Computer Networks 143 (2018) 221–246

Contents lists available at ScienceDirect

Computer Networks

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

Review article

IoT survey: An SDN and fog computing perspective

Ola Salman*, Imad Elhajj, Ali Chehab, Ayman Kayssi

Department Electrical and Computer Engineering, American University of Beirut, Beirut 1107 2020, Lebanon

ARTICLE INFO

Article history:
Received 18 January 2018
Revised 21 June 2018
Accepted 12 July 2018
Available online 17 July 2018

Keywords:
IoT
Survey
SDN
Fog
Cloud
5G

ABSTRACT

Recently, there has been an increasing interest in the Internet of Things (IoT). While some analysts disvalue the IoT hype, several technology leaders, governments, and researchers are putting serious efforts to develop solutions enabling wide IoT deployment. Thus, the huge amount of generated data, the high network scale, the security and privacy concerns, the new requirements in terms of QoS, and the heterogeneity in this ubiquitous network of networks make its implementation a very challenging task. SDN, a new networking paradigm, has revealed its usefulness in reducing the management complexities in today's networks. Additionally, SDN, having a global view of the network, has presented effective security solutions. On the other hand, fog computing, a new data service platform, consists of pushing the data to the network edge reducing the cost (in terms of bandwidth consumption and high latency) of "big data" transportation through the core network. In this paper, we critically review the SDN and fog computing-based solutions to overcome the IoT main challenges, highlighting their advantages, and exposing their weaknesses. Thus, we make recommendations at the end of this paper for the upcoming research work.

1. Introduction

One of the all-time most impactful innovations is the Internet. Internet has permitted the interconnection of all traditional computing devices and it was natural for this desire for access and control to extend to non-traditional devices. Here came the evolution into Internet of Things (IoT). Mentioned seventeen years ago by Kevin Ashton [1], IoT draws the lines of the second digital revolution [2,3]. Cisco expected that, by 2020, 50 billion objects would be connected to the Internet [4]. This large scale is one of the unavoidable challenges for the IoT domain. The ***high scalability*** is accompanied with an increased complexity in the management of this large number of things/gateways, and network devices. Managing all these devices in the traditional way (manually and each device separately) is no longer viable.

As the Metcalfe's law states, the importance of a communication network increases exponentially with the number of connected devices [5]. Therefore, with billions of connected things in the future network, the IoT value is extremely high [6]. In addition, IoT is depicted as one of the most disruptive technologies [7,8]. Many firms and technology leaders (Intel, Microsoft, Cisco, InterDigital, etc.) have taken note of the IoT economical value [9], and put serious efforts to enable IoT real deployment (Table 1 lists some of the important ongoing projects). However, this drive to develop IoT solutions has resulted in proposing disjoint ones. Lacking interoperability between the different IoT platforms limits their potential. We all know that the root enabler of the Internet success and wide adoption is its openness and its standardized architecture. Having different IoT architectures and platform resulted in having heterogeneous silos of networks. In addition to this kind of heterogeneity, different formats of data are used, and different types of communication technologies are invoked. This makes the IoT a vertically fragmented network. Therefore, the ***heterogeneity*** is another important challenge facing IoT.

Moreover, the large number of connected devices will naturally result in enormous amount of data, which challenges the ability of today's networks to handle. The current centralized paradigm of data processing and storage is not feasible. New ways to analyze, filter and aggregate this data at the network edges will be essential in any upcoming IoT solution. The IoT ***"Big Data"*** is not only about the size of the generated data, but it is more about the variety of this data in terms of type, semantic, frequency, place and time.

Finally, ***security and privacy*** guarantees present one of the most important challenges that effectively hinders any real IoT wide deployment. In addition to the current security vulnerabilities, IoT poses new ones.

In the light of the cited challenges, there is a need for new approach to networking. Software Defined Networking (SDN), a new networking paradigm, aims to separate the control and data planes. This separation provides the network controller with a global view of the network, facilitating traffic engineering and network management at runtime [10]. On the other hand, fog comput-

* Corresponding author.
E-mail addresses: oms15@mail.aub.edu (O. Salman), ie05@aub.edu.lb (I. Elhajj), chehab@aub.edu.lb (A. Chehab), ayman@aub.edu.lb (A. Kayssi).

https://doi.org/10.1016/j.comnet.2018.07.020
1389-1286/

Table 1
IoT commercial projects.

