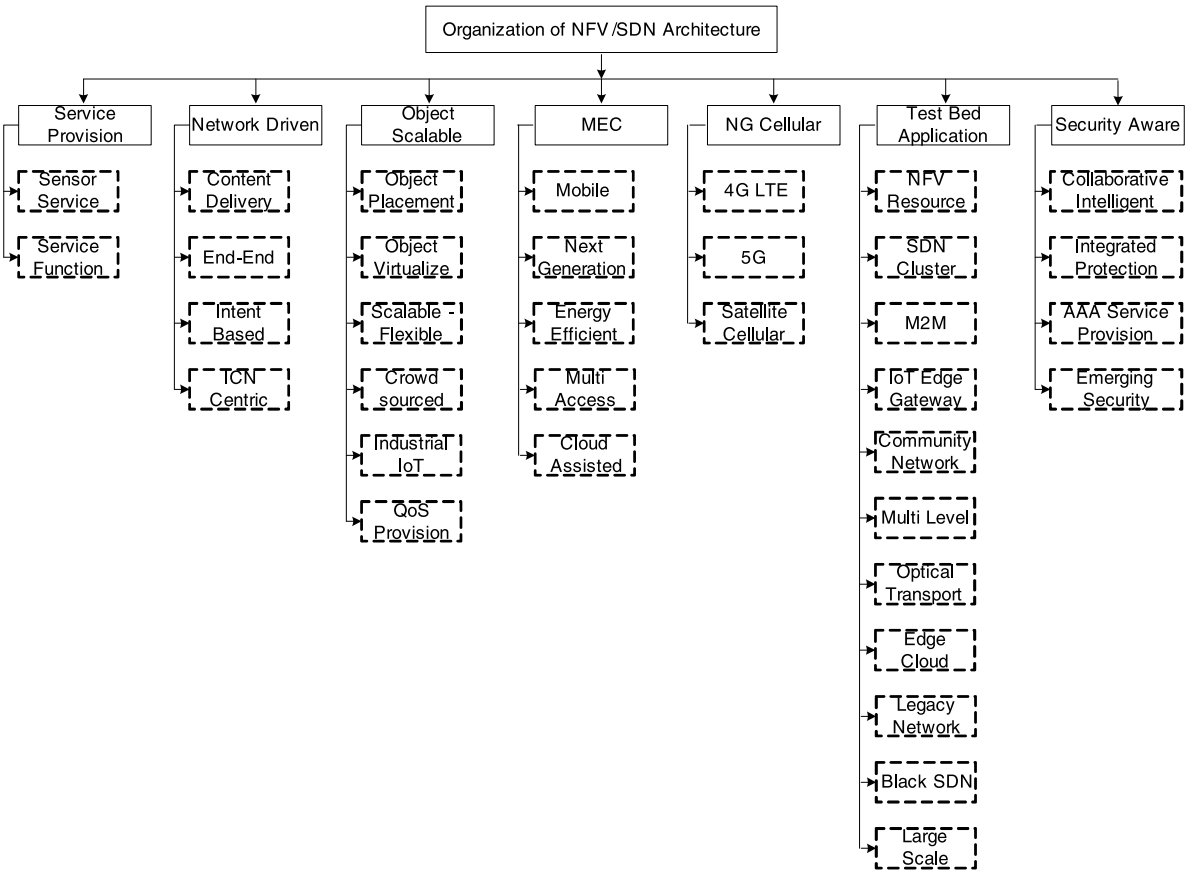

Fig. 1. Organization of the IoT-based edge-cloud orientation for SDN/NFV ecosystem architecture.

virtual machine running on the control plane. SDN invokes control plane to take decision about the routing of packets within the network whereas networking hardware just handles the data traffic [8]. NFV enables visualization of the physical elements of the network so that scalability can be achieved without using excessive network elements.

Thus, integration of SDN and NFV would aim at minimizing the operational cost of the network and improve service mitigation facilities. Moreover, an opportunity of enhancement of overall dynamic behavior of the network might be comprehended. Efficient integration of SDN and NFV would reduce dependency on the network physical components that improving security prospects. In this context, integration of edge and cloud platforms would be beneficial under the internet of things plethora. As more number of network devices will grow more expansion of physical layer would be perceived. We could aim to design an architecture that would allow a portion of cloud services might be dragged to the edge platforms where smart devices are connected. In such scenario, packets coming from the smart devices might be served with appropriate decision-making algorithms deployed at the edge without forwarding them to cloud controller. This might result in improvement of quality of service and minimize the security issues as only a portion of packets would need to be served by the cloud engines. We need to cater the integration of edge and cloud along with the internet of things to harness the key qualities from both the SDN and NFV in seamless manner.

Edge computing is a recent inclusion into the computing domain that is envisioned to bring a set of network services closer to the user which were earlier accessible but from far of user's reach i.e., cloud. Edge computing has shown promising behavior in terms of (i) minimization of delay during communication between two nodes in network, (ii) versatile network-wise service selection, (iii) reliable presence of network services, (iv) scalable orientation of networking infrastructure, and (v) security of end networking device pool. Thus, recent trend has shifted the mindset of enterprises to pave the cloud-based services to the customers at the edge level so that user can get best quality networking services [9].

A number of interventions of latest technologies have already begun to get incorporated in this regard and started to benefit many applications in different fields, such as, healthcare, agriculture, elderly emergency service, transportation, smart city, and industry [10–21]. 5G, next generation internet, tactile internet, and fog computing have been merged with the stated aspect to leverage futuristic network service provisioning.

IoT is such a genre of advanced technology that has proven itself to convert the existing society into smarter one. Many works have been carried out to seek whether IoT is good candidate for service mitigation between edge and cloud. IoT has successfully facilitated this worry with high level of interoperability, heterogeneity, and scalable distributed features. SDN/NFV paradigm has also been tested against IoT to deliver high quality network facilities to the users. Research has been conducted to integrate the SDN/NFV with IoT so that edge-cloud pathway centric services could be realized. Security, core packetization, cellular mobile, and programming logics are already validated and specifically justified by recent researches. Vertical silo-oriented architectures are also studied and implemented.

In this context, an IoT-based edge-cloud orientation refers a scenario where IoT-based device pool and services are paved through the amalgamation of edge and cloud in seamless manner. Usually, IoT-based systems are highly dependent on the cloud-based data centers for harnessing distributed applications. IoT sensor data is permanently stored and analyzed in the cloud servers based on which some actuation or decision is made. However, edge computing is meant to deliver cost effective and minimum-delay aware services to the end the users of a network. We may thus think of connecting edge with the cloud services in such way so that IoT-based sensor might provide the data directly to

the edge servers which are geographically closely positioned, resulting instantaneous service mitigation instead of traveling an uncertain, and vulnerable path to and from the remote cloud servers. However, this approach does not deter the IoT sensors to get served by the powerful and resourceful services form the cloud data centers. In the situation when the requested service to the local edge is not performed well, the same might then go to the cloud servers for efficient performance comprehension.

1.2. Contributions

Thus, contributions of this review can be summarized as follows:

- Depiction, in-depth study, survey, and discussions about SDN/NFV architectures for edge-cloud assisted incorporation to IoT
- Deliberation of architectures for next generation network virtualization servicing, development of application/test-beds, and security framework
- Discussions about key challenges and leveraging of future directions for architecture-based virtual IoT-service mitigation by using edge and cloud interaction

1.3. Organization

Rest of the paper is organized as follows. Section 2 presents SDN/NFV centric IoT edge-cloud service provisioning architectures. Section 3 presents network driven architectures in SDN/NFV oriented ecosystem. Section 4 discusses object scalable and flexible architecture inculcating SDN/NFV in IoT perspective. Section 5 presents mobile edge cloud integration for IoT based SDN/NFV architectures. Section 6 presents next generation cellular networking architectural dimensions. Section 7 deals with novel test bed and application architectures. Section 8 discusses various security architectures in protection of futuristic SDN/NFV wise IoT-based edge-cloud integration. Section 9 depicts open challenges and future directions to progress the pathway. Section 10 presents related works and comparisons between present work with existing literature. Section 11 concludes the review work. Table 1 shows the key abbreviations and their full forms used throughout the paper. Fig. 1 shows the organization the IoT-based ecosystem for SDN/NFV architectural aspect incorporating edge and cloud interplay.

2. Related works

2.1. Literature survey and analysis

This section presents related works performed in recent past to provide comprehensive approach and understanding for SDN/NFV orchestration for edge-cloud interplay, especially considering IoT as a key enabler. We searched IEEE Xplore, Sciencedirect, Google scholar, and Springerlink databases to best match other survey/review articles to correlate to our study. We used following keyword and phrases while searching the articles that includes, (i) "SDN + NFV + IoT", "SDN + NFV + IoT + Architecture", (ii) "SDN + NFV + IoT + Edge + Architecture", (iii) "SDN + NFV + IoT + Edge computing", (iv) "SDN + NFV + IoT + Edge + Cloud", (v) "SDN + NFV + IoT + Architecture", and (vi) "SDN + NFV + IoT + Edge + Cloud + Architecture".

Such systematic approach gave a total of 21 articles. Out of which, we selected 19 papers for establishing the significance and uniqueness of our work. The selection was based on following parameters, such as, (i) survey/review articles, (ii) covering SDN/NFV as key topic, (iii) possible association with IoT, (iv) edge-cloud interaction, and (v) architecture wise deployments, classifications, contributions, and discussions.

We present Table 2 that shows the comparisons between all such papers while taking four key aspects into considerations, that includes(i) techniques/ technology/ topics Surveyed, (ii) IoT compatibility, (iii) architecture survey, and (iv) major contributions.

Nguyen et al. [22] surveyed mobile network-based architectures suitable for SDN centric 4G-LTE mobile backhaul networks. This study was not compatible to IoT directly due to its main biasness for SD-VMN architecture designed for efficient utilization of SDN/NFV in this

Table 1
Acronyms and abbreviations.

AAA	Authentication, Authorization, and Accounting
ACM	Adoption, Configuration and Management
ANF	Applicative Network Function
CAPI	Communication cum API Integration
CDF	Continuous Delivery Framework
CDPI	Control-to-Data Plane Infrastructure
CDN	Content Delivery Network
CI/CD	Continuous Information/Delivery
D2D	Device-to-Device
DPWS	Device Profile for Web Services
DVS	Deployed Virtual Switch
E2E	End-to-End
EAP	Extensible Authentication Protocol
EDC	Edge Data Center
GFS	Gateway Function Store
GOM	Gateway Overlay Manager
GTP	GPRS Tunneling Protocol
ICM	Information Consumer
ICN	Information Centric Network
ILP	Integer Linear Program
IoT	Internet of Things
IoT-VM	IoT-based Virtual Machine
ISA	IoT-based Service Abstraction
LLCF	Local Content Caching Function
LRRF	Local Request Resolution Function
LSC	Local SDN Controller
MAEC	Multi-Access Edge Computing
MANO	Management and Network Orchestration
MAPE	Monitoring, Analysis, Pacification and Execution
MME	Mobility Management Entity
MRCF	Multi RAN Function
MSN	Mobile Social Networking
NBI	North Bound Interface
NCLS	Network Controlled Logic Software
NDSF	Network Device Specialized Function
NEV	Network Element Virtualization
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
NMS	Network Management System
NSF	Network Security Function
NSH	Network Service Header
ONOS	open Network Operating System
OPEX	Operation Expenses
OTA	Over-the-air
OSS	Operation Support System
OVS	Open Virtual Switch
PAA	Privileged-Level Access Agreement
pCPE	Physical CPE
PCRF	Policy and Charging Rules Function
PCS	Packet-level Security
PDP	Policy Decision Point
PEC	Placement the Edge and Cloud
RAN	Radio Access Network
RSN	Routing, Slicing, and Naming
SAVI	Smart Applications on Virtualized Infrastructure
SBI	South Bound Interface
SFC	Service Function Chain
SDN	Software Defined Network
SDVMN	SDN-based Virtual Mobile Network
SFC	Service Function Chaining
SLA	Service Level Agreement
SPN	Software-Programmed Networking
TINBR	Topology Independent Name-based Routing
uCPE	Universal Customer Premises Equipment
UNI	User to Network Interface
VIM	Virtual Infrastructure Manager
VIRM	Virtual Infrastructure Resource Manager
VNFM	Virtual Network Function Manager

Table 2
Comparison between related survey literatures.

Paper	Techniques/Technology/Topic surveyed	IoT compatibility	Architecture	Major contributions
Nguyen et al. [22]	SDN, LTE, SDVMN, NFV, RAN, Mobile Backhaul Network, RRS	Not Mentioned	Mobile Networks Architecture	SDVMN architecture study, hierarchical taxonomy for SDN/NFV, SDN/NFV protocols, Use cases of SDVMN study, Benefits of SDVMN to mobile cellular networks
Farris et al. [23]	SDN, NFV, IoT	Yes	SDN/NFV for IoT Security Architecture	SDN security threats for IoT, NFV security threats for IoT, Open research areas
Yan et al. [24]	SDN, DDoS	Not Mentioned	DDoS SDN Attack Architecture	SDN and Cloud computing related DDoS attack classification, Open challenges and broader prospects
Trois et al. [25]	SDN, SDN Programming languages	Not Mentioned	SDN Programming Logic	SDN programming languages study, Comparison, Discussion, and Open issues
Hantouti et al. [26]	SDN, SFC, NFV, SFC traffic steering	Not Mentioned	SFC Architecture	SDN based SFC comprehensive study, Qualitative evaluation, Open challenges, and Future direction
Salman et al. [27]	SDN, NFV, IoT, Mobile Networks	Partially	SDN-IoT Fog computing Architecture	SDN standards, platforms, security, privacy study, IoT-big data, Open issues and future direction
Bizanis et al. [28]	SDN, NFV, IoT, 5G, WSN	Partially	Generic SDN framework	SDN IoT for cellular network, WSN and 5G study, Framework study
Alam et al. [29]	SDN, NFV, IoT	Partially	SDN architecture	SDN ecosystem for IoT study, NFV for IoT study, and Future direction
Binfim et al. [30]	SDN, NFV	Not Mentioned	SDN/NFV architecture	SDN/NFV integration study, Mobile and wireless network support for multi-tenancy, Future direction
Cox et al. [31]	SDN, NFV, SDWN, 5G, RAN, ICN, SDX	Not Mentioned	Generic SDN study with NV integration	SDN tools and comparative study, Emerging technology discussion, Future direction
Zhao et al. [32]	SDN, NFV, Edge computing, C-RAN, IoT	Not Mentioned	SDN/RAN Edge architecture	SDN/RAN for Edge computing study, Applications discussions
Nguyen et al. [33]	SDN, NFV, Evolved packet core (EPC), MPC	Not Mentioned	SDN EPC architecture	SDN/NFV architecture for EPC, Technology adoption strategy, Taxonomy, Future direction
Saif et al. [34]	SDN, NFV, 5G, Mobile backhaul	Not Mentioned	SDN Solution architecture	SDN solution classifications study, 5G, Mobile backhaul study
Wang et al. [35]	SDN, NFV, MEC, CDN, D2D	Not Mentioned	SDN MEC architecture	SDN MEC offloading, Use cases, Key enablers study, Open issues, Direction
Gil et al. [36]	SDN, NFV, NGN, Mobile networks	Not Mentioned	SDN NGN architecture	SDN-NGN technology study, Analysis, Future direction
Mijumbi et al. [37]	NFV, Cloud, Future internet, VNF	Not Mentioned	NFV generic architecture	NFV project, data models, security threats, energy efficiency, Research challenges
López et al. [38]	NFV, SDN	Not Mentioned	NFV SDN generic architecture	NFV projects, Discussions
Aguessy et al. [39]	SDN, NFV, Cyber attacks	Not Mentioned	SDN attack architecture	SDN attack types, discussion, analysis
Pandeeswari et al. [40]	SDN, Fog computing,	IoT Partially	SDN fog-IoT computing architecture	Generic SDN fog discussion
Proposed Work	SDN, NFV, Cloud computing, Edge computing, Fog computing,	Full IoT	Discussion of all types of SDN/NFV architectures	Complete discussion about architectures, analysis, challenges and future direction, comprehensive survey

domain of research. Farris et al. [23] targeted IoT as beneficiary of their study where security related issues and architectures were only elaborated and analyzed. This study also provided important security threats in SDN-based IoT scenarios. No other types of avenues were depicted in this work. DDoS attack is a severe element in current networking domain.

Thus, Yan et al. [24] surveyed DDoS attack mitigation architectures while taking SDN as key entity in their study. All the architectures were based on DDoS and SDN centric. Trois et al. [25] surveyed various languages and related platforms which may play important role for SDN programming in purely virtual manner.

On the other hand, Aguessy et al. [39] just discussed few SDN attack mitigation architecture. No detailed comprehension was provisioned in this work. Hantouti et al. [26] paved a detailed study on SFC programming features under the aegis of SDN architecture. They also provided comparative and open research challenges in this regard.

Samlan et al. [27] aimed their study toward fog enablement with SDN-based architectures. Their study included SDN-centric open standards for creating fog-based services and IoT-based big data dissemination. However, Bizanis et al. [27] and López et al. [38] surveyed generic SDN architectures to relate IoT-based cellular network and WSN-5G integration in their study.

Similarly, Alam et al. [29] provided investigation of SDN/NFV integration for IoT centric architectures. This study was concisely designed to show how SDN/NFV could be benefit IoT by incorporating new types of architectures.

Binfim et al. [30] paved support for SDN/NFV ecosystem for IoT-based mobile and wireless network facility provisioning. Generic SDN-based comparative was formulated by Cox et al. [31]. Their work involved RAN, ICN, SDX and SDWN into the scope while discussing about architectural prospects. Ran and SDN were seamlessly integrated in various studies in recent past.

The same was showed in the article by Zhao et al. [32]. This work concentrated the utilization of SDN for edge-centric approaches while involving RAN and its variants for actual application in telcos-based service scenario. Nguyen et al. [33] focused the EPC-based architectures related to SDN networking aspects. Related technology adoption features were discussed in this work.

SDN solution architecture were mitigated by Saif et al. [34]. They classified 5G and mobile backhaul in terms of SDN. Edge computing

is may play important role in SDN/NFV framework realization. Thus, Wang et al. [35] surveyed MEC architecture for efficient offloading in the underlying network scenario. Next generation networking was subsequently investigated with SDN to analyze and provide future directions by Gil et al. [36].

Security and threats on SDN/NFV enabled network systems were surveyed by Mijumbi et al. [37] where energy efficient future generation internetworking service provisioning was discussed. Pandeeswari et al. [40] provided SDN and fog assisted IoT centric architectural views to facilitate the progress of existing fog-enabled IoT systems. Table 9 presents the comparative analysis between the reviewed studies.

3. Existing challenges

3.1. Interoperability

SDN/NFV aspect inherits interoperability features that varies I form of network functions, virtualization concepts, and platform dependent behavior. Inclusion of IoT has made this list of interoperable features longer. Due to amalgamation of heterogeneous technologies ranging from edge, fog, cloud, cloudlets, and MEC the task has become more difficult than ever [27]. Under the periphery of edge-cloud interplay, existing SDN/NFV formulation for IoT is not stringent enough to serve all types of facilities in efficient manner. Such type of interoperability should be tackled with immense importance by combining of hybrid horizontal–vertical segments of novel layered architecture.

3.2. Compatibility

Being heterogeneous, SDN/NFV conjunction to IoT has emerged as a challenging task. Due to the incompatible service provisioning into the existing layered centric architectural approaches, issues behind compatibility sometimes get missed out. That results into a chaotic situation for the heterogeneous networking services to get associated to the IoT-based aspect. Edge and cloud intercommunication are another hindering object that repels back the compatibility measures a step behind. It is hereby comprehended that compatibility within the layers of architecture and software tools should be precisely designed to advocate the optimum compatibility in the said ecosystem.

3.3. Reliability

Edge-cloud incorporation into the IoT-based envisaged aspect require to be highly reliable. Huge number of virtual services are regularly provisioned in the SDN/NFV augmented environment where IoT-based devices play very crucial role. Due to the resource constrained behavior of the IoT devices, it is hard to get reliable services all the time. Thus, futuristic networking system should involve more reliable algorithmic and architectural input so that software-defined facilities could be largely benefited.

3.4. Security

Security of any network system is a great challenge. It is true for the earlier discussed scenarios too. In recent past lots of vulnerable attacks and worm/malicious involvement and intrusions have been imposed over the IoT network. Thus, futuristic SDN/NFV enabled IoT must be architected in more robust manner so that security breaches could be minimized. In this regard, decentralized computing and advanced hybrid cryptographic techniques should be paved.

3.5. Gateway modeling

IoT gateways play very important role in propagating and translating the messages. Involvement of SDN/NFV perspective has brought new challenge to make the IoT gateways more intelligent and sophisticated but low cost and low power consumable so that a portion of the virtualization tasks could be directly facilitated from the IoT gateway itself. Thus, novel architectural design should be developed and tested against gold standard IoT-based high end protocols and computing systems so as to leverage quality communication services to its users.

3.6. Communication gap

Existing speed of communication signals is well enough to pursue regular activities, such as web service provisioning, cloud data access, security assignment etc. But, in coming days, the scenario is going to be different where low latency communication shall be highly desired [28]. Thus, 5G, 6G, and other hybrid communication technologies must be integrated with the IoT-based network backbone so that communication delay could be minimized. Further, SDN/NFV centric edge-cloud communication layers must be re-architected to lower the communication gap between the SBI and NBI elements.

3.7. Vulnerable IoT devices

IoT devices are normally resource constrained and lacks several capabilities, such as, computational power, memory, and high-end servicing. These limitations of the IoT devices make them a soft target to be called as vulnerable systems. More attention should be given to improve existing vulnerable situation of IoT devices by involving advanced mixed-signal processing modules, high-end 64-bit system on chip, solid state hard disks, and graphics processors [29]. Such incorporations would surely make those systems rigid in manner that would stay in the vulnerable state of work. Minimization of vulnerability in IoT devices will be of great importance in next years.

3.8. SDN/NFV edge platform

Existing SDN/NFV platforms are situation dependent, i.e. they are not independent on all types of architectural scenarios and neither platform agnostic. It makes problem when such facilities need to be aligned with the edge-cloud paradigm. Due to the huge communication gap and underlying differences between the deployed technologies, SDN/NFV conglomeration must be designed in more sophisticated manner. It is surely a difficult job to make such association technically advanced and paradigm agnostic. However, changes in architecture design layers may improve this condition in future.

3.9. Combined SDN-virtualization

Virtualization of networking services have been started since last decade. It has gained rapid speed in recent years. Though, many researches as discussed in earlier section have tried best to integrated SDN and NFV in seamless manner, on average the process was seen to be in preliminary or moderate level. There is still options available to make this integration more sophisticated and expand its actual strength for betterment of IoT-based services. Combination of SDN-NFV in edge-cloud ecosystem brings astonishing challenges which is not solved shall create system breakdown and inappropriate service mitigation in coming times.

4. Service provisioning architectures

4.1. Sensor service provisioning architectures

Due to specific behaviors e.g., application and manufacture, sensors are mainly used in very rigid form in IoT-based ecosystem with nominal programmable and reusable configuration capabilities. Thus, effective sensor service provisioning requires dynamic programmability which only be harnessed by conglomerating SDN and NFV. In [1], a novel

Table 3
Comparative analysis of service provisioning architecture.

Paper	Objective	Novel contributions	Advantages/Limitations
[1]	Software defined IoT architecture development	SD-IoT provisioning, SD-IoT architecture deployment and validation, designs, streamlines SD-IoT controller, SD-VSensor, and S-MANAGE protocol	High interoperability, efficiency, programmability, energy efficiency, multiple application utilization using underlying multiple sensors, lack of detailed specifications of modules used in SD-IoT architecture
[2]	Solves service function chaining using integer linear program	System model for SFC provisioning, objective function realization, tests on mesh network topology, proposed fog-to-cloud outperforms only cloud and ASP techniques	Minimizes end-to-end delay, realizes high band width between user device and cloud, effects number of instances in the fog-cloud scenario, physical implementation is not performed

architecture was presented and validated against the combination of three key components, such as, (i) software-defined IoT controller (SD-IoT), (ii) SD-VSensors, and (iii) S-MANAGE protocol. The architecture involved SDN and NFV while serving dynamic programmability of deployed virtual sensors place with help of SD-VSensors. Such architecture benefited the sensor service alignment in four ways, such as, (i) higher interoperability, (ii) programmability, (iii) energy efficiency, and (iv) efficiency in sensor data collection. The SD-IoT architecture paved three planes of abstractions that included (i) application plane, (ii) control plane, and (iii) data plane. Application plane served accommodation of IoT-based applications, whereas other two supported with processing capabilities in demand–response format and virtual sensor operation, respectively. The SD-IoT controller incorporated S-MANAGE protocol to communicate north bound interface (NBI) and south bound interface (SBI) with help of SD-VSensor, underlying sensors and resource management, configuration and sensor management attributes. S-MANAGAE was utilized by the SD-IoT controller to receive sensors centric services from SD-VSensor to configure the connection between IoT-based applications and SD-VSensor function and behavior. Moreover, two types of messages were facilitated in this scenario (i) message between SD-IoT and SD-VSensor and (ii) between SD-VSensor to SD-IoT. Four Raspberry Pi were used to implement the architecture that performed five different case studies (e.g., 1R-1SS-1SD-Vsensor, 1R-MSS-1SD-Vsensors, MR-1SS-1SD-Vsensor, MR-MSS-1SD-VSensor, and 1R-1SS-MSD-VSensor) to analyze the performance of the architecture where R, SS and M denotes request, sensor service, and multiple respectively. The study advocated proper utilization of sensor service provisioning under edge-cloud interplay where all sensors were placed at the edge devices and SD-IoT controller incorporated cloud-based services to mitigate IoT-based application scenario. Fig. 2 presents the SD-IoT architecture.

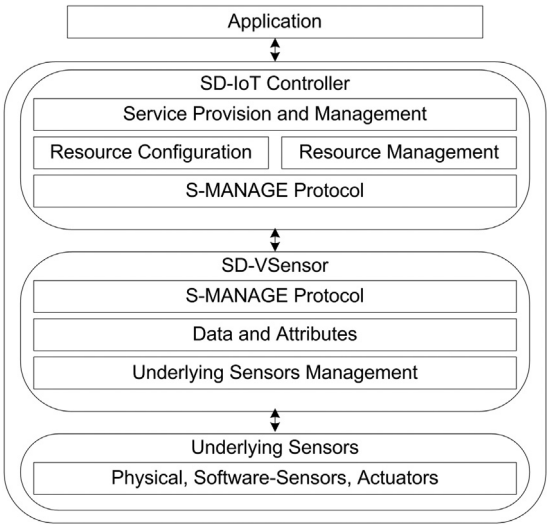

Fig. 2. SD-IoT architecture and its components.

4.2. Service function chain mapping framework

In last few years, IoT has emerged as ever-growing technology that is being applied in service function chain (SFC) mapping. In this task, IoT establishes communications between the edge to the cloud in seamless manner. However, such task requires compromise in terms of higher latency and higher bandwidth consumption. Thus, minimizing the actual aspect of getting efficient service function mapping in existing IoT domain. Recently a study a revealed the possibility of smarter SFC mapping by combining computational power, storage facilities, and a set of applications under edge-cloud scenario. In such technique [2]. A complex set of specific VNFs can be chained together to provide VNF traffic routing and placement under one networking plethora. The work deployed an integer linear program (ILP) model to minimize edge to cloud communication latency by using SDN and NFV together to improve the number of real-time instances by incorporating IoT-based devices. This study utilized service level agreement (SLA) along with the proposed ILP model to showcase its effectiveness to lower the overall latency in the deployed ILP architecture. The ILP model showed that overall latency could be minimized by increasing the number of SLA instances. Table 3 presents the comparative analysis of surveyed articles in terms of service provisioning architecture.

5. Network driven architecture

5.1. Content driven network framework

IoT provides a number of facilities starting from low end device level to high end cloud services. However, continuous integration and continuous delivery (CI/CD) framework is still in nascent stage of development. [3] developed a continuous delivery framework (CDF) between IoT-enabled edge devices and cloud by using SmartX-mini platform. The studies also performed data visibility operation under the aegis of development and operations (DevOps) aspect.

SmartX-mini is based on SDN, NFV, and edge-cloud integration plethora where IoT-based application can be efficiently developed. The proposed CDF started working after successful commit of software developer from the edge of the network. A Jenkins server was deployed to detect the real-time changes in the git repository (repo). The server later pulled the changed codes from the repo and loaded the correct codes on docker-based platforms. At the same time, Jenkins server instantiated one Jenkins slave that helped to build the docker image codes when necessary. The docker images were then transferred to cloud if they were found to be verified by the Jenkins server. Thus, a container-based CDF was formulated where services and communications between the edge of the network were paved with help of underlying docker, Jenkins and SDN/NFV integrated middleware. In this work, code quality verification was made by deploying JSLint, PEP8, and Pylint tools where PEP8 overperformed than other alternatives. 40 Raspberry Pi 2 were implemented with 13 Intel NUCs i.e. mini computers. Raspberry Pis acted as re edge side data collectors while NUCs hosted the IoT-based gateway service facilitation. Thus, a CDF architecture was proposed and proven to be effective in real-life scenario [4].

Table 4
Comparative analysis of network driven architecture.

Paper	Objective	Novel contributions	Advantages/Limitations
[3]	Development of continuous integration and continuous delivery (CI/CD) framework	Developed a CDF by using SmartX-mini platform DevOps	Formulation carried away, not intuitive in design
[4]	CDN development using Jenkins server	JSLint, PEP8, and Pylint tools where PEP8 overperformed than other alternatives. 40 Raspberry Pi 2 were implemented with 13 Intel NUCs i.e. mini computers. Raspberry Pis	Tested against IoT gateway scenario, does not show promise towards network mitigation
[5]	Development of end-to-end network service orchestrator (E2EO)	SPN orientation with virtual network object, NFV-MANO, uCPE and NSH header inclusion	RESTful interface design, unchecked LLDP usage
[6]	Prediction and maintenance of IoT network connectivity	PNF layering by using TL1, OFCONFIG, OpenFlow, ForCES, NETCONF, and OVSDB	VNFM, VNM and EMS module deployment
[7]	Slicing IoT concept proposed	E2E network slicing, distributed modeling of slicing capabilities, resource composition, and reconfiguration of slicing resources	rACM, CAPI and RSLA modules integration, user requirement mitigation
[8]	Intent management system development	OpenFlow model formulation, OVNFM, NFVO, Nf-Vi modules developed	Open network operating system was tested, QoS validation, effectiveness analysis not mentioned
[9]	User-to-network interface provisioning	TINBR, INC and PCS modules developed L1/L2/L3 cache facilitation	CAPEX, OPEX minimization, ICN based SaaS validated, efficiency measure not tested
[41]	Data slicing ICN development	Three-layered architecture proposed, data slicing is materialized within the SDN/NFV enabled ICN aspect	Architecture tested against Kubernetes cluster and OpenHAB IoT platform nodes, InfluxDB and OneM2M modules were validated

5.2. End-to-End network service architecture

Edge-cloud interplay depends on the aspects of the end-to-end network service facilitation. SDN/NFV can certainly improve such provision in better way. Thus, [5] deployed the end-to-end network service orchestrator (E2EO) architecture that followed the underlying software-programmed networking (SPN) orientation where virtual network object (VNO) abstraction was incorporated with help of Amazon web service (AWS) and Fujistu K5. The E2EO architecture used the TOSCA template and NFV-based management and network orchestration (NFV-MANO). This architecture implemented a universal customer premises equipment (uCPE)-based functions with inclusion of representational state transfer (REST)-ful application programming interface (API). Elastic search database from EWS facility was involved for communication between the user-site controller and E2EO work flow manager. Network service header (NSH)-enabled virtual switches were used in conjunction to link layer discovery protocol (LLDP) to pave the end-to-end network service orchestration. Fig. 3 presents the E2EO architecture and demo setup.

Users, locating at edge often face lack of response time and service availability when interacted with cloud-based scenario. Thus, overall quality of user experience (QoUE) seemed to be lacking in most of the cases. [6] proposed an SDN/NFV based architecture to deal with prediction and maintenance of connectivity of underlying IoT-based network ecosystem. The study proposed a four-layered architecture that consisted of (i) infrastructure layer, (ii) controller layer, (iii) application service layer, and (iv) end-to-end orchestration layer. Infrastructure layer consisted of different types of physical resources i.e. physical network functions (PNF), nodes, links, edge computing devices, and cloud data centers. This layer supported other three layers via tools like TL1, OFCONFIG, OpenFlow, ForCES, NETCONF, and OVSDB. Thus, a complete structure of SBI was developed. This SBI communicated with the controller layer where access, core, cloud and edge controllers played important role. Controller layer invoked NBI via the application service layers that employed VNF manager (VNFM) and virtual infrastructure manager (VIM) to cater element management system (EMS) for effective end-to-end interfacing. A virtual end-to-end (E2E) topology was formulated top of the architecture helped the user to access the system in more reliable, privacy-aware, and scalable fashion. The propose architecture improved the deployment aspect of any SDN/-NFV scenario under IoT-based ecosystem while decreasing the overall system complexity level.

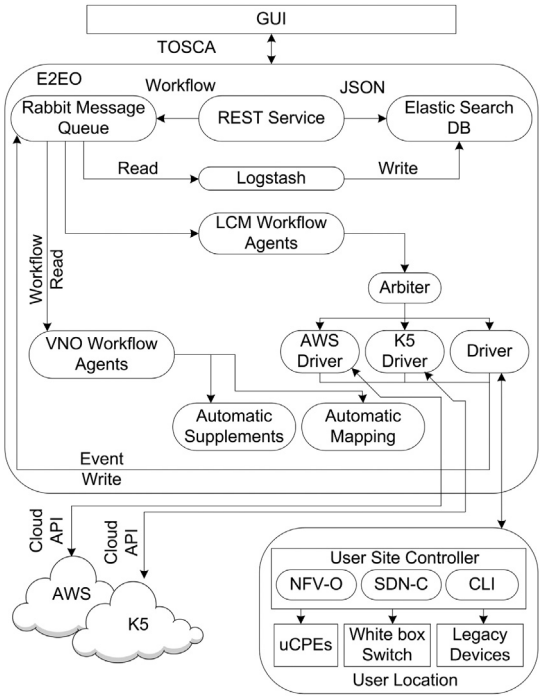

Fig. 3. E2EO Architecture and demo setup.

Slicing is another requirement that an SDN/NFV system must support. Due to overwhelming growth of IoT-based users, service requirements are gradually getting dynamic in type. Challenges are faced to meet such slicing requests in IoT-based models. Thus, a slicing IoT, network functions, and clouds i.e. (SINC) was conceptually proposed [7]. In this architecture, following benefits were achieved that includes (i) E2E network slicing, (ii) distributed modeling of slicing capabilities, and (iii) resource composition, and (iv) reconfiguration of slicing resources. SINC architecture used a three-layer approach where IoT networks, SDN/NFV and cloud-based APIs were kept in lowest layer. Middle layer deployed SINC-based resource adaptation, configuration, and management (rACM) module. Finally, the top most layer was made of various applications e.g., emergency, on-demand sensing, quality

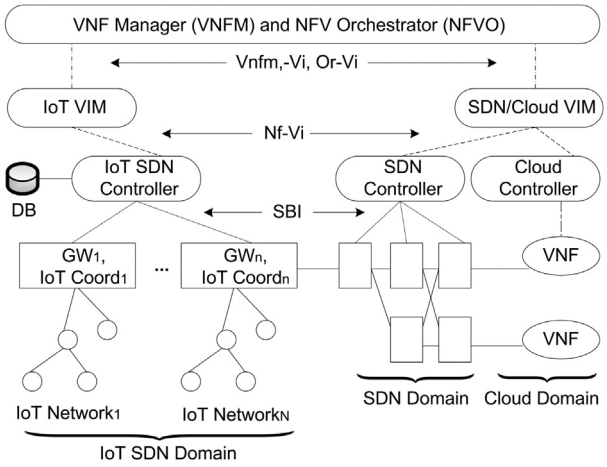

Fig. 4. Intent-based management architecture.

measurement, functional performance monitoring, and geo-sports monitoring. The rACM module provided the actual E2E slicing facilities to the lower layer via SINC-based routing, slicing, and naming (RSN) layer, and communication cum API integration (CAPI) layer. The main role of rACM was to provide network routing, naming, API integration with the on-demand applications so that API of IoT-network, SDN/NFV and cloud could be mitigated. SINC was further advanced by inclusion of runtime slice adaption (RSLA) policy that resolved two key issues such as, monitoring of changes (i) user requirements and (ii) underlying architecture.