Company	Project
Intel [11]	Intel IoT Platform
Microsoft [12]	Azure IoT Suite
Libelium [13]	Smart World Sensor Applications
Frankhaufer FOKUS [14]	OpenMTC
Cisco [15]	Cisco IoT System
Hewlett Packard Enterprise [16]	vCore
Dell [17]	Edge Gateway
AT&T [18]	AT&T IoT
InterDigital [19]	M2M/IoT
IBM [20]	Watson IoT

ing (a cloud computing complement) aims at bringing the cloud to the network edge making it more scalable and more responsive. In this survey, we will investigate how these technologies have been applied in the IoT field and how their application will enable the IoT wide deployment.

In the literature, several surveys have tackled different IoT related subjects (see Table 2): IoT applications, challenges, and opportunities [21–31], IoT frameworks [32–37], IoT security [38–43], IoT standardization [44–48], SDN application in IoT [49–54], IoT and cloud integration [55,56].

However, the existing surveys do not comprehensively review the main IoT challenges. The Internet already presents QoS and security related challenges, but in the IoT case, some of the existing challenges become more crucial. Thus, the existing work includes specific and non-specific-IoT challenges. In addition, the IoT challenges are listed without including the related proposed solutions. However, in this work, we presented the four main IoT-specific challenges and we reviewed the proposed solutions coping with these challenges. In this context, new technologies emerge in the network, communication, and IT domains. These technologies can enable innovative IoT applications and help in coping with many of the IoT challenges. However, the existing work does not cover the most recent technologies and the role of these technologies in alleviating the IoT challenges. Thus, this work presents the most recent enabling technologies, and how these technologies can be employed to cope with the presented IoT challenges. Specifically, this paper reviews the application of SDN, NFV, cloud computing, and fog computing to handle the main IoT challenges.

This paper is organized as follows: In Section 2, we discuss the most relevant IoT definitions and we list the main related IoT concepts. In Section 3, we investigate the IoT enabling technologies. In Section 4, we review the most important IoT, SDN, NFV, and edge computing standardization efforts. In the subsequent sections, we present the IoT main challenges (as shown in Table 3): IoT security, IoT Big Data, IoT heterogeneity, and IoT scalability, and the corresponding SDN/NFV and cloud/edge-based solutions. Thus, in Section 5, we review the IoT security related work and we show how SDN can alleviate the IoT security concerns. Section 6 reviews the IoT "Big Data" and the application of cloud and fog computing to manage it. The IoT gateway is an essential part to cope with the heterogeneity challenge, so in Section 7, we review the propositions of IoT gateways. IoT scalability imposes new architectural considerations, so Section 8 reviews the most known IoT architectures and the SDN integration into a general IoT architecture. In Section 9, we present the main limitations of the current IoT solutions and we make some recommendations for the future research directions. Finally, we conclude in Section 10.

2. IoT definition

Beyond the IoT hype, a real definition is essential to highlight the characteristics of this new concept [57]. Several definitions have been proposed resulting in a storm of terms and definitions. Important work is being done by the IEEE Internet initiative in order to find a conceptual IoT definition [58]. ITU defines IoT as being an infrastructure that will connect physical and virtual devices [59]. IETF defines IoT as being the Internet that considers TCP/IP and Non-TCP/IP suites at the same time and the things as being "objects" identified by unique addresses [60]. IEEE, in its special report on Internet of Things, defines it as a network that connects devices having sensing capabilities [58]. In [58], the IEEE Internet initiative gives its own definition as follows: The Internet of Things is a network that connects uniquely identifiable virtual and physical devices, using existing or new communications protocols. These Things are dynamically configurable and have interfaces that must be accessible distantly through the Internet [58].

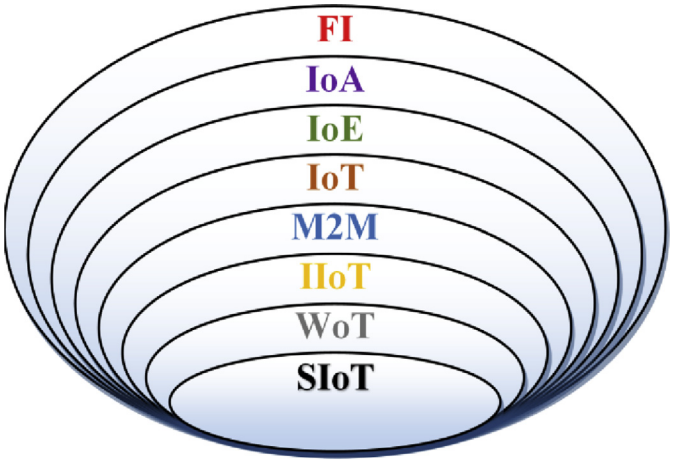


Fig. 1. The different IoT related concepts.