5.3. Intent-based management architecture

E2E service provisioning becomes difficult when unified management functions and orchestrations functions lack in quality. Thus, intent-based management could be seen as a possible solution to such issues which could be normalized by abstraction of data and control planes. An OpenFlow model was recently tested in [8] that used SDN/NFV centric intent-based management architecture to leverage seamless sensor data collection, processing and publishing to the IoT-based cloud platforms. This work utilized two key components such as, (i) overarching VNFM (OVNFM) and (ii) NFV orchestrator (NFVO) to formulate the VIM under edge-cloud scenario. The proposed architecture presented three layers of abstractions, that included (i) technology-specific SBI, (ii) network/cloud controller-based NBI (Nf-Vi), and (iii) VIM centric intent-based NBI (VNFM, Or-Vi) to realize the IoT-specific aspects. The SBI layer was comprised of IoT-based gateways (GWs) and IoT coordinator nodes (CorNode) that helped to sense and receive data flow ground level of hardware and sensors. The approach behind such layered implication was to involve VNF in multi-layered format so that Nf-Vi layer could be benefited with incorporation of distributed database and IoT-based SDN/cloud controller facilities. Finally, the NFVO approach was realized by intervention of IoT-based VIM and SDN/cloud-based VIM integrations. The work evaluated IoT and OpenFlow domain performances over the open network operating system (ONOS) to assess the quality of service (QoS) of the deployed architecture. Fig. 4 presents the proposed intent-based management architecture. In this architecture, the IoT-SDN controller is different than SDN/Cloud controller in terms of (i) use of IoT-based protocols, (ii) connectivity with the IoT-based DBMS, (iii) IoT-based VM service profiles, and (iv) direct controlling of IoT-based gateway coordinations.

5.4. Information centric network architecture

Information centric network (ICN) refers to the process of decoupling of applications from the transport layer by separating content, services, and application and later binding those with the resolution layer of ICN framework. Such, de-coupling of ICN benefits various dynamic attributes of networks such as, (i) resolving named objects (e.g., content, service and IoT-based devices), (ii) migration, and (iii) mobility of content-specific services. Reduction of capital expenses (CAPEX) and operation expenses (OPEX) may be furnished by indulging following factors of ICN into the existing IoT-based network infrastructure, such as, (i) topology independent name-based routing (TINBR), (ii) packet level security (PCS), (iii) in network caching (INC), (iv) mobility support, and (v) multicast/anycast support.

A recent study showed how to develop a user-to-network (UNI) interface for peer-to-peer (P2P) communication between the stakeholders of an envisaged online conferencing application [9]. The architecture incorporated an edge-cloud intercommunication scenario by including ICN-based UNI-API and ICN-based service API. All deployed ICN service platforms were interconnected by using high speed L1/L2/L3 cache interfacing which were dynamically controlled by the ICN cloud orchestrator. The ICN service platform used ICN service router to pave various networking facilities within the ICN service gateway and ICN service profile managers. Further, ICN protocol was leveraged with help of software as a service (SaaS) aspect of cloud. SDN/NFV services were integrated throughout the architecture. Thus, a content centric network design was formulated under the edge-cloud interplay for an IoT-based application.

Efficient ICNs may upgrade existing IoT-enabled systems with more information-oriented servicing. But, regular and continuous data update within an IoT-based application become very difficult to manage, especially when edge-cloud interplay is there. Thus, an effective data slicing mechanism could enrich the said issue in better way. [41] proposed a data slicing centric ICN architecture to formulate service abstraction, generalization, and containment.

A three-layered architecture showed how data slicing could be materialized within the SDN/NFV enabled ICN aspect. Lowest layer was developed for monitoring of data sources, middle layer served the distributed data collectors, and top most layer supported the centralized data collectors. Data coming from lowest layer was first sliced and then transmitted to the distributed data repositories that managed the message queues, data adaptor, and data processor units. Drivers of various data handlers acted like resource agents and assisted in storing of logs and configuration for analysis at the centralized data repositories. The architecture was tested against the Kubernetes cluster and OpenHAB IoT platform nodes.

InfluxDB and OneM2M platforms were deployed to emulate the timely mitigation of sensor data. Thus, an efficient IoT-based ICN centric slicing service was paved. Fig. 5 presents the ICN monitoring architecture. Table 4 presents the comparative analysis of surveyed articles in terms of network driven architecture.

6. Object scalable and flexible architectures

6.1. Object placement and virtualization architecture

Object placement plays a crucial role in SDN/NFV service mitigation. Inappropriate positioning of an object in such scenario may impose limitations like increase of overall deployment cost and maximizing E2E delay under a specified SLA. Thus, revision of existing approach needs to be advocated. [42] deployed a mobile edge computing (MEC) assisted cloud computing supported VNF placement problem solving architecture.

The architecture targeted to facilitate network services such as, firewall control, IoT traffic prioritization and network address translation (NAT) in the given scenario. Service provider (SP) and service chain (SC) assisted hybrid architecture provided IoT-based objects' accurate placement in the VNF-based placement at the edge and cloud (VNF-PEC) ecosystem that formulated instance consolidation (IC) of IoT-objects within the non-uniform memory access (NUMA) by deploying a mixed integer programming (MIP) technique. A Tabu search (TS)

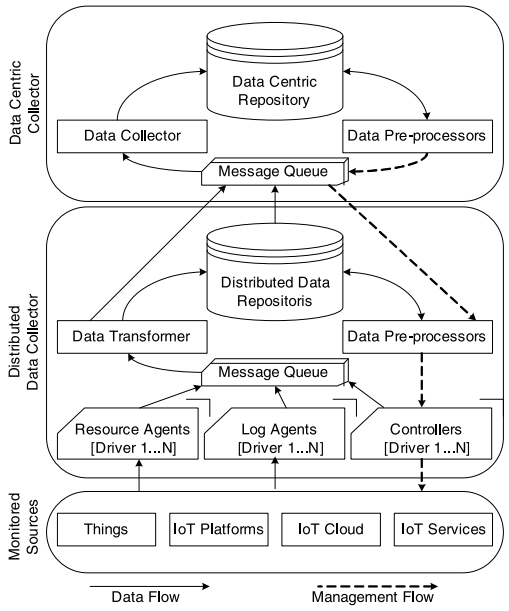

Fig. 5. ICN monitoring architecture.

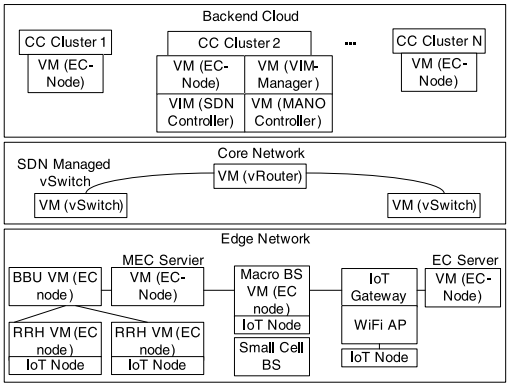

Fig. 6. Collaborative edge-cloud architecture.

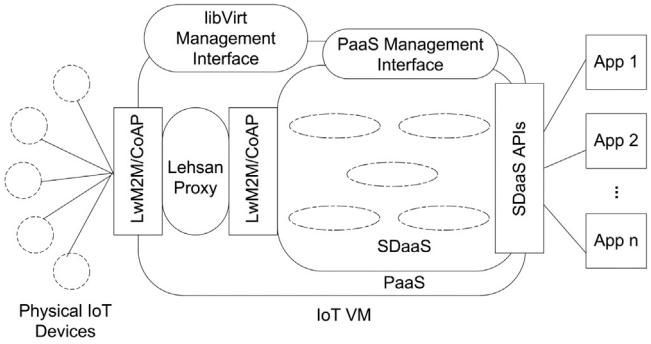

Fig. 7. Object virtualization using LwM2M protocol architecture.

method was implemented into the proposed architecture to solve the object localization in the edge-cloud interplay.

On the other hand, object virtualization is another important factor that has also recently gained huge importance. Due to huge number of objects connected with the IoT, object virtualization has become an immense area of research where edge-cloud communication delay could be reduced. Thus, an architecture was proposed and validated to prove the significance of IoT-object virtualization with help of SDN/NFV facilities [43]. The architecture had two layers i.e. (i) local and (ii) cloud layer. In local layer, user centric facilities were provided such as, sensors, OMA LwM2M proxy i.e. Lehsan protocol support, smart device as a service (SDaaS) and cache storage. Cloud layer acted as back end of the architecture while comprising of device manager and data storage services.

A number of applications were tested against a simulated environment under the aegis of the propose architecture that included SDaaS based APIs as well as LwM2M/constrained application protocol (CoAP) within the IoT-based virtual machine (IoT-VM) infrastructure. A libVirt Mngmt interface was deployed that helped the Lehsan proxy to successfully communicate between the LwM2M/CoAP and LwM2M/HTTP interfacing layers. Fig. 7 presents the Lehsan protocol enabled architecture.

6.2. Scalable and flexible architecture

Scalability is a key element for SDN/NFV centric IoT-based applications. Due to the huge growth of IoT ecosystem, gradual scalability and flexibility of underlying ecosystem are becoming crucial factors for success of edge-cloud delay diminishing movement. Machine learning (ML) has been recently integrated with an architecture to make SDN/NFV allied IoT applications more scalable and flexible in nature [44]. The aim of the architecture was to incorporate data analytics facility into the existing IoT-based scenario by using programmability, virtualization, and overall management of the ecosystem. Fig. 6 presents the collaborative edge-cloud platform.

The proposed architecture was developed in three layered structure where lowest layer dealt with edge network, middle layer served the core and aggregation network, and top layer mitigated the backend cloud services. Edge network layer comprised of following elements such as, (i) IoT gateway, (ii) IoT device, (iii) VM edge computing (EC) models, (iv) remote radio head (RRH), and (v) base band unit (BBU). Edge network was commutating with the core network through the backhaul internetwork connectivity.

Several VM switches and routers managed the whole SDN-centric activities in this layer. Cloud computing (CC) clusters came to play on the top layer where VM (CC nodes), VM (MANO controller), and VM (SDN controller) served the whole backend facilities. ML was used in learning the managerial behavior of the architecture, thus making architecture a super flexible and scalable one.

6.3. Crowdsourcing architecture

Resource sharing in the EC paradigm need to be handled with utmost care, otherwise, OPEX could be higher than the expected, resulting a negative impact on the underlying system. It is seen that single CPE has very restricted capacity, especially if it is a physical CPE (pCPE). So, sharing information of a greater number of pCPE could perform complex tasks in the customer edge (CE) perspective. For example, IoT-gateways at home are underutilized during day time as the habitants are out for the work, on the contrary office IoT-gateways become idle after the working hours. In such cases, if information sharing of pCPE i.e. IoT-gateways could behave possible then resource utilization of such devices would have been greater. Thus, a novel architecture was proposed to mitigate this issue of crowdsourcing of pCPEs in the CE space while leveraging SP-centric approaches in the SDN/VNF application domain [10]. The architecture was composed of three layers, such as, (i) NFV infrastructure (NFVI) and VIM layer, (ii) VNFM layer, and (iii) NFVO layer, from bottom to top, respectively. The NFVI utilized a resource manager to manage the activities of the underlying VM scheduler (VMS) to perform assigned tasks along with the pCPE modules as well as the cloud host service in consultation with the deployed VIM. The instances of pCPEs communicated their

Table 5
Comparative analysis of object scalable and flexible architectures.

Paper	Objective	Novel contributions	Advantages/Limitations
[42]	Object placement, object virtualization architecture modeled	MEC assisted cloud computing supported VNF placement problem solving architecture proposed, VNF-PEC, NAT, SP, SC modules integrated	NUMA, MIP techniques tested, Tabu search method validated
[43]	IoT virtualization by SDN/NFV aspect proposed	Two layer local-cloud integration in IoT centric ecosystem was modeled	IoT-VM, OMA LwM2M protocol supports were provisioned, SDaaS, CoAP schemes were tested
[44]	Scalable and flexible IoT centric architecture was catered	RRH, BBU modules implemented, machine learning used for managerial behavior augmentation	VM-MANO, VM-CC, VM-SDN modules tested
[10]	Crowdsourced pCPE architecture proposed	NFVI, VNFM, VIM, NFVO layered implemented, pCPE instances deployed	Parametric information such as, vCPU, memory usage, network bandwidth consumption and placement were tested
[11]	Industrial IoT architecture proposed	DPWS, TLS, SSL based IIoT architecture deployed	Modules were tested against SCADA and NSPs
[12]	Self-adaptive management service provisioning deployment	ANFO, MAPE, QoS service mitigation implemented	EDC and OM2M testing were performed

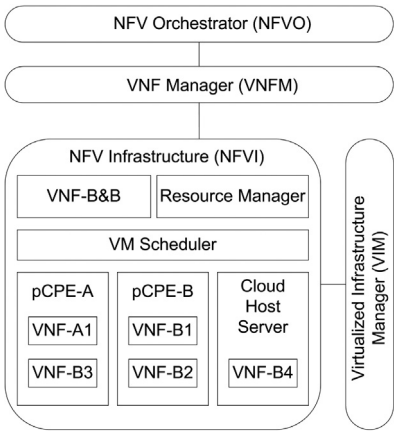

Fig. 8. ETSI NFV crowdsourcing architecture.

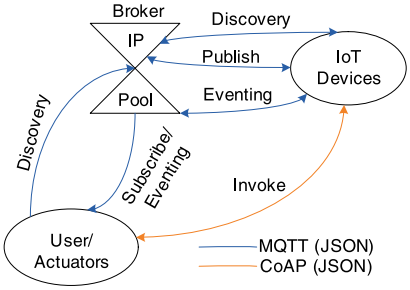

Fig. 9. Hy-LP architecture.

resource specific information with each other by using real-time IoT-based infrastructure. The same is systematically uploaded with the cloud counterpart for remote access by the CEs. Such crowdsourcing architecture paved the instantaneous availability of pCPEs and their parametric information such as, virtual CPU (vCPU), memory usage, network bandwidth consumption and placement, with other nodes. Fig. 8 presents the crowdsourcing architecture.

6.4. Industrial IoT centric architecture

Circular economy is recent trend that can harness value creation and innovation domains in the industrial IoT (IIoT). Circular economy is a requirement of IIoT that can efficiently utilize the emerging looping assets, natural capital regeneration, and asset utilization for betterment of feedback-rich IIoT centric mindset. Thus, an architecture was formulated and validated against the hybrid protocol of circular economy for the IIoT perspective to mitigate the earlier said issues. The architecture involved transport layer security (TLS) and secure sockets layer (SSL) protocols to enable the design for IIoT-based sustainable economy development. The architecture was tested against the devices profile for web services (DPWS)-based architecture to validate its effectiveness.

The architecture used MQTT and CoAP protocols to discover and publish/subscribe the events happened between the IoT-users and cloud centers via the SDN/NFV formulation. The architecture was also simulated for wind park monitoring application that used supervisory control and data acquisition (SCADA) along with the SDN controller of the deployed architecture. Network service providers (NSPs) centric routers were incorporated to create an internetwork facility for providing the SDN controller communication between different DPWS users of wind parks. The proposed hybrid protocol i.e. Hy-LP architecture paved a reliable model for achieving the IIoT-based circular economic boom into the future market [11]. Fig. 9 presents the Hy-LP architecture.

6.5. QoS provisioning architecture

IoT system management is still in nascent stage of development. Most of the times, it is static and consumes more time to facilitate the required service and costly. Thus, such immature system management is poorly suited for the emerging dynamic behavior of the IoT-based applications.

A recent study has proposed and validated an architecture to dynamically provision self-adaptive management services via the QoS metrics for the IoT-based systems under the aegis of edge-cloud interplay [12]. The high-level architecture of the proposed work incorporated IoT applications, local area network (LAN), personal area network (PAN), sensors, actuators, edge node, cloud node, applicative network function (ANF), ANF-orchestrator (ANFO), SDN controller, and IoT-gateways, SDN network, and Monitoring, Analysis, Pacification and Execution (MAPE) loop.

The architecture was deployed for wild life monitoring application where OM2M platforms were involved to harness the QoS provisioning of the Raspberry Pi enabled sensor modules via the edge data center (EDC). This type of architecture brought agility to the existing IoT-ecosystem where economic and commercial tradeoffs were mitigated by advanced virtualized QoS services. Table 5 presents the comparative analysis of surveyed articles in terms of object scalability and flexibility architecture. Fig. 10 presents the QoS provisioning architecture.

7. Mobile edge cloud architectures

7.1. Mobile edge cloud architecture

Futuristic IoT applications shall require similar characteristic and unified traffic patterns. Device to server (DS) service may be included into the IoT ecosystem for efficient mobile edge assisted provisioning on data planes, distributed control, and light-weight service abstractions.

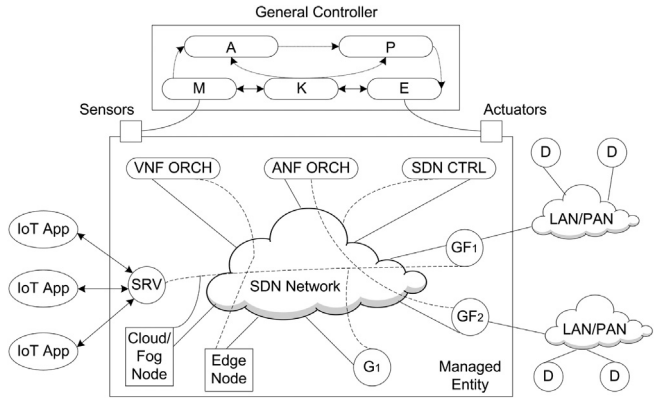

Fig. 10. QoS provisioning architecture.

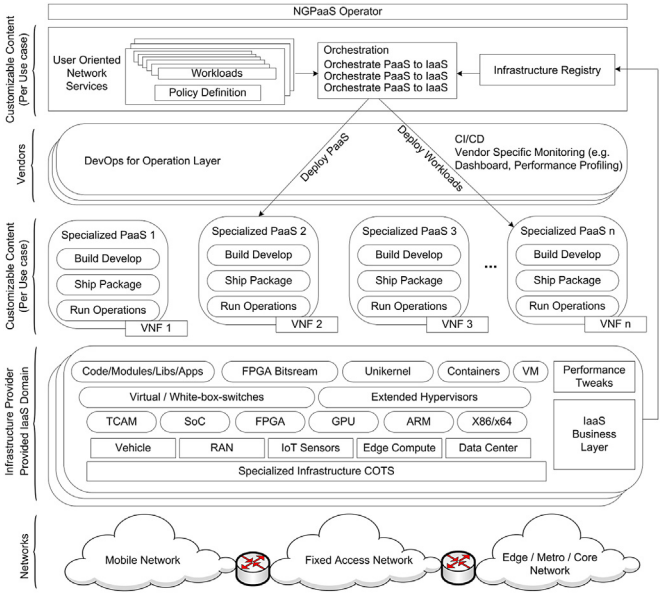

Fig. 11. NGPaaS provisioning architecture.

SIMECA architecture was validated to check the effectiveness of the P2P communication wise cost and delay under the SDN/NFV scenario. SIMECA used LTE/EPC layering for core network elements like SGW/PGW for best-effort minimization of tunneling overhead in seamless manner. IoT-based service abstraction (ISA) layer was placed atop the architecture where RESTful, NAS, and OpenFlow enabled mobile edge computing (MEC) devices were brought into the frame. OpenEPC nodes were deployed to mitigate the SDN-MEC interconnection for region-wise IoT-devices' data migration [13]. The server-side service platform was consisted of SDN controllers and open virtual switch (OVS) to cater the mobility aware functionalities.

7.2. Next generation platform as a service architecture

Next generation IoT must be equipped with the versatile factor that can blend all types of connectivity between the objects, humans, and machines. Existing infrastructure as a service (IaaS) in not enough to solve such versatility issue. Thus, a next generation platform as s service (NGPaaS) architecture was proposed while aiming at the versatile third-party service and application facilitation by the telecommunications industries.

NGPaaS was a boon for the telecommunication service providers who would like to serve IoT-centric applications under the hood of edge-cloud interplay [14]. This architecture facilitated the infrastructure providers and vendors simultaneously by allowing to orchestrate the operations support system (OSS) via the DevOps layer. OSS deployed workloads and ancillary services to the VNFs through the specialized platform as a service (PaaS) where development, packaging, and operations were altogether implied. Both the customizable and IaaS services were originated from the bottom layer of architecture i.e. infrastructure layer. In this layer, a set of commercial off-the-shelf (COTS) tools and device pools were integrated that supported the vendors by invoking the IaaS business module for benefitting the MANO-wise VNF services. Fig. 11 presents the NGPaaS architecture in detail.

SLA assurance was given in the vendor layer that invoked CI/CD facilities while harnessing the SDN/NFV conjunction approach. The NGPaaS was further integrated with the IoT-based applications where E2E and demand/response business as a service (BaaS) were provided from the cloud counterpart.

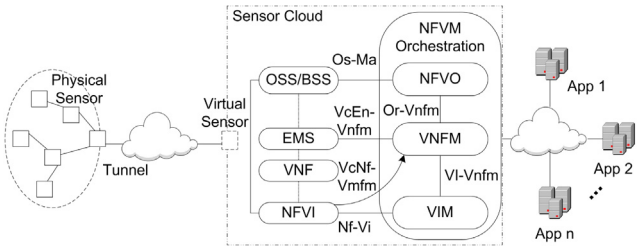

Fig. 12. Energy efficient SDN sensor cloud architecture.

7.3. Energy efficient architecture

Current trend of IoT-based ecosystem leverages incorporation of information producers (IPD) and information providers (IPV) to minimize the trade-off between the sensor data prediction and accuracy of data. Such trade-off is important due to the on/off or sleep mode processing of IPV or IPD. When IPD is in sleep mode, IPV works, when IPV is sleeping, IPD works. Thus, overall energy consumption is reduced which is a great benefit of the prospective IoT-based applications. Recently a research showed how to minimize energy consumption under the SDN/NFV computing plethora by utilizing the dynamic change of states i.e. active IPD (aIPD) and inactive IPV (iIPV) so that overall information correlated communities (ICC) of edge-cloud enabled use cases could be facilitated [15]. Tiny OS-based simulator TOSSIM and radio-frequency (RF)-based module CC2420 were deployed that paved the communication between the internal information correlation (IIC) factors to the SDN/NFV assisted sensor type community (STC) by using low power listening protocol (LPL). The architecture used clear channel assessment (CCA) over the implied collection tree protocol (CTP) under the direction of SLA-based tolerance of data accuracy (TDA) mechanism. IPDs were enabled with the IoT-based virtual sensor (VR) oriented data processing via the OSS/BSS, NFVI, VNF, and EMS modules to communicate with the information consumer (ICM). Several service provisioning like VeNF-Vmfm, Nf-Vi, VeEn-Vnfm, and Os-Ma were correlated with Or-Vnfm and VI-Vnfm on top of OpenStack platform. Thus, the architecture leveraged an energy aware architecture where edge-cloud communication delay and data accuracy were provided. Fig. 12 presents the SDN-NFV information centric energy efficient cloud architecture.

7.4. Multi-access edge computing architecture

Futuristic IoT is envisaged to support smart customer services for both service and product domains. Multi-access edge computing (MAEC) paradigm aims at leveraging cloud services and capabilities

Table 6
Comparative analysis of mobile edge cloud architectures.

Paper	Objective	Novel contributions	Advantages/Limitations
[13]	Device to server architecture proposed	SIMECA used LTE/EPC layering for core network elements like SGW/PGW for best-effort minimization of tunneling overhead in seamless manner	SDN controllers and OVS were validated
[14]	Next generation platform as a service architecture deployed	Orchestration of OSS via DevOps layer, COTS tools used, MANO-VNF deployed	CI/CD facilities tested BaaS service was investigated
[15]	Energy efficient IPD-IPV architecture proposed	aIPD, iIPV and ICC modules deployed. TOSSIM-RF based STC, LPL, CCA and CTP correlation were performed	VeNF-Vmfm, Nf-Vi, VeEn-Vnfm, and Os-Ma were correlated with Or-Vnfm and VI-Vnfm on top of OpenStack platform
[16]	MAEC architecture proposed	RNS community was catered to run capacity aware applications	Mobility management, security, privacy, trust management, NFV-aware integration, ICN, and network slicing were tested
[17]	Cloud assisted architecture was formulated	VN, NCLS, VIRM, VNFM, VNFO modules deployed	High gain in cost saving and energy efficiency were perceived
[18]	Cloud-based virtualization architecture was proposed to harness the IoT-edge services	SDN controllers atop the presentation which persuaded the virtualization functions	IoT-domain, IoT-gateway, and IoT-applications were tested
[19]	Proposed IoT-devices related services in close proximities of the E2E backbone service Leveraged dynamic offloading, automated orchestration, and coherency of SDN and NFV	Involved a SND-enabled multi-cloud prospect	
[20]	Complete IoT virtualization was proposed	FMT, TCAM, LVX, DVS mechanisms were deployed	IoT edge-cloud ecosystem harness with help of complete virtualization
[21]	Optimal algorithm to calculate the throughput was proposed	Probable approximation ratio was computed upon arrival of each such request to the cloud	Time slot division was performed in SDN/NFV allied layer for IoT services

to the edge devices and customers. Thus, MAEC is seemed to lower the requirement of bandwidth consumption and latency to the radio network resources (RNS). In [16], myriad of MAEC possibilities have been investigated to exploit the SDN/NFV assisted edge-cloud service provisioning under the IoT-based ecosystem. MAEC is developed to provide context and capacity aware facilities to the RNS community. MAEC has extended its reach to a range of application such as, smart home, autonomous vehicle, healthcare, wearable device, energy, transport, smart city, agriculture, and industry. It depends on three types f communication access namely, wireless, backhaul, and intercommunication among IoT devices. Several benefits are being harnessed for the MAEC in mitigating issue like (i) mobility management, (ii) security, (iii) privacy, (iv) trust management, (v) NFV-aware integration, (vi) ICN, and (vii) network slicing. The underlying architecture provide computation offloading, scalability, resource allocation, and virtualized applications. Thus, MAEC is a good candidate for the realization of EC-based IoT application developments.

7.5. Cloud assisted architecture

Gradual demand of IoT has arisen the need of new type of shareable architecture that can provide flexible services to its customer as per the dynamically changing demands. Thus, a subscriber centric approach may improve the dynamic demand information sharing scenario. [17] proposed a novel architecture to solve such issue that involved a multi-layered approach starting from programmable virtual networks (VN) at the bottom to the network device specialized function (NDSF) at the top. The architecture was based on the existing COTS forwarding hardware and related network control logic software (NCLS). Thus, the control plane of the SDN/NFV involvement virtual storage, virtual firewall, and VM as the virtual device section. A cross-platform virtualization layer was embedded within the architecture that worked with virtual infrastructure resource manager (VIRM), VNFM, and VNFO. The software controller paved the interfacing between the NBI and SBI tool set. A set of open standard APIs were included to pave a quality of service to the hypervisor on device via the installed VMs. The architecture formulated a simulation that showed a high gain of cost saving and energy reduction in the overall system that levied the cloud-based approach. Another cloud-based virtualization architecture was proposed to harness the cloud services into the edge-located IoT devices. The architecture used SDN controllers atop the presentation which persuaded the virtualization functions by involving IoT-domain, IoT-gateway, and IoT-applications as a whole [18].

Due to centralized computation, IoT-based applications impose huge load over the cloud datacenters which may sometimes make the process difficult to enable IoT-based aspects in resource-poor situation. Such issue may come with other disturbances into the system that may include (i) varied volume and velocity of IoT-data, (ii) latency between IoT device and cloud data center, and (iii) monopoly marketization of some tools. [19] presented an architecture that could make the IoT-devices related services always available by keeping those close proximities of the E2E backbone service. The architecture aimed at leveraging dynamic offloading, automated orchestration, and coherency of SDN and NFV. It also involved a SND-enabled multi-cloud prospect in the existing scenario. Complete virtualization has been recently attained by another similar work [20]. In this work, a substrate agnostic virtual SDN network was formulated. A full virtualization layer was embedded within the earlier said substrate-based layer and a physical network layer. Concept of flexible matching table (FMT) was introduced herein in accordance to topology and ternary content addressable memory (TCAM). Late binding key extractor (LBX) was used to assist the deployed virtual switch (DVS) with help of FMT pipeline mechanism. The study showed how full virtualization cloud be invoked with the IoT-based edge-cloud ecosystem. The study develops a SVirt architecture as shown in Fig. 13.

When cloud services are paved for SDN/NFV framework, throughput of admitted NFV requests must be monitored. A recent study presented an optimal algorithm to calculate the throughput when all SDN/NFV request have similar packet transmission rates [21]. Probable approximation ratio was computed upon arrival of each such request to the cloud. Shot-wise periodic optimizations could be harnessed from this algorithm that was deployed into an architecture. The architecture helped to divide the time slot into multi components to provide throughput assurance in the IoT-based system. Thus, admissibility of requests into the cloud could be dynamically monitored so as to enhance the overall QoS. Table 6 presents the comparative analysis of surveyed articles in terms of MEC architecture.

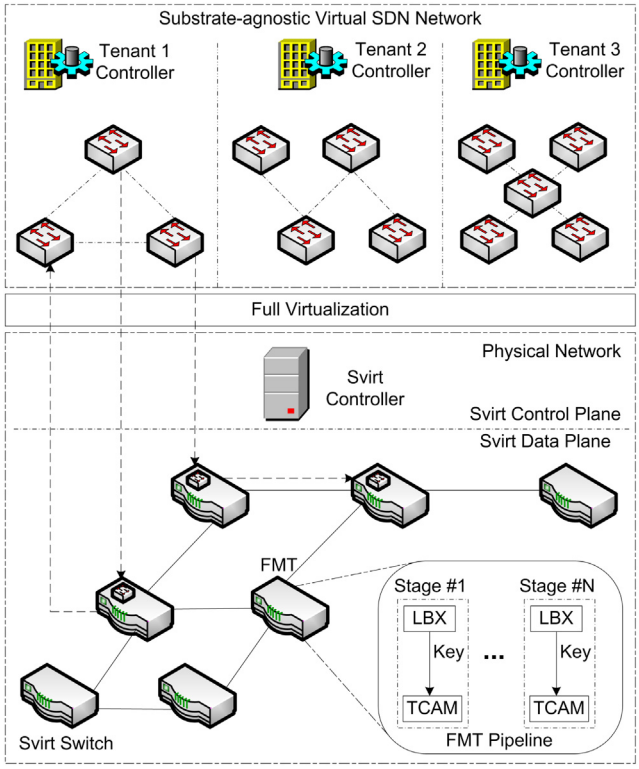

Fig. 13. SVirt architecture.

8. Next generation cellular architectures

8.1. 4G architecture

Existing long-term evolution (LTE) networks are getting heavily popular in different parts of globe. Most of the nations have already deployed 4G-LTE in variant forms for high speed voice over data connectivity. However, the LTE networks are unable to accommodate SDN/NFV, IoT, MEC, mobile social networking (MSN), and mobile cloud computing (MCC). Some paradigms are superfluously adopted within the LTE framework, but they are not scalable and efficient in nature. 4G LTE is adopting the heterogeneous network (HetNet) and multiple radio access network (RAN) along with the distributed ICN-based routing. A recent architecture has involved advanced routing functions and traffic management protocols with the LTE for dissemination of edge-cloud formulation under the aegis of IoT [45]. The cellular architecture integrated distributed internet backhaul and MCC along with content delivery network (CDN). The architecture was efficiently developed atop small and macro cell bate stations, (SBS) and (MBS), respectively. Tracking area (TA) coverage facility was mitigated by indulging local SDN controller (LSC) into the structure. NBI and SBI interfacing were successfully convened under the local request resolution function (LRRF) deployment.

Simultaneously, multi-RAN function (MRCF) was deployed over the local content caching function (LLCF) to assess the local IP access (LIPA) and selected IP traffic overload (SIPTO) in efficient manner. Core content and mobility functions (i.e. CCRF, CMMF) were implemented in the given SDN/NFV centric scenario.

Such huge capacity makes an architecture over burden. Thus, cost analysis becomes priority in related aspects. [46] proposed a cost analysis architecture by complying SDN/NFV amalgamation to identify the expenses in the 4G network. The architecture evaluated IoT-based devices and cost savings by implying a novel architecture. A comprehensive study was performed to improve the network virtualization

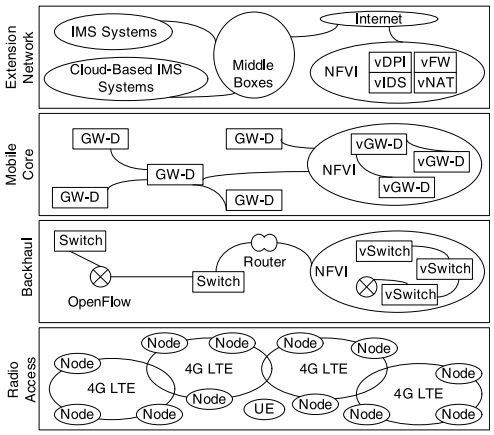

Fig. 14. SDVMN architecture.

of 4G network by involving SDN/NFV, IoT and other virtualization services [22]. The study proposed a novel SDN-based virtualization architecture for 4G mobile networks. The architecture was composed of user/data plane, control plane, and application plane. All the planes were segregated into four layered structure where radio access layer was placed at the bottom and backhaul, mobile core, and external network layers were place on top of it. The SBI interfered with the user/data plane while facilitating distributed access points (AP), eNode base stations, and RRH to communicate with the NFVI device pool. Management plane controlled the architecture to pave the SBI-NBI interfacing. Technologies like OpenFlow, BGP, and ForCES were used to interact with SBI while RPC, JSON, and RESTful APIs were used to communicate with NBI. SDN-based RAN controllers, backhaul controllers, core controllers, and service controllers played the vital role in the control plane. Applications of the architecture comprised of routing, monitoring, offloading, mobility management entity (MME), interface management, device to device (D2D) connectivity, and QoS service provisioning. VMNO instances were deployed to cater a range of other related activities. Fig. 14 presents the proposed SDVMN architecture as mentioned earlier.

8.2. 5G architecture

5G network is at the verge to get deployed by the telecommunication operators within coming few years. Dynamic scalability shall be a need of IoT, video streaming, and high-speed internet gaming. Future network cost shall be minimized with enhancement of network services, especially virtualized services. SDN/NFV shall play major role in integration of virtualized services with the 5G networks. In [47], a dual layer architecture was proposed that paved the communication between user and control planes. Besides, packet forwarding, user plane layer provided GPRS tunneling protocol (GTP) for QoE mitigation. Control plane was positioned at the cloud end where mobile network cloud services were paved via incorporation of SDN controller, SDN service chaining, MME, and gateway user plane applications. Policy and charging rules function (PCRF) were deployed the core 5G network function into the architecture where 5G service-based architecture (SBA) commissioned NAT and OFS services.

Agile management was recently formulated by the 5G-based SDN/NFV architecture and implemented in the proof of concept (PoC) for the Pyungchang Winter Olympics [48]. In this architecture following characteristics were given most importance that includes proximity, location awareness, higher network bandwidth, and ultra-low latency. Several auto-scaling processes were involved that included MANO, MANO/SDN, vEPC, and VNFM. The architecture leveraged a new way to incorporate agility into 5G networks under the edge-cloud perspective. SDN orchestration in 5G network is another issue that need

Table 7
Comparative analysis of next generation cellular architectures.

Paper	Objective	Novel contributions	Advantages/Limitations
[45]	4G-based improved routing function and traffic management protocols developed	CDN, MBS, LBS, LSC modules integrated, LRCF, MRRF, LLCF were deployed	LIPA, CIPTO, CCRF, CMMF were tested
[46]	4G cost analysis proposed for IoT ecosystem	SDN/NFV cost expenditure calculated	Cost savings schemes were evaluated
[22]	4G network virtualization improvement architecture proposed	OpenFlow, BGP, and ForCES were used to interact with SBI while RPC, JSON, and RESTful APIs were used to communicate with NBI	MME, D2D, RAN and VNMO instances were tested
[47]	5G dual layer architecture proposed	GTP implemented, QoE aspect was tested	PCRA, SBA, OFS modules were tested
[48]	5G agile management architecture proposed	Proximity, location awareness, higher network bandwidth, and ultra-low latency measures were mitigated	Auto scaling process including MANO, MANO/SDN, vEPC, and VNFM was tested
[49]	5G dynamic service chaining in real-time architecture proposed	Operating platform was abstracted	Scheduling and orchestration of IoT device manager was formulated
[50]	5G CVT architecture proposed	RSPAN, sFlow, RSPAN modules were encapsulated	DPDK was tested
[51]	5G multi-tenancy architecture proposed	T-API and TelcoFog architecture were integrated	Multi domain control planes were tested
[52]	5G verification and validation architecture proposed	5GTANGO architecture integrated, time-to-market time was reduced	OSS, VIM, SD-WAN and WIM infrastructural platforms were tested
[53]	Satellite–cellular architecture proposed	NFVI-PoP, SCC and NMS were implemented	OpenStack, OpenDaylight, OpenSAND, OpenFlow were tested

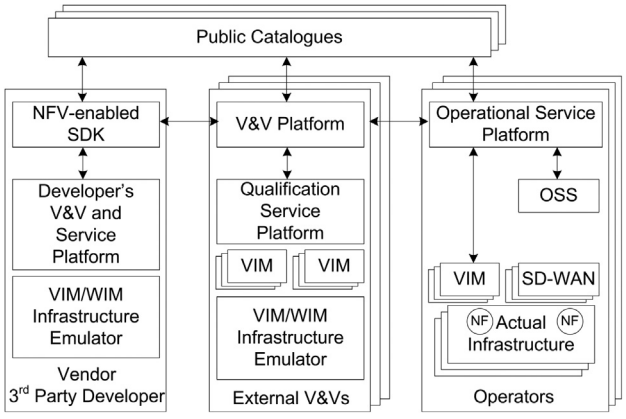

Fig. 15. 5GTANGO architecture.

to be covered for effective IoT deployments. Thus, [49] experimented an architectural procedure to develop a reference framework. In this study, real-time 5G operating platform (OP) was abstracted to assist in dynamic service chaining, scheduling, and database supporting in real-time. The abstraction layer orchestrated IoT device manager, SDN controller and cloud controllers via a specialized service component.

A recent study showed importance of virtualized MAEC (vMAEC) platform for IoT-based application under the 5G network scenario [50]. A novel architecture was proposed herein that included container-based virtualization technology (CVT) to assist vMAEC applications in IoT. The architecture used OVS to support a range of standards including encapsulated RSPAN (ERSPAN), sampled flow (sFlow), and remote SPAN (RSPAN). A data plane development kit (DPDK) was involved to overcome the smaller throughput limitation. Overall architecture was simulated both the cache and through modes. It was found that incorporation of CVT reduced edge-cloud communication latency by 30

Multi-tenancy is another vital characteristic that 5G network should have. In that case, SDN/NFV orchestration must be done in seamless manner. TelcoFog architecture was thus paved to assimilate the multi-tenancy approach into the 5G networking. The architecture utilized ONF transport API (T-API) to enable interoperability among multiple vendors of telecommunication service sector. Multi-domain SDN controllers were deployed to handle 5G network complexity and vivid heterogeneity [51]. Novel P2P and hierarchical control were jointly orchestrated to use the 5G network slicing for quality IoT application developments. Deployment of several services in 5G network is not enough if they are not properly checked. Thus, a check point should be included into the 5G network so that DevOps and related IoT applications could be verified. [52] proposed a novel verification and validation (V&V) concept for checking the 5G networking services and IoT-based applications. The V&V concept was incorporated into the 5GTANGO architecture to accelerate DevOps service model within the third-party telecom operators. The architecture also enabled new business models to get virtualized so that time-to-market could be reduced. Thus, this architecture reduced the entry barrier for the external service providers to play network QoS. IoT applications were significantly benefited with this approach. The architecture used public catalogues to aware vendors and 5G customers about the available services. The service mitigation was formulated through the OSS, VIM, SD-WAN and WIM infrastructural platforms. Fig. 15 presents the 5GTANGO architecture.

8.3. Hybrid satellite–cellular architecture

4G, 5G are obviously great networking paradigms. However, satellite networks have not been given adequate importance so far in this journey of technological advancement. SDN/NFV could be implemented alongside the satellite infrastructure toward development of smarter hybrid cellular structure. [53] presented a hybrid cellular architecture that employed two layers of abstraction, such as, (i) terrestrial domain, and (ii) satellite domain. Terrestrial domain implied the NFVI-point of presence (NFVI-PoP) that involved computer clusters, SDN switches, and non-SDN routers. Thus, terrestrial orchestrator module i.e. network management system (NMS) paved VIM and WAN manager to connect NFVI-PoP. Customer front-end was connected with the terrestrial domain and federated manager. Federated manager was connected with satellite domain in terms of satellite orchestrator i.e. satellite NMS. The satellite NMS talked to NFVI-PoP or satellite gateways via SDN/NFV-enabled satellite which was associated to the satellite control center (SCC) via a VIM. Customer networks got effective satellite terminals that would help edge connected IoT device and the SCC was provisioned by the cloud end. The architecture was developed using OpenFlow switch and Wi-Fi communication to communicate with content server which was in tun associated with the OpenStack and OpenDaylight tools to orchestrate the OpenStack compute cluster. The work used OpenSAND satellite terminal, emulator, and OpenFlow virtual switch to illustrate the proof of concept topology. Fig. 16 presents the abstraction of satellite-based SDN/NFV architecture. Table 7 presents the comparative analysis of surveyed articles in terms of next generation cellular architecture.

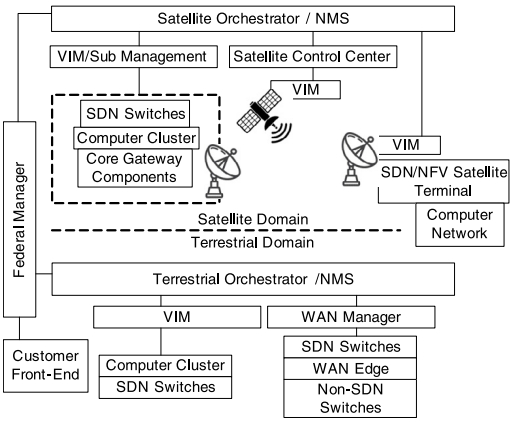

Fig. 16. Satellite-enabled SDN/NFV architecture.

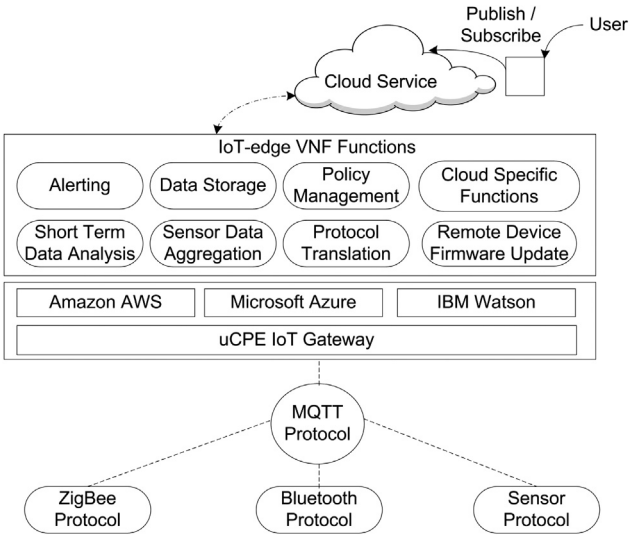

Fig. 17. uCPE centric IoT-edge gateway architecture.

9. Applications and test bed architectures

9.1. NFV for heterogeneous resources

In [54], an SDI-based architecture was evaluated while aiming at the study was to enable NFV service chains for employability into the heterogeneous cloud service provisioning. A multi-layer cloud framework was developed with IoT-based devices and diverse set of computing modules. NFVs were implied in multiple forms to communicate with the proposed smart applications on virtualized infrastructure (SAVI). The SAVI testbed was divided into three layers i.e. (i) physical resources, (ii) open API, and (iii) external application and services layer. Physical resource layer consisted of IoT devices and acted like edge paradigm. Open API layer hosted the SDI manager that worked with OpenStack, OpenFlow controller, and monitoring service. Several virtual resources were deployed in this layer that included SNMP, OFP, and IPMI.

9.2. Cluster SDN-IoT testbed

A cluster SDN-based IoT testbed was developed to investigate how effectiveness of such testbed could be formulated into reality [55]. The underlying architecture used a novel SDN cluster head (SDNCH) to leverage IoT-based rules and NFV routing functions to control every EC controller. An OpenFlow centric network was emulated to integrate model driven service abstraction layer (MD-SAL) into the study. Multiple SDNCH were deployed into the framework to coordinate the domain of action, whereas IoT gateway node (GN) acted like bridging up the information between the cluster of each SDNCH. This work advocated the cluster-wise impact of SDN/NFV inclusion into the edge-cloud scenario.

9.3. Energy efficient M2M network testbed

In recent past, IPv6 over low power wireless personal area network (6LoWPAN) has been constantly used in many wireless machine-to-machine (M2M) network development. IPv6 could be seen as a good candidate for development similar network ecosystem with more number device connectivity. IoT is envisaged to have billions of devices connected with each other, thus shortage of network address may be fulfilled by IPv6 protocol. In this regard, an architecture was developed by comprising 6LoWPAN that integrated SDN/NFV for edge-cloud communication traffic management virtualization [56]. The architecture was implemented by using 6LoWPAN protocol stack where IEEE 802.15.4 was utilized as MAC and physical layers. A customized SDN flow table was included to support the data flow within the M2M communication, while SDN/NFV M2M gateway was deployed in accordance to PAN coordination to serve the remote user data upload scenario. Incorporation of SDN/NFV paradigm increased the nodes' lifetime by 65% and simultaneously provided energy efficient approach.

9.4. IoT edge gateway

With the growth of IoT, demand has been increased to guarantee the QoS via reduction of latency between edge-cloud communication, real-time service aware network system, and secure data transmission. User CPE (uCPE)-based edge gateway has become a demand of the time. Thus, a study developed such IoT-based edge-gateway that worked on uCPE to cater the earlier said requirements [57]. Various SDN/NFV functions were facilitated such as, sensors data aggregation, data storage, altering the user about any mishap, policy management, protocol translation, and cloud specific function realization. The IoT-gateway was connected to the Amazon IoT AWS where lambda function was delivered with help of AWS Greengrass core facility. MQTT protocol was deployed to make the data flow easier between the SBI and NBI. Bluetooth modules, ZigBee module and temperature-humidity sensor were assimilated together to setup the uCPE. The development provided a realistic gateway that paved communication between multiple cloud services, such as, Greengrass, Azure, and IBM's Watson cloud. Fig. 17 presents the uCPE centric IoT-edge gateway architecture.

9.5. Community network management

As the technology is getting smarter, community service should also be smarter. Future telecom organization shall leverage smart supporting service that include multiaccess, multitenant, and multiservice to satisfy its customers' needs. Virtual attributes may be incorporated into this paradigm that may improve the community aware infrastructure in near future. A study revealed that such direction of research could be realized by including wireless-optical broadband access network WOBAN) with existing SDN/NFV facilities [58]. In this work, optical line terminals (OLTs) were used in conjunction to optical network unit (ONU). Passive optical network (PON) facility was deployed with REST/HTTP protocol suites with OpenFlow-based platform. OvSwitch, ethernet, and Wi-Fi wireless Aps were successfully mitigated with the SDN controller where dynamic host configuration protocol (DHCP), routing, and QoS provisioning were formulated. In this architecture, smart community services were made in two ways, (i) centralized

Table 8
Comparative analysis of applications and test bed architectures.

Paper	Objective	Novel contributions	Advantages/Limitations
[54]	SDN/NFV ecosystem for heterogeneous IoT resources test bed	SAVI test bed deployment, Open API layer hosted the SDI manager that worked with OpenStack, OpenFlow controller integration	SNMP, OFP, IPMI implementation
[55]	Cluster SDN-IoT test bed development	SDNCH, EC, MD-SAL with OpenFlow integration	SDN/NFV cluster mitigation
[56]	Energy efficient M2M network test bed for IoT devices	6LoWPAN integration, SDN flow-table with MAC integration	65% increase in life-time
[57]	IoT-edge gateway deployment	Sensors data aggregation, data storage, altering the user about any mishap, policy management, protocol translation, and cloud specific function realization	uCPE mitigation with Greengrass, Azure, ad IBM's Watson cloud
[58]	Community network management using WOBAN	OLT, ONU, PON integration with REST/HTTP based OpenFlow suite	I-CSCF, S-CSCF and MGW inclusion
[59]	Multi-level centralized access deployment	ACTP, XACML interaction with SDN/NFV ecosystem	Authentication, anonymity, data integrity was tested
[60]	Optical transport network test bed development	ADRENALINE project initiated, scalable QoS intervention, EOS and SDOT module integration	QoS and scalability tested
[61]	Mobile data traffic minimization test bed using optical transport network	ADRENALINE project involved	S-BVT and AS-PCE sliceable capacity tested
[62]	Future mode operation test bed development	OPEX and SELFNET management modules integration	SDN-SON and VIM layer correlation tested
[63]	Efficient MEC servicing application development	SIMECA, SDN-BN, SDN-EN were deployed	Light-weight header translator tested
[64]	Legacy network upgradation application deployment	CDPI, NBI, SBI, SDN data path and SDN controller modules integration	ATM/LANE, BCF routing server tested
[65]	BlackSDN implementation test bed	DistBlackNet test bed provisioned, BlackIoT ecosystem harnessed	NEV, TTP, NFVI were investigated against the black SDN-IoT mitigation
[66]	Large scale network management orchestration using SDN/NFV	GFS, GOM centric business application development	Dynamicity and flexibility of the system perceived

and (ii) distributed. In centralized method, NFV functions like, interrogating called call/session control functions (I-CSCF), serving called call/session control functions (S-CSCF), media gateway (MGW), and MGWF were involved at the cloud/serving side. Whereas, it was opposite for distributed approach. Thus, smart community aware servicing could be harnessed in the low cost and flexible fashion.

9.6. Multi-level centralized access

Legitimate access into the cloud is an important factor to make the network services better. A recent study implemented an access control policy tool (ACPT) to provide multi-level centralized access to the cloud by suing SDN/NFV orchestration [59]. The architecture performed following level-wise activities that includes (i) IoT device registration, (ii) user registration, (iii) edge node registration, and (iv) access policy preparation. After completing these activities, second phase was initiated that included two levels of services, such as, data dissemination of IoT device and users' request for device access. Extensible access control markup language (XACML) was utilized to levy the ACPT protocol implementation. The architecture was analyzed against the performance analysis that took following parameters under consideration, such as, authentication, efficiency, anonymity, access control, confidentiality, and data security. Thus, the model truly provided the multi-level access in centralized manner.

9.7. Optical transport network testbed

Optical communication plays a significant role in SDN/NFV ecosystem. The main usp of optical transport network is to provide high speed network connectivity which is a strong need of existing IoT. Thus, a testbed i.e. ADRENALINE was developed to integrate multi-layered distributed computing services under the aegis of IoT. The testbed realized the necessity of flexible, cost-effective, and effective SDN-enabled optical network aggregation via switching facility while leveraging QoS in high-scalable fashion [60]. By inclusion of such test bed mobile data traffic was lowered 1000 times which was a fascinating result obtained

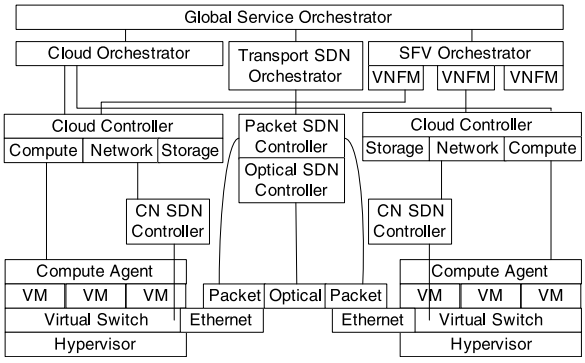

Fig. 18. Optical-multiple cloud controller architecture.

from the testbed [61]. Multi-tenant service providers were deployed at top of the underlying architecture. The architecture mitigated micro-datacenter controller, SDN packet modules, SDN packet controllers, SDN-based optical transmission module (SDOT) along with EOS optical transmitter. Myriad active state PCE (AS-PCE) and 5G enabled transceivers such as sliceable bandwidth variable transceiver (S-BVT) was seamlessly integrated into the proposed architecture. Deployment of ADRENALINE paved a new way of high-speed edge-cloud communication facilitation under the IoT-based scenario. Fig. 18 presents the multiple cloud controller under the optical network.

9.8. Future mode operation approach

OPEX is a key performance indicating factor of any networking system. Same is true for the IoT-enabled application domain, Thus, an efficient future mode selector architectural approach might improve existing issues in OPEX management. This would certainly reduce the organizational cost in terms of operation management and dissemination. A recent study showed how the SELFNET architecture could solve

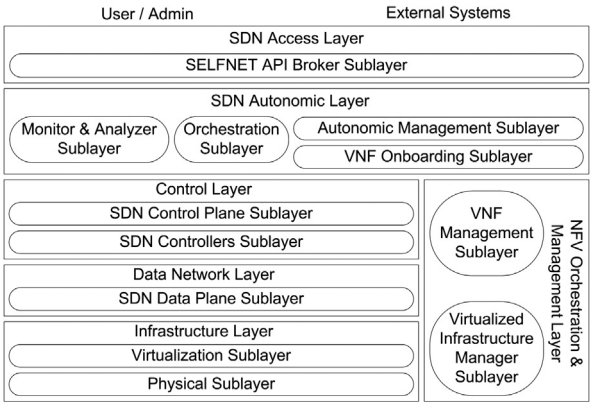

Fig. 19. SELFNET architecture.

the OPEX minimization of any SDN/NFV orchestrated system [62]. In this architecture, a five layered approach was presented. As other architectures, lowest layer was infrastructure layer that consisted of physical and virtualized sublayers. Next layer was data network layer where SON-based data plane sublayer came into the play. Next layer was control layer, where SDN-SON combined sublayers were deployed. Top two layers were based on SON assisted autonomic and access layer, respectively. The job of these layers was to cater the monitoring, analysis, and orchestration services to the underlying layers. An NFV orchestrated VIM layer was vertically existed along with the bottom three layer. The overall design of the architecture dealt with the organizational as well as user level query mitigation. Fig. 19 presents SELFNET architecture.

9.9. Mobile edge cloud servicing

Success of an IoT-based system depends on the efficient integration between various sub-systems and networking paradigms such as, SDN/NFV, edge, and cloud. SIMECA is such an architecture which was presented to solve the integration issues between different paradigm of network [63]. The insights of SIMECA was based on following four aspects, such as, (i) best-effort packet forwarding for high quality QoS delivery, (ii) service and mobility function, (iii) novel packet header translation scheme, and (iv) P2P communication between each of the nodes. The architecture of SIMECA used SDN-based BS, SDN-edge network, edge-cloud facility, and ISA. The light-weight header translator routed device identity and routing identity while packet forwarding. The actual achievement of the architecture was laid into the service provisioning of a large number of IoT-based device in a heterogeneous cellular network.

9.10. Upgradation of legacy networking

Legacy networking infrastructures depend on the old networking architecture, complex integration approach, minimal policy retention, and agility of network. Thus, SDN/NFV could be used in existing solutions to harness the disrupting elements of the legacy networks. Thus, novel type of architecture was formulated to provision these issues in seamless manner [64]. The architecture involved SDN control to data plane (CDPI), NBI, SBI, SDN data path and SDN controller. Distributed data and control planes were facilitated with intervention from the separated and hybrid planes. Different functional planes were tested against the developed architecture where ATM/LANE and route server were validated by utilizing OpenFlow. Big cloud fabric (BCF) was included into the architecture to communicate with the big switch networking infrastructure being highly available. Thus, the architecture paved a new direction toward upgradation of legacy networking for sake of IoT and related smart technologies.

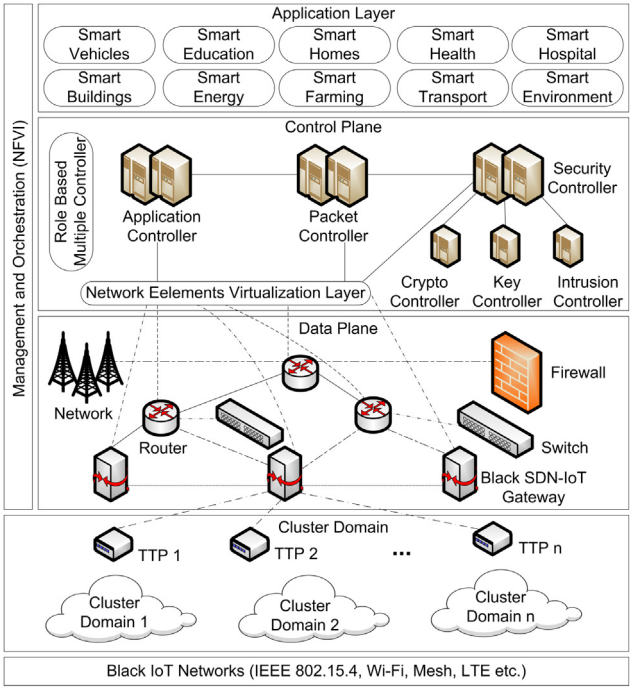

Fig. 20. DistBlackNet architecture.

9.11. Black SDN implementation

SDN is an intelligent technology paradigm which may improve reliability, security, trust, and privacy for any deployed application. Smart city has attained great importance in terms of usefulness and better living prospects. Thus, inclusion of robust and highly secure SDN/NFV combination would enhance the earlier said factors. DistBlackNet was recently presented to improve integrity, confidentiality and availability of any virtualized services at the edge-end [65]. The architecture had three layers of abstractions such as, (i) cluster domain, (ii) network element virtualization (NEV) layer (divided into data and control plane), and (iii) application layer. Black IoT-based networking tools were used at the bottom most layer while leveraging trusted third party (TTP) approach. Novel, black SDN-IoT gateway was incorporated into the data plane of the next layer which supported the control plane by involving router assisted services to the crypto controller, key controller, and intrusion controller. Packet and application controllers paved the NFVI vertical while mitigating the smart city application in easy and efficient way. Fig. 20 presents the DistBlackNet architecture in details.

9.12. Large scale network management

Vulnerable situations may arise at any point of time in the society and natural aspect. Thus, it would be great if large-scale virtualization services could be provided to such scenarios while utilizing distributed gateways, dynamic SDN/NFV facilities and edge-cloud integration under the aegis of IoT. In [66], a novel business model was proposed to cater the large-scale networking service provisioning with help from IoT gateway, IoT provider, and end-user applications located at the edge. The IoT gateway domain was consisted with VIM, VNFM, VNF catalogue, VNF agent, gateway function store (GFS), and gateway overlay manager (GOM). Each of these elements got associated with the IoT provider domain via IoT provider agent. An IoT-based MANET-VNFI sublayer was introduced to interconnect the overlay functions and applications. Although, the architecture was divided into three domains, vertically, control and forwarding planes hosted the architecture. The prototype of the architecture proved its efficacy by showing

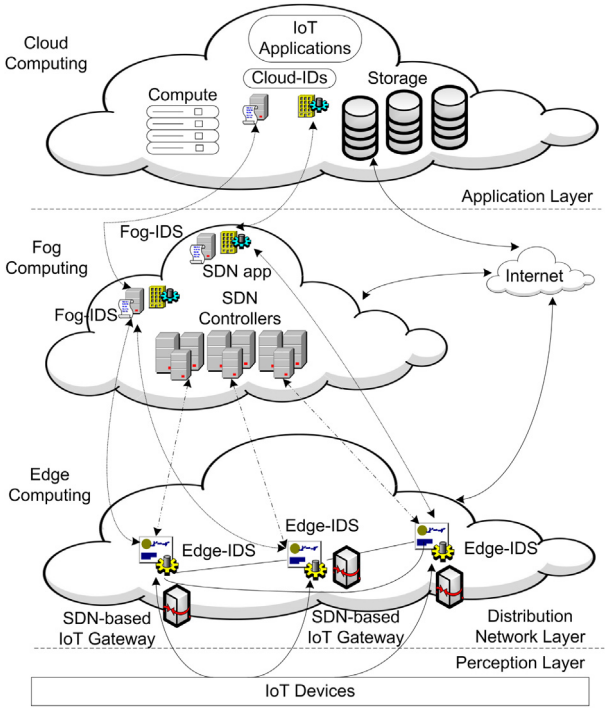

Fig. 21. NIDS architecture.

the dynamicity and flexibility characteristics. Thus, the architecture was truly a scale agnostic approach that must be inculcated to enrich the large-scale virtualization into reality. Table 8 presents the comparative analysis of surveyed articles in terms of application and test bed centric architecture.

10. Security aware architectures

10.1. Collaborative and intelligent intrusion detection

Intrusion into internetwork infrastructure is a common thing now-a-day. The situation may worsen when distributed environment like IoT come to play into the scene. It may also get exaggerated if SDN/NFV are involved. Thus, to detect any such intrusion in the IoT-based system, novel technique must be framed. Fortunately, [67] presented a SeArch architecture to solve this issue. The architecture was based on the collaborative and intelligent intrusion detection system (NIDS) that yielded outstanding performance to detect anomalies into the system. SeArch used machine learning technique to identify the intrusion. The architecture was composed of two layers, (i) distribution network layer, and (ii) application layer. Distribution network layer acted on top of perception layer which accommodated the IoT devices for receiving sensor data through IoT gateway. Thus, perception layer emulated the edge of the network. The distribution network layer incorporated all types of SDN controllers that included edge intrusion detection system (IDS), SDN apps, and internetwork protocols. As usual, application layer hosted the cloud IDS and computational facilities. Thus, the architecture paved all three layers of IDS into the SDN/NFV ecosystem. By doing so, efficient system resource management became possible. Approximately, 95.5% of intrusions were successfully detected by this architecture. Fig. 21 presents NIDS architecture.

10.2. Integrated protection

Unexpected attack on any network system can severely undermine the overall system's performance. IoT is thus a very soft target for such attacks due its dependency over the low-cost and resource-constrained device pool. An integrated protection scheme would hence possibly improve the resilience toward to attacks on IoT-sub systems. SDN/NFV could be thought of the Savior in this regard. In [68], a related protection architecture was proposed and validated that came into the force with two layered approach, (i) security enforcement plane and (ii) security orchestration plane. Security enforcement plane provided facilities for IoT-based devices via IoT controller, SDN controller and NFV MANO. VIM, VNF manager and NFVO came together to serve the enforcement in two sub layers, namely VNF and infrastructure domain. The enforcement was entrusted with the incorporation of security orchestration plane that paved monitoring, reacting, and policy interpreting mode of applications. Repositories were created to store security policies and security enablers to successfully orchestrate integrated security for the underlying IoT ecosystem.

10.3. AAA service provisioning architecture

Security of any system could be measured by the authentication, authorization, and accounting (AAA) feature set. IoT is not an exception to this rule when SDN/NFV paradigm are in the place. The importance of AAA feature lies on the timely deployment of network security functions (NSF) for mitigating a holistic and smart network security adopter. [69] leveraged an ANASTACIA architecture that was converted into more secure AAA-aware framework by involving key management framework (KMF). NFV MANO was sincerely integrated with the proposed architecture for harnessing the power of the extensible authentication protocol (EAP). The architecture was enriched with virtual AAA (vAAA) functionality which was seamlessly positioned with the virtual bootstrapping VNF facility. Policy decision point (PDP) and OVS were bootstrapped with the underlying IoT broker service. Further, datagram transport layer security (DTLS)-based channel protection feature was augmented to this architecture to wider the range of security on the IoT devices. Fig. 22 presents the AAA architecture.

Another study showed how vAAA could be used as channel protection proxy in the given scenario [70]. In this work, privileged-level access agreement (PAA) and protocol for carrying authentication for network access (PANA) were used to secure the communication channel. Virtual PAA (vPAA) was installed at the edge-end IoT devices while PANA was assimilated into the whole system starting from edge to cloud. The architecture was tested against 500 IoT devices that enforced DTLS facility within 30 s which is relatively less time to attack any device. Thus, the AAA security architecture was proven to be a good candidate for providing security under the edge-cloud interplay.

10.4. Emerging security mechanisms

An extensive study on emerging security mechanisms was recently performed to showcase various possible attacks on the SDN/NFV centric IoT environment and how to mitigate the attacks [23]. As found, a number of attacks have been imposed over the IoT-based ecosystem that includes, (i) hardware Trojan attack [71], (ii) replication attack [72,73], (iii) tampering attack [74,75], (iv) battery draining attacks [76,77], and (v) malicious code injection attack [78]. Several security threats were also paved on the IoT-based cloud network, that included (i) eavesdropping attack, (ii) denial-of-service attack [79–81], (iii) spoofing attack [82,83], (iv) man-in-the-middle attack [84], (v) routing attack [85–87], (vi) IoT cloud service manipulation, and (vii) security inter-working. IoT applications were also attacked by many types of threats, such as, malicious virus/worm [88], application data leakage [89], service logging failure [90], malicious scripts, phishing attacks, and inconsistent software patches [91–94].

Conventional security mechanisms for IoT ecosystem includes, (i) authentication and authorization [95–97], (ii) traffic filtering and firewalls [98,99], (iii) encryption protocols [100–103], and (iv) anomaly-based detection [104,105]. Recently, SDN-based security mechanisms were studied and tested where following features were considered,

Table 9
Comparative analysis of security aware architectures.

Paper	Objective	Novel contributions	Advantages/Limitations
[67]	Collaborative and intelligent intrusion detection in the SDN/NFV enabled IoT system	SeArch, NIDS, IDS correlation with SDN/NFV security layer	95.5% intrusion detection successfully
[68]	Integrated protection provisioning	Security enforcement plane and security orchestration plane mitigation	VIM, VNF manager and NFVO came together to cater the policy and integrated security layer orientation
[69]	AAA service provisioning architecture	ANSTACIA, KMF, EAP and NSF integration	IoT broker and DTLS incorporation tested
[70]	vAAA service provisioning architecture	PAA, vPAA, PANA modules integrated	500 IoT devices tested against DTLS
[23–26, 71–137]	Emerging security architecture [23], hardware Trojan attack [71], replication attack [72,73], tampering attack [74,75], battery draining attacks [76,77], malicious code injection attack [78], DoS attack [79–81], spoofing attack [82,83], man-in-the-middle attack [84], routing attack [85–87], malicious virus/worm [88], application data leakage [89], service logging failure [90], inconsistent software patches [91–94], decoupling software-hardware [127,129,137], on-demand scalability security tolerance [130,131], mobility support of NFV [132–134], and network service chaining [26,135–137]	IDS, firewall, DPI, encryption, authentication and authorization, and security SFC modules developed and tested	Minimization of security hazards in IoT centric SDN/NFV ecosystem

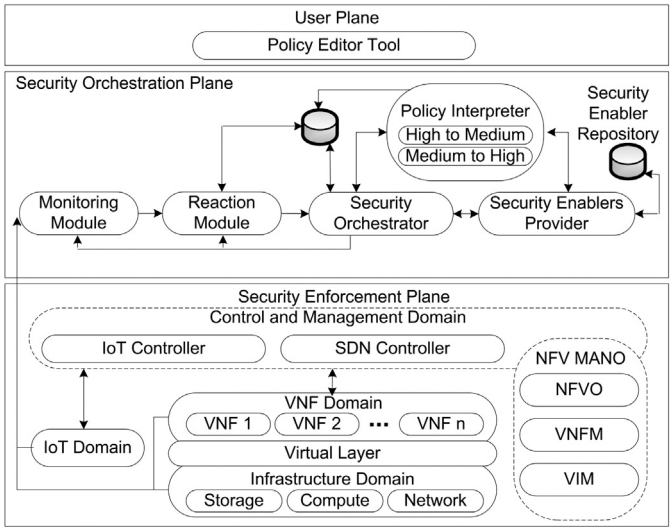

Fig. 22. AAA architecture.

such as, traffic isolation [106,107], centralized visibility approach [24, 108–112], dynamic flow control [113–116], host and routing obfuscation [117–120], and security network programmability [25,121–126]. Further, NFV security features were imposed over the IoT ecosystem that was followed by decoupling software-hardware [127–129], on-demand scalability security tolerance [130,131], mobility support of NFV [132–134], and network service chaining [26,135–137].

It was comprehended that security should be enhanced in the domains like IDS, firewall, deep packet inspector (DPI), encryption, authentication and authorization, and security SFC. To fill-up the gaps in these areas, more research should be paved toward secure SDN/NFV platform development by identifying SDN/NFV threats for IoT network, optimal selection of SDN/NFV security schemes, and facilitation of customized network slicing approach into the existing system. Architectural notions should be employed in the given scenario to address the security issues in more strategic and cost-effective way. Table 9 presents the comparative analysis of surveyed articles in terms of security aware architecture.

11. Future direction

11.1. Standardization

Standardization has been a long-cherished dream in IoT-based technology domain. It is true that a portion of communication technologies has been given consideration to get standardized. But, a major area of such domain is not touched till date. Standardization could be a great point to start with for mitigating earlier mentioned issues and challenges in IoT-based SDN/NFV infrastructure for edge-cloud interplay. Standardization process may be started with architectural point of view, where vast discrepancies are seen [138]. Modeling and layering of architectures for all types of IoT-based application should be categorically framed to streamline the development process in this domain of study.

11.2. Deployment of network services

Network services are deployed based on intentions of the telco service providers. Governments, in most of time just derive a policy is leave everything to the telcos. Such behavior is bringing devastating affects into the networking service provisioning in real-time and industrial domain. A clear understanding should be paved and agreed upon by all the stakeholders in the IoT-based SDN/NFV edge-cloud interplay so that a common way of deployment of VNFs could be leveraged [30]. A stringent policy should be governed and testified for all the telcos and service providers about the process of deployment of networking services.

11.3. Improving programmability

Programming of software-defined networks plays a very important role to ascertain the QoS of the underlying network and system. Over-the-air (OTA) programming notion is in practice since last few years. OTA programming capability should be improved by including novel language specific rules and

11.4. New business model

Business model drives new direction of growth in technology domain. Simplistic view of existing business mindset should be reconsidered to cope up with the new challenges for upcoming SDN/NFV framework in the edge-cloud amalgamation. As discussed earlier, new challenges are about to get introduced in the envisaged IoT-base infrastructure. Business models must be carefully designed to formulate the issues arisen. It is important to apprehend that demand of dynamic customization of network service need to be mitigated by utilizing of architecture-wise development of business strategies.

11.5. Technology interaction

IoT plays with a range of different technologies, such as, communication, networking, hardware platform, edge ecosystem, cloud service etc. Thus, technology interaction could be seen as a possible way out of the challenges identified. Appropriate amalgamation of technologies and their interaction with each other may widen the way of envisaged edge-cloud integration. Virtualized frameworks and services need to be well interacted for harnessing the SDN/NFV familiarization with the IoT ecosystem.

11.6. Management perspective

SDN controller and management could be a great avenue to improve the discussed scenarios. Each of the SDN/NFV architecture plays with SDN controllers to manage the underlying service provisioning and activity mitigation in the edge-cloud interaction perspective. Such managerial capacity needs to be well formulated so as to get the actual power of SDN controlling feature in real-life IoT-based applications. Future of IoT driven technology domain needs perfect blending of SDN controller/manager acts with the SBI and NBI ends.

11.7. Control and application layering

As discussed earlier, controlling of the network may improve the efficiency of underlying applications. SDN/NFV formulation always depend on the controller and application layering notions to serve a number of function virtualizations. It would be great if layering of control and application could be managed and deployed with utmost stringent manner. Such, layering of control and application would obviously enrich the envisaged growth of edge-cloud communication.

11.8. Blockchain

Blockchain is a recently introduced technology that provides highly secure, chain-wise decentralized block storage facility. Blockchain is seen as a key enabler of futuristic technology revamp which has been successfully tested with IoT, edge, and cloud environments. In all the cases, blockchain has proven its efficiency toward normalization and privacy aware service mitigation in highly decentralized manner. Consensus mechanisms have been deployed in various IoT-based applications to protect the privacy and anonymity of the underlying data processing. Thus, blockchain may be implied over the SDN/NFV framework to successfully co-opt with the edge-cloud ecosystem.

11.9. AI and machine learning layering

Artificial intelligence (AI) is not a new term, neither machine learning (ML). However, recent buzz about ML has attracted a large portion of research and industry netizen to deploy ML in vast number of applications. IoT has been a good premise where ML has shown its power of improvement in terms of decision making and efficient predictive behavior. Thus, SDN/NFV paradigm may be juxtaposed with the novel ML techniques along with IoT-enabled edge-cloud scenario to predict when and how to virtualize network functions in proper way.

11.10. IoT identity naming system

IoT places billions of devices within its umbrella that lacks naming facility. Without a prominent naming opportunity, it would be very tough for the telcos to manage the large number of IoT devices. IoT identity naming system (IDNS) is such a technique which may enhance the naming conventions of IoT devices to get easily identified and routed for data transmission in edge-cloud type of distributed environment.

11.11. Dew computing

Dew computing is a recent inclusion into the computing paradigm that aims at bringing all types of network services to the users' end. Closer than edge, dew computing is envisaged to be positioned nearby the users' periphery in form of personal assistance services [139–141]. Dew computing aims at minimizing the communication delay between conventional edge-cloud framework by incorporating highly context-aware and dew server assisted facilities that would help the users to get informed and assisted with dew computing-based services. It ensures to use super-flexible P2P communication directly between the edge and cloud to minimize the communication gap. If required information is not responded from the dew server, it may search the same in the dew cluster i.e. nearby dew community or may further look for tenant-aware cloud repositories. Dew computing may be seen as an alternative to upgrade existing network service provisioning in the SDN/NFV framework [142,143]. IoT-based application would get direct benefit from this approach while assimilating a novel dew of things service architecture.

11.12. Next generation IoT

SDN/NFV architecture should be integrated with big data analytics engine in an IoT-based scenario to enhance multimedia data processing in seamless manner [144]. We may think of integrating spatio-temporal big data analysis of vehicular notions in coalition oriented approaches [145,146]. Ambient intelligence spectrum might be investigated to get associated with the Bayesian-IoT augmentation in this context [147]. On the other hand, next generation SDN/NFV orientation must cater the dynamic channel scheduling in the cloud centric wearable healthcare sectors [148,149]. Smart city augmentation with support from the multi-tenant cloud-assisted smart grids could be envisaged [150]. Thus, we can conclude that next generation IoT would be investigated to get implied with the SDN/NFV architecture provisioning aspects. Further, new architectures should be developed in and around the existing SDN/NFV architecture to make the futuristic systems worthy for the flexible network virtualization.

11.13. Lessons learned

Despite of all such efforts a set of gaps are yet not fully comprehended or paved that includes the answers of the following research questions,

- (RQ1) how does state-of-the-art architecture under the aegis of SDN/NFV integrated IoT-based edge-cloud service look like? It includes (a) sensor-based service provisioning, (b) service function chain mapping, (c) content delivery framework, (d) end-to-end networking, (e) intent-based management, (f) information centric networking service, (g) object virtualization, (h) scalability and flexibility, (i) crowd-sourcing aspect, (j) industrial orientation, (k) quality of service mitigation, (l) next generation servicing, (m) energy efficiency, (n) multi-access edge provisioning,
- (RQ2) how to solve next generation networking and cellular service through novel architectures by employing SDN/NFV, IoT and edge-cloud ecosystem? It includes (a) 4G, (b) 5G, (c) hybrid satellite–cellular,
- (RQ3) what type of application and test-bed architecture should be deployed? It includes, (a) NFV-based heterogeneity, (b) clustered SDN-IoT, (c) machine to machine test-bed development, (d) gateway development, (e) community wise networking, (f) optical transportation, (g) mobile edge-cloud servicing, and (h) large scale networking,
- (RQ4) which genre of security feature should be implied over the SDN/NFV aware virtualization mitigation? It includes, (a) collaborative and intelligent intrusion detection, (b) integrated protection mechanism, and (c) authentication, authorization, and accounting-based security facilitation.

Upon completion of the comparative study on various literatures published in different reputed avenues, it seems very clear to mention that to our best of knowledge none of the works exist in public domain that discusses and depicts in-depth and comprehensive study on need and appropriateness on the SDN/NFV integrated architectures for IoT-based edge-cloud interplay. All surveys except Farris et al. discussed and paved mainly SDN oriented approaches for mobile network, 5G, cellular, fog, edge, MEC, or next generation network design and development. Farris et al. presented a nice article but it only focuses on the DDoS attack-based architecture provisioning.

We should comprehend the difference between the MEC and the next generation cellular architecture as mentioned in this study. The main characteristics of MEC relies on the following factors, such as, (i) improved cost savings, (ii) better efficiency, (iii) innovative service offerings, (iv) ensuring distributed computing, (v) new use cases opportunities. On the other hand, next generation cellular architecture depends on the following architectures, such as, (i) energy efficient spectrum usage, (ii) extremely reliable service mitigation, (iii) ultra-low latency application development, (iv) mobility-aware dissemination of application provisioning, and (v) cognitive inclusion.

Thus, we can apprehend that our presented work is novel and unique than other studies in terms of (i) overall orientation of SDN/NFV centric practices in IoT domain, (ii) state-of-the-art comprehensions on SDN/NFV architecture mitigation in edge-cloud assisted IoT scenario, (iii) next generation cellular architecture, (iv) applications and test-bed architectures, (v) security aware architecture, (vi) precise selection on key issues and future directions. Thus, our work provides new knowledge in the domain of SDN/NFV integrated need of IoT-based architectures for understanding how to solve the underlying challenges to meet the requirements to (i) minimize the communication delay, (ii) improve the QoS, and (iii) assist in fully virtualizing the pathway between edge and cloud [150].

We also focus on the inclusion of innovative AI-based techniques into the SDN/NFV orchestration under the edge-cloud enabled IoT scenario. Importance should be given on the network intrusion detection and classification use cases. Both the supervised and unsupervised learning methods could be implied. Similarly, cognitive radio networks and heterogeneous networks (HetNet) approach must be aligned with the SDN/NFV domain. Further, reinforcement learning might be applied into the network traffic control and self organizing cellular networks so that efficient integration with the IoT-based services might be significantly inferred.

12. Conclusions

In this study, we reviewed various literatures that deals with architectures to solve a range of problems identified by fellow researchers in multiple domains. We presented a state-of-the-art review on various architectural aspects in SDN/NFV specific virtualization mitigation by involving IoT in edge-cloud interplay. We also discussed how next generation mobile and cellular service can be virtualized by incorporation of architecture-centric approaches. Next, we delivered in-depth analysis and discussions on necessity and solution strategy toward solving application development and test-bed design perspectives. Lastly, we depicted key open research challenges that should be catered by involving prescribed future directions. Thus, overall review paves an important and very crucial knowledge toward SDN/NFV enabled network service virtualization by enabling architecture centric approaches while including IoT, edge and cloud to improve network services.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] T.M.C. Nguyen, D.B. Hoang, T. Dat Dang, Toward a programmable software-defined IoT architecture for sensor service provision on demand, in: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, 2017, pp. 1–6, http://dx.doi.org/10.1109/ATNAC.2017.8215419.

[2] A. Zamani, S. Sharifian, A novel approach for service function chain (SF) mapping with multiple SFC instances in a fog-to-cloud computing system, in: 2018 4th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), Tehran, Iran, 2018, pp. 48–52, http://dx.doi.org/10.1109/ICSPIS.2018.8700535.

[3] J. Bae, J. Kim, An experimental continuous delivery framework for smartx-mini IoT-cloud playground, in: 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, 2016, pp. 348–350, http://dx.doi.org/10.1109/ICOIN.2016.7427129.

[4] S. Kim, J. Kim, Enabling operation data visibility for smartx-mini IoT-cloud playground, in: 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, 2016, pp. 428–430, http://dx.doi.org/10.1109/NETSOFT.2016.7502480.

[5] N. Oguchi, X. Wang, P. Palacharla, T. Ikeuchi, Seamless network service orchestration across on-premises and cloud infrastructures, in: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, 2017, pp. 1–2, http://dx.doi.org/10.1109/NFV-SDN.2017.8169863.

[6] P. Habibi, S. Baharlooei, M. Farhoudi, S. Kazemian, S. Khorsandi, Virtualized SDN-based end-to-end reference architecture for fog networking, in: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, 2018, pp. 61–66, http://dx.doi.org/10.1109/WAINA.2018.00064.

[7] H. Truong, N. Narendra, SINC - An information-centric approach for end-to-end IoT cloud resource provisioning, in: 2016 International Conference on Cloud Computing Research and Innovations (ICCCRI), Singapore, 2016, pp. 17–24, http://dx.doi.org/10.1109/ICCCRI.2016.12.

[8] W. Cerroni, et al., Intent-based management and orchestration of heterogeneous openflow/IoT SDN domains, in: 2017 IEEE Conference on Network Softwarization (NetSoft), Bologna, 2017, pp. 1–9, http://dx.doi.org/10.1109/NETSOFT.2017.8004109.

[9] R. Ravindran, Xuan Liu, A. Chakraborti, Towards software defined ICN based edge-cloud services, in: 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, CA, 2013, pp. 227–235, http://dx.doi.org/10.1109/CloudNet.2013.6710583.

[10] H. Zhu, C. Huang, IoT-B & b: Edge-based NFV for IoT devices with CPE crowdsourcing, Wirel. Commun. Mob. Comput. (2018) 3027269, http://dx.doi.org/10.1155/2018/3027269, 15 pages.

[11] G. Hatzivasilis, K. Fysarakisa, O. Soultatosa, I. Askoxylakisa, I. Papaefstathioub, G. Demetriouc, The industrial internet of things as an enabler for a circular economy hy-LP: A novel iIoT protocol, evaluated on a wind park's sdn/nfv-enabled 5G industrial network, Comput. Commun. 119 (2018) 127–137, http://dx.doi.org/10.1016/j.comcom.2018.02.007.

[12] C.A. Ouedraogo, E. Bonfoh, S. Medjiah, C. Chassot, S. Yangui, A prototype for dynamic provisioning of qos-oriented virtualized network functions in the internet of things, in: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, 2018, pp. 323–325, http://dx.doi.org/10.1109/NETSOFT.2018.8459955.

[13] B. Nguyen, N. Choi, M. Thottan, J. Van der Merwe, SIMECA: SDN-based IoT mobile edge cloud architecture, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, 2017, pp. 503–509, http://dx.doi.org/10.23919/INM.2017.7987319.

[14] A. Mimidis, et al., The next generation platform as a service cloudifying service deployments in telco-operators infrastructure, in: 2018 25th International Conference on Telecommunications (ICT), St. Malo, 2018, pp. 399–404, http://dx.doi.org/10.1109/ICT.2018.8464838.

[15] N. Dinh, Y. Kim, An energy efficient integration model for sensor cloud systems, IEEE Access 7 (2019) 3018–3030, http://dx.doi.org/10.1109/ACCESS.2018.2886806.

[16]].P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, T. Taleb, Survey on multi-access edge computing for internet of things realization, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2961–2991, http://dx.doi.org/10.1109/COMST.2018.2849509.

[17] Mamdouh. Alenezi, Mamdouh alenezi khaled almustafa khalim amjad meerja cloud based SDN and NFV architectures for IoT infrastructure, Egypt. Inform. J. 20 (2019) 1–10, http://dx.doi.org/10.1016/j.eij.2018.03.004.

[18] O. Salman, I. Elhajj, A. Kayssi, A. Chehab, Edge computing enabling the internet of things, in: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, pp. 603–608, http://dx.doi.org/10.1109/WF-IoT.2015.7389122.

[19] J. Pan, J. McElhannon, Future edge cloud and edge computing for internet of things applications, IEEE Internet Things J 5 (1) (2018) 439–449, http://dx.doi.org/10.1109/JIOT.2017.2767608.

[20] Junfeng Li, Dan Li, Yirong Yu, Yukai Huang, Jing Zhu, Jinkun Geng, Towards full virtualization of SDN infrastructure, Comput. Netw. (2018) http://dx.doi.org/10.1016/j.comnet.2018.06.014.

[21] Zichuan Xu, Weifa Liang, Alex Galis, Yu Ma, Qiufen Xia, Wenzheng Xu, Throughpsut optimization for admitting NFV-enabled requests in cloud networks, Comput. Netw. (2018) http://dx.doi.org/10.1016/j.comnet.2018.06.015.

[22] VG. Nguyen, TX. Do, Y. Kim, SDN And virtualization-based LTE mobile network architectures: A comprehensive survey, Wirel. Pers. Commun. 86 (2016) 1401, http://dx.doi.org/10.1007/s11277-015-2997-7.

[23] I. Farris, T. Taleb, Y. Khettab, J. Song, A survey on emerging SDN and NFV security mechanisms for IoT systems, IEEE Commun. Surv. Tutor. 21 (1) (2019) 812–837, http://dx.doi.org/10.1109/COMST.2018.2862350.

[24] Qiao Yan, et al., Software-defined networking (SDN) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges, IEEE Commun. Surv. Tutor. 18 (1) (2016) 602–622.

[25] Celio. Trois, et al., A survey on SDN programming languages: toward a taxonomy, IEEE Commun. Surv. Tutor. 18 (4) (2016) 2687–2712.

[26] H. Hantouti, et al., Traffic steering for service function chaining, IEEE Commun. Surv. Tutor. (2018) 1.

[27] Ola. Salman, Imad. Elhajji, Ali. Chehab, Ayman. Kayssi, Ola salman imad elhajji ali chehab ayman kayssi IoT survey: An SDN and fog computing perspective, Comput. Netw. (2018) http://dx.doi.org/10.1016/j.comnet.2018.07.020.

[28] N. Bizanis, F.A. Kuipers, SDN And virtualization solutions for the internet of things: A survey, IEEE Access 4 (2016) 5591–5606, http://dx.doi.org/10.1109/ACCESS.2016.2607786.

[29] Iqbal Alam, Kashif Sharif, Fan Li, Zohaib Latif, Md Monjurul Karim, Boubakr Nour, Sujit Biswas, Yu Wang, IoT Virtualization: A Survey of Software Definition & Function Virtualization Techniques for Internet of Things, arXiv:1902.10910.

[30] Michel S. Bonfim, Kelvin L. Dias, Stenio F. L. Fernandes, Integrated NFV/SDN architectures: A systematic literature review, ACM Comput. Surv. 51 (6) (2019).

[31] J.H. Cox, et al., Advancing software-defined networks: A survey, IEEE Access 5 (2017) 25487–25526, http://dx.doi.org/10.1109/ACCESS.2017.2762291.

[32] Y. Zhao, W. Wang, Y. Li, C. Colman Meixner, M. Tornatore, J. Zhang, Edge computing and networking: A survey on infrastructures and applications, IEEE Access 7 (2019) 101213-101230, http://dx.doi.org/10.1109/ACCESS.2019.2927538.

[33] V. Nguyen, A. Brunstrom, K. Grinnemo, J. Taheri, SDN/NFV-Based mobile packet core network architectures: A survey, IEEE Commun. Surv. Tutor. 19 (3) (2017) 1567–1602, http://dx.doi.org/10.1109/COMST.2017.2690823.

[34] D. Saif, F. Arsiwala, I. Khanna, Software defined networking in next generation mobile backhauls: A survey, in: 2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, 2018, pp. 106–111, http://dx.doi.org/10.1109/5GWF.2018.8517068.

[35] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, W. Wang, A survey on mobile edge networks: Convergence of computing, caching and communications, IEEE Access 5 (2017) 6757–6779, http://dx.doi.org/10.1109/ACCESS.2017.2685434.

[36] J. d. J. Gil, J.F. Botero Vega, Network functions virtualization: A survey, IEEE Lat. Amer. Trans. 14 (2) (2016) 983–997, http://dx.doi.org/10.1109/TLA.2016.7437249.

[37] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. De Turck, R. Boutaba, Network function virtualization: State-of-the-art and research challenges, IEEE Commun. Surv. Tutor. 18 (1) (2016) 236–262, http://dx.doi.org/10.1109/COMST.2015.2477041.

[38] L.I. Barona López, .L. Valdivieso Caraguay, L.J. Garcí a Villalba, D. López, Trends on virtualisation with software defined networking and network function virtualisation, IET Netw. 4 (5) (2015) 255–263, http://dx.doi.org/10.1049/iet-net.2014.0117.

[39] F. Reynaud, F. Aguessy, O. Bettan, M. Bouet, V. Conan, Attacks against network functions virtualization and software-defined networking: State-of-the-art, in: 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, 2016, pp. 471–476, http://dx.doi.org/10.1109/NETSOFT.2016.7502487.

[40] S.T. Pandeeswari, S. Padmavathi, Role and impact of softwarization of networks and network functions in fog based IoT application architectures, in: 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 2018, pp. 1–4, http://dx.doi.org/10.1109/ICCIC.2018.8782311.

[41] Binh Minh Nguyen, Huan Phan, Duong Quang Ha, Giang Nguyen, An information-centric approach for slice monitoring from edge devices to clouds, Procedia Comput. Sci. 130 (2018) 326–335, http://dx.doi.org/10.1016/j.procs.2018.04.046.

[42] A. Leivadeas, G. Kesidis, M. Ibnkahla, I. Lambadaris, VNF Placement optimization at the edge and cloud, Future Internet 11 (2019) 69, http://dx.doi.org/10.3390/fi11030069.

[43] L. Atzori, J.L. Bellido, R. Bolla, G. Genovese, A. Iera, A. Jara, C. Lombardo, G. Morabito, SDN & NFV Contribution to IoT objects virtualization, Comput. Netw. (2018) http://dx.doi.org/10.1016/j.comnet.2018.11.030.

[44] J. Serra, L. Sanabria-Russo, D. Pubill, C. Verikoukis, Scalable and flexible IoT data analytics: when machine learning meets SDN and virtualization, in: 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, 2018, pp. 1–6, http://dx.doi.org/10.1109/CAMAD.2018.8514997.

[45] V.G. Vassilakis, I.D. Moscholios, B.A. Alzahrani, M.D. Logothetis, A software-defined architecture for next-generation cellular networks, in: 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, 2016, pp. 1–6, http://dx.doi.org/10.1109/ICC.2016.7511018.

[46] Khaled. Almustafaa, Mamdouh. Alenezi, Cost analysis of SDN/NFV architecture over 4g infrastructure, in: The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017), in: Procedia Computer Science, vol. 113, 2017, pp. 130–137, http://dx.doi.org/10.1016/j.procs.2017.08.328.

[47] J. Costa-Requena, et al., SDN And NFV integration in generalized mobile network architecture, in: 2015 European Conference on Networks and Communications (EuCNC), Paris, 2015, pp. 154–158, http://dx.doi.org/10.1109/EuCNC.2015.7194059.

[48] T. Choi, T. Kim, W. TaverNier, a. Korvala, J. Pajunpaa, Agile management of 5G core network based on SDN/NFV technology, in: 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 840–844, http://dx.doi.org/10.1109/ICTC.2017.8190795.

[49] S. Fichera, M. Gharbaoui, P. Castoldi, B. Martini, A. Manzalini, On experimenting 5G: Testbed set-up for SDN orchestration across network cloud and IoT domains, in: 2017 IEEE Conference on Network Softwarization (NetSoft), Bologna, 2017, pp. 1–6, http://dx.doi.org/10.1109/NETSOFT.2017.8004245.

[50] H.-C. Hsieh, J.-L. Chen, A. Benslimane, 5G virtualized multi-access edge computing platform for IoT applications, J. Netw. Comput. Appl. (2018) http://dx.doi.org/10.1016/j.jnca.2018.05.001.

[51] Ricard Vilalta, A. Mayoral, Raul Muoz, Ramon Casellas, Ricardo Martínez, Distributed multi-tenant cloud/fog and heterogeneous SDN/NFV orchestration for 5G services, 2016, Available at http://5G-crosshaul.eu/wp-content/uploads/2016/09/NetVirt16_RVilalta_v1.pdf (Accessed on September 5, 2016).

[52] M. Zhao, et al., Verification and validation framework for 5G network services and apps, in: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, 2017, pp. 321–326, http://dx.doi.org/10.1109/NFV-SDN.2017.8169878.

[53] G. Gardikis, H. Koumaras, C. Sakkas, et al., Towards SDN/NFV-enabled satellite networks, Telecommun. Syst. 66 (2017) 615, http://dx.doi.org/10.1007/s11235-017-0309-0.

[54] T. Lin, N. Tarafdar, B. Park, P. Chow, A. Leon-Garcia, Enabling network function virtualization over heterogeneous resources, in: 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, 2017, pp. 58–63, http://dx.doi.org/10.1109/APNOMS.2017.8094179.

[55] Olivier. Flauzac, Carlos. Gonzalez, Florent. Nolot, Developing a distributed software defined networking testbed for IoT, in: The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016), in: Procedia Computer Science, vol. 83, 2016, pp. 680–684.

[56] B.R. Al-Kaseem, H.S. Al-Raweshidyhamed, SD-NFV As an energy efficient approach for M2m networks using cloud-based 6lowpan testbed, IEEE Internet Things J. 4 (5) (2017) 1787–1797, http://dx.doi.org/10.1109/JIOT.2017.2704921.

[57] L. Zhou, et al., IoT Gateway edge VNFs on uCPE, in: 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 2018, pp. 1–2, http://dx.doi.org/10.1109/NFV-SDN.2018.8725618.

[58] K. Nguyen, M. Cheriet, Virtual edge-based smart community network management, IEEE Internet Comput. 20 (6) (2016) 32–41, http://dx.doi.org/10.1109/MIC.2016.127.

[59] A. Lohachab, Karambir, Next generation computing: Enabling multilevel centralized access control using UCON and capbac model for securing IoT networks, in: 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2018, pp. 159–164, http://dx.doi.org/10.1109/IC3IoT.2018.8668191.

[60] R. Muoz, R. Vilalta, R. Casellas, A. Mayoral, R. Martínez, Integrating optical transport network testbeds and cloud platforms to enable end-to-end 5G and IoT services, in: 2017 19th International Conference on Transparent Optical Networks (ICTON), Girona, 2017, pp. 1–4, http://dx.doi.org/10.1109/ICTON.2017.8025035.

[61] R. Muoz, et al., The adrenaline testbed: An SDN/NFV packet/optical transport network and edge/core cloud platform for end-to-end 5G and IoT services, in: 2017 European Conference on Networks and Communications (EuCNC), Oulu, 2017, pp. 1–5, http://dx.doi.org/10.1109/EuCNC.2017.7980775.

[62] Pedro Neves, Rui Calé, Mário Costa, Gonçalo Gaspar, Jose Alcaraz-Calero, Qi Wang, James Nightingale, Giacomo Bernini, Gino Carrozzo, ngel Valdivieso, Luis Villalba, Maria Barros, Anastasius Gravas, José Santos, Ricardo Maia, Ricardo Preto, Future Mode of Operations for 5G – The SELFNET Approach Enabled by SDN/NFV, Comput. Stand. Interfaces, http://dx.doi.org/10.1016/j.csi.2016.12.008.

[63] B. Nguyen, N. Choi, M. Thottan, J. Van der Merwe, SIMECA: SDN-based IoT mobile edge cloud architecture, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, 2017, pp. 503–509, http://dx.doi.org/10.23919/INM.2017.7987319.

[64] M. Oppitz, P. Tomsu, Software defined virtual networks, in: Inventing the Cloud Century, Springer, Cham, 2018, http://dx.doi.org/10.1007/978-3-319-61161-7_8.

[65] M.J. Islam, M. Mahin, S. Roy, B.C. Debnath, 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), Cox'sBazar, Bangladesh, 2019, pp. 1–6, http://dx.doi.org/10.1109/ECACE.2019.8679167.

[66] Carla Mouradian, Narjes Tahghigh Jahromi, Roch H. Glitho, NFV And SDN - based distributed IoT gateway for large-scale disaster management, 2018, https://arxiv.org/abs/1808.06874.

[67] T.G. Nguyen, T.V. Phan, B.T. Nguyen, C. So-In, Z.A. Baig, S. Sanguanpong, Search: A collaborative and intelligent NIDS architecture for SDN-based cloud IoT networks, IEEE Access 7 (2019) 107678-107694, http://dx.doi.org/10.1109/ACCESS.2019.2932438.

[68] 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), Helsinki, 2017, pp. 169–174, http://dx.doi.org/10.1109/CSCN.2017.8088617.

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

[70] Alejandro Molina Zarca Dan Garcia-Carrillo, Jorge Bernal Bernabe, Jordi Ortiz, Rafael Marin-Perez, Antonio Skarmeta, Enabling virtual AAA management in SDN-based IoT networks, Sensors 19 (2019) 295, http://dx.doi.org/10.3390/s19020295.

[71] A. Mohsen Nia, N.K. Jha, A comprehensive study of security of internet-of-things, IEEE Trans. Emerg. Top. Comput. PP (99) (2016) 1.

[72] John Paul Walters, et al., Wireless sensor network security: A survey, Secur. Distrib. Grid Mob. Pervas. Comput. 1 (2007) 367.

[73] Bryan Parno, et al., Distributed detection of node replication attacks in sensor networks, in: Security and Privacy, 2005 IEEE Symposium on, IEEE, 2005, pp. 49–63.

[74] Xun Wang, et al., Search-based physical attacks in sensor networks, in: Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on, IEEE, 2005, pp. 489–496.

[75] Alexander Becher, et al., Tampering with motes: Real-world physical attacks on wireless sensor networks, in: International Conference on Security in Pervasive Computing, Springer, 2006, pp. 104–118.

[76] MHR. Khouzani, Saswati Sarkar, Maximum damage battery depletion attack in mobile sensor networks, IEEE Trans. Automat. Control 56 (10) (2011) 2358–2368.

[77] David R. Raymond, et al., Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Trans. Veh. Technol. 58 (1) (2009) 367–380.

[78] Xinyu Yang, et al., Towards a low-cost remote memory attestation for the smart grid, Sensors 15 (8) (2015) 20799–20824.

[79] Guevara Noubir, Guolong Lin, Low-power dos attacks in data wireless LANs and countermeasures, ACM SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.

[80] David R. Raymond, Scott F. Midki_, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervas. Comput. 7 (1) (2008).

[81] E. Bertino, N. Islam, Botnets and internet of things security, Computer 50 (2) (2017) 76–79.

[82] Ayman. Mukaddam, et al., IP Spoofing detection using modified hop count, in: Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on, IEEE, 2014, pp. 512–516.

[83] Yong-Zhen. Li, et al., Security and privacy on authentication protocol for low-cost RFID, in: Computational Intelligence and Security, 2006 International Conference on, Vol. 2, IEEE, 2006, pp. 1101–1104.

[84] B. Revathi, D. Geetha, A survey of cooperative black and gray hole attack in MANET, Int. J. Comput. Sci. Manag. Res. 1 (2) (2012) 205–208.

[85] Chris Karlof, David Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, Ad hoc Netw. 1 (2) (2003) 293–315.

[86] James. Newsome, et al., The sybil attack in sensor networks: analysis & defenses, in: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, ACM, 2004, pp. 259–268.

[87] I. Andrea, et al., Internet of things: Security vulnerabilities and challenges, in: 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180–187.

[88] Mohamed Abomhara, GM. Kien, Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks, J. Cyber Secur. 4 (2015) 65–88.

[89] B. Grobauer, et al., Understanding cloud computing vulnerabilities, IEEE Secur. Priv. 9 (2) (2011) 50–57.

[90] Ye Yan, et al., A survey on cyber security for smart grid communications., IEEE Commun. Surv. Tutor. 14 (4) (2012) 998–1010.

[91] Jing Liu, et al., Cyber security and privacy issues in smart grids, IEEE Commun. Surv. Tutor. 14 (4) (2012) 981–997.

[92] Mohamed Nidhal Mejri, et al., Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. 1 (2) (2014) 53–66.

[93] Ahmad-Reza. Sadeghi, et al., Security and privacy challenges in industrial internet of things, in: Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, IEEE, 2015, pp. 1–6.

[94] A. Sajid, et al., Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges, IEEE Access 4 (2016) 1375–1384.

[95] T. Mamouni, et al., Universal AAA for hybrid accesses, in: 2015 European Conference on Networks and Communications (EuCNC), 2015, pp. 403–407.

[96] Jose L. Hernandez-Ramos, et al., Toward a lightweight authentication and authorization framework for smart objects, IEEE J. Sel. Areas Commun. 33 (4) (2015) 690–702.

[97] Helge Janicke Jianmin Jiang Mohamed Amine Ferrag, Leandros A. Maglaras, Lei Shu, Authentication protocols for internet of things: A comprehensive survey, Secur. Commun. Netw. 2017 (1) (2017) 41.

[98] R.K. Sharma, et al., Different firewall techniques: A survey, in: Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2014, pp. 1–6.

[99] N. Gupta, et al., A firewall for internet of things, in: 2017 9th International Conference on Communication Systems and Networks (COMSNETS), 2017, pp. 411–412.

[100] H. Hasan, et al., Secure lightweight ECC-based protocol for multiagent IoT systems, in: 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2017, pp. 1–8.

[101] S.L. Keoh, et al., Securing the internet of things: A standardization perspective, IEEE Internet Things J. 1 (3) (2014) 265–275.

[102] David.J. Malan, et al., A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography, in: Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, IEEE, 2004, pp. 71–80.

[103] D. Daz-Snchez, et al., Proxy re-encryption schemes for IoT and crowd sensing, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016, pp. 15–16.

[104] Gulshan. Kumar, et al., The use of artificial intelligence based techniques for intrusion detection: a review, Artif. Intell. Rev. 34 (4) (2010) 369–387.

[105] A.A. Gendreau, M. Moorman, Survey of intrusion detection systems towards an end to end secure internet of things, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 84–90.

[106] Rob. Sherwood, et al., Rob Sherwood Others Flowvisor: A Network Virtualization Layer, OpenFlow Switch Consortium, Tech Rep., 2009, pp. 1–13.

[107] Mathieu. Boussard, et al., Software-defined LANs for interconnected smart environment, in: Teletra_c Congress (ITC 27), 2015 27th International, IEEE, 2015, pp. 219–227.

[108] Rodrigo. Braga, et al., Lightweight ddos flooding attack detection using NOX/openflow, in: Local Computer Networks (LCN), 2010 IEEE 35th Conference on, IEEE, 2010, pp. 408–415.

[109] Sajad Shirali-Shahreza, Yashar Ganjali, Effficient implementation of security applications in openflow controller with flexam, in: High-Performance Interconnects (HOTI), 2013 IEEE 21st Annual Symposium on, IEEE, 2013, pp. 49–54.

[110] Seungwon Shin, Guofei Gu, Cloudwatcher: Network security monitoring using openflow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?), in: Network Protocols (ICNP), 2012 20th IEEE International Conference on, IEEE, 2012, pp. 1–6.

[111] Seungwon. Shin, et al., A first step toward network security virtualization: from concept to prototype, IEEE Trans. Inf. Forensics Secur. 10 (10) (2015) 2236–2249.

[112] Syed.Akbar. Mehdi, et al., Revisiting traffic anomaly detection using software defined networking, in: International Workshop on Recent Advances in Intrusion Detection, Springer, 2011, pp. 161–180.

[113] Changhoon Yoon, et al., Enabling security functions with SDN: A feasibility study, Comput. Netw. 85 (2015) 19–35.

[114] Seyed.Kaveh. Fayaz, et al., Bohatei: Flexible and elastic ddos defense, in: USENIX Security Symposium, 2015, pp. 817–832.

[115] Narmeen Zakaria Bawany, et al., Ddos attack detection and mitigation using SDN: Methods, practices, and solutions, Arab. J. Sci. Eng. 42 (2) (2017) 425–441.

[116] Federico Griscioli, et al., Leveraging SDN to Monitor Critical Nfrastructure Networks in a Smarter Way, Tech. Report, Cornell University, 2017, arXiv: 1701.04293.

[117] Jafar.Haadi. Jafarian, et al., Openflow random host mutation: transparent moving target defense using software defined networking, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, ACM, 2012, pp. 127–132.

[118] Marc. Mendonca, et al., A flexible in-network IP anonymization service, in: Communications (ICC), 2012 IEEE International Conference on, IEEE, 2012, pp. 6651–6656.

[119] Qi. Duan, et al., Efficient random route mutation considering flow and network constraints, in: 2013 IEEE Conference on Communications and Network Security (CNS), 2013, pp. 260–268.

[120] Shaibal. Chakrabarty, et al., Black SDN for the internet of things, in: Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on, IEEE, 2015, pp. 190–198.

[121] Seungwon Shin, et al., FRESCO: Modular composable security services for software-defined networks, in: NDSS, 2013.

[122] Philip. Porras, et al., A security enforcement kernel for openflow networks, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, ACM, 2012, pp. 121–126.
[123] Seungwon Shin, et al., Avant-guard: Scalable and vigilant switch flow management in software-defined networks, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ACM, 2013, pp. 413–424.
[124] John. Sonchack, et al., Enabling practical software-defined networking security applications with OFX, in: NDSS, Vol. 16, 2016, pp. 1–15.
[125] Aaron. Gember, et al., ECOS: leveraging software-defined networks to support mobile application offloading, in: Proceedings of the Eighth ACM/IEEE Symposium on Architectures for Networking and Communications Systems, ACM, 2012, pp. 199–210.
[126] K. Kalkan, S. Zeadally, Securing internet of things (IoT) with software defined networking (SDN), IEEE Commun. Mag. (2017) 1–7.
[127] Justine Sherry, et al., Making middleboxes someone else's problem: network processing as a cloud service, ACM SIGCOMM Comput. Commun. Rev. 42 (4) (2012) 13–24.
[128] Anat. Bremler-Barr, et al., Deep packet inspection as a service, in: Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies, ACM, 2014, pp. 271–282.
[129] Diego. Montero, et al., Virtualized security at the network edge: a user-centric approach, IEEE Commun. Mag. 53 (4) (2015) 176–186.
[130] Lianjie. Cao, et al., Nfv-vital: A framework for characterizing the performance of virtual network functions, in: Network Function Virtualization and Software Defined Network (NFV-SDN), 2015 IEEE Conference on, IEEE, 2015, pp. 93–99.
[131] Carlos Colman-Meixner, et al., A survey on resiliency techniques in cloud computing infrastructures and applications, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2244–2281.
[132] Tarik Taleb, et al., Mobile edge computing potential in making cities smarter, IEEE Commun. Mag. 55 (3) (2017) 38–43.
[133] A. Aissioui, et al., On enabling 5G automotive systems using follow me edge-cloud concept, IEEE Trans. Veh. Technol. 67 (6) (2018) 5302–5316.
[134] T. Taleb, et al., Follow-me cloud: When cloud services follow mobile users, IEEE Trans. Cloud Comput. (2017) 1.
[135] Faizul Bari, et al., Orchestrating virtualized network functions, IEEE Trans. Netw. Serv. Manag. 13 (4) (2016) 725–739.
[136] Zafar Ayyub Qazi, et al., SIMPLE-Fying middlebox policy enforcement using SDN, ACM SIGCOMM Comput. Commun. Rev. 43 (4) (2013) 27–38.
[137] Aaron. Gember-Jacobson, et al., Opennf: Enabling innovation in network function control, in: ACM SIGCOMM Computer Communication Review, Vol. 44, ACM, 2014, pp. 163–174.
[138] J. Pan, Z. Yang, Cybersecurity Challenges and Opportunities in the New Edge Computing + IoTWorld, SDN-NFV Sec'18, Tempe, AZ, USA, 2018, http://dx.doi.org/10.1145/3180465.3180470.
[139] P.P. Ray, An introduction to dew computing: Definition, concept and implications, IEEE Access 6 (2018) 723–737, http://dx.doi.org/10.1109/ACCESS.2017.2775042.
[140] M. Samaniego, C. Espana, R. Deters, Smart virtualization for IoT, in: 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, 2018, pp. 125–128, http://dx.doi.org/10.1109/SmartCloud.2018.00028.
[141] M. Gusev, A dew computing solution for IoT streaming devices, in: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017, pp. 387–392, http://dx.doi.org/10.23919/MIPRO.2017.7973454.
[142] S. Luo, Z. Zhou, X. Chen, W. Wu, Dewing in fog: Incentive-aware micro computing cluster formation for fog computing, in: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, Singapore, 2018, pp. 722–729, http://dx.doi.org/10.1109/PADSW.2018.8644977.
[143] G. Cristescu, R. Dobrescu, O. Chenaru, G. Florea, DEW: A new edge computing component for distributed dynamic networks, in: 2019 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 2019, pp. 547–551, http://dx.doi.org/10.1109/CSCS.2019.00100.
[144] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. Maasberg, KKR. Choo, Multimedia big data computing and Internet of Things applications: A taxonomy and process model, J. Netw. Comput. Appl., 124, 169-195.
[145] N. Kumar, S. Misra, JJPC. Rodrigues, MS. Obaidat, Coalition games for spatio-temporal big data in Internet of Vehicles environment: A comparative analysis, IEEE Internet Things J., 2 (4), 310-320.
[146] N. Kumar, R. Iqbal, S. Misra, JJPC. Rodrigues, Bayesian coalition game for contention-aware reliable data forwarding in vehicular mobile cloud, Future Gener. Comput. Syst., 48, 60-72.
[147] N. Kumar, N. Chilamkurti, SC. Misra, Bayesian coalition game for the internet of things: an ambient intelligence-based evaluation, IEEE Commun. Mag., 53 (1), 48-55.
[148] N. Kumar, M. Kumar, RB. Patel, Capacity and interference aware link scheduling with channel assignment in wireless mesh networks, J. Netw. Comput. Appl., 34 (1), 30-38.
[149] J. Srinivas, AK. Das, N. Kumar, J. and Rodrigues, Cloud centric authentication for wearable healthcare monitoring system, IEEE Trans. Depend. Secure Comput..
[150] N. Kumar, AV. Vasilakos, JJPC. Rodrigues, A multi-tenant cloud-based DC nano grid for self-sustained smart buildings in smart cities, IEEE Commun. Mag., 55 (3), 14-21.

Partha Pratim Ray received the B.Tech. degree in computer science and engineering and the M.Tech. degree in electronics and communication engineering, with specialization in embedded systems, from the West Bengal University of Technology, Kolkata, India, in 2008 and 2011, respectively. He is currently a full-time Assistant Professor with the Department of Computer Applications, Sikkim University, Gangtok, India. He has authored more than 36 articles in SCI journals and 16 IEEE Conferences of repute. He has filed 7 national patents. He has co-authored 1 book and 1 mono-graph. His research interests include Internet of Things, Dew computing, Blockchain and Pervasive biomedical informatics. He has published papers in IEEE Access, IEEE Systems, IEEE Transactions on Consumer Electronics, IEEE/ACM Transactions on Computational Biology and Bioinformatics, Computer Networks, Journal of Network and Computer Applications and IEEE GLOBECOM 2019. He is guest editor in the special issues of the IoT journal, Elsevier, Sensors (MDPI). He has been awarded with Young Engineers Award by the Institution of Engineerings India (IEI) for 2019–20. His google scholar citation is 1660, h-index 18 and i10-index is 26. He is a senior member of IEEE.

Neeraj Kumar received his Ph.D. in CSE from SMVD University, Katra (J & K), India, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala (Pb.), India since 2014. Dr. Neeraj is an internationally renowned researcher in the areas of VANET & CPS Smart Grid & IoT Mobile Cloud computing & Big Data and Cryptography. He has published more than 400 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, and Taylor and Francis. His paper has been published in some of the high impact factors journals such as-IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Power Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Smart Grid, IEEE Journal of Biomedical and Health Informatics, IEEE Access, IEEE Transactions on Consumer Electronics, IEEE Systems Journal, IEEE IoT Journal, IEEE Wireless Communication Magazine, IEEE Vehicular Technology Magazine, IEEE Communication Magazine, IEEE Networks Magazine etc. Apart from the journals conferences, he has also published papers in some of the core conferences of his area of specialization such as-IEEE Globecom, IEEE ICC, IEEE Greencom, IEEE CSCWD. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. His research is supported by funding from TCS, CSIT, UGC and UGC in the area of Smart grid, energy management, VANETs, and Cloud computing. He is member of the Cyber–Physical Systems and Security (CPSS) research group. He has research funding from DST, CSIR, UGC, and TCS. He is a senior member of IEEE.