Actually, IoT is not the exclusive name for this new concept. In the IoT storm, there are different and confusing terms such as: Machine-to-Machine (M2M), Industrial Internet of Things (IIoT), Internet of Anything (IoA), Internet of Everything (IoE), Web of Things (WoT), and Social Internet of Things (SIoT). An inclusion relation can be established between these different concepts as shown in Fig. 1. In the following, we will try to present the definitions of these concepts ***IoE***, coined by Cisco [61], consists of connecting things, devices, humans, and data to a global network [62]. ***IoA***, presented in [63], consists of connecting not only the existing well-known things as implied in the IoE definition, but also it refers to connect all possibly *"imagined"* things. ***M2M*** is a subset of IoT [64], which includes the M2M communications as well as Machine-to-Human interaction. ETSI defines M2M in [65] as: an automated communication between two devices without a human intervention [65]. While IoT focuses on the physical objects' representation, M2M is connectivity centric. Thus, moving from M2M to IoT necessitates further considerations [66].

While IoT applications tackle different human life domains, the industrial field remains one of the most critical ones. Applying IoT in the industrial domain requires careful attention and special efforts [67,68]. Talking about industries means that we include businesses ranging from small ones to large ones. Security and privacy are the most challenging issues in this context [69]. Recently, a consortium for the industrial IoT, ***IIoT***, has been established [70]. This consortium, founded by AT&T, Cisco, GE, IBM, and Intel in March 2014, aims at pushing the standardization in this area [71].

In the Auto-ID Labs white paper presented in [72], a comparison between IoT and Web of things, WoT, is performed. It is stated that IoT is a wider concept than WoT, having structural concerns (e.g. unique identity for the things), which cannot be resolved by the web technology. Essentially, ***WoT*** is a web framework to which

Table 2
IoT surveys summary.

Subject	Reference	Contributions	Limitations
IoT applications, challenges, and opportunities	[21–31]	The main IoT benefits, applications (smart home, healthcare, connected cars), and challenges are presented.	The challenges are just mentioned without presenting the enabling technologies and solutions.
IoT frameworks	[32–37]	The different proposed IoT frameworks are presented.	The SDN and fog-based frameworks are not included.
IoT Security	[38–43]	The IoT security challenges and the proposed protocols are presented.	The SDN benefits in terms of security are not considered.
IoT Standardization	[44–48]	The standardization efforts in the IoT domain are reviewed.	The standardization efforts for the new emerging technologies like SDN and fog computing are not presented.
SDN application in IoT	[49–54]	The SDN application at different IoT levels are presented.	The role of SDN in alleviating the IoT challenges is not included.
Cloud/Edge computing for IoT	[55,56]	The cloud related application to enable different IoT applications are presented.	The focus is on the big data related challenge. However, the networking aspect of the different data nodes is not considered (the application of SDN for data networking).

Table 3
IoT challenges, benefits, and limitations.

IoT challenges	Benefits	Limitations
Scalability	• Connecting new kinds of devices • Gain more control over the connected devices	• Management complexity • Network capacity • QoS
Big Data	• Enabling innovative applications • Getting useful insights from Big Data analysis	• Big Data management • Data centralization: high latency, redundancy, etc. • Data at the network edge: security, management, networking, etc.
Heterogeneity	• Integrating different IoT vertical silos • Integrating different communication technologies, devices' types, data types, etc.	• Interoperability
Security and Privacy	• Enabling innovative applications using sensitive data	• New types of attacks • Private data inspection

the things are connected through the Internet and have their collected data pushed to it. Web data analysis, and user interfaces are keys to provide services that enable innovative applications. The web can be used to access data but the communication between devices, automation, auto-configuration, and management capabilities are outside the scope of the existing web.

SIoT, which allows the things to have their social networks [73,74], is a related concept to WoT. Inheriting the success of social networks (e.g. Facebook), that can be considered as "*banks of data*", the socialization concept can be employed in the IoT context. The projection of the IoT world in the social one results in the projection of the things into the social world, which requires new things' definitions (social objects) [75].

The Future Internet (***FI***) is a global network that will encompass all the above-mentioned networks. Six principles (C6) will enable this innovation. The C6 annotation refers to: Connectivity, Content, Cloud, Context, Collaboration, and Cognition [76]. In such a network, mobile and constrained things will be connected to the Internet generating huge amount of data. This data, handled by advanced cloud based technologies, will shift context-aware behavior into a collaborative environment between the different things. The analysis of this data will result in a cognitive world. Effectively, IoT is an essential part of the Future Internet [77].

Accordingly, it is important to show the distinction between these concepts in the aim to solve their specific problems and to allow their realization in the near future [78].

3. Enabling technologies

In this section, we present the recent technologies designated to play an essential role in the IoT realization.

3.1. SDN & NFV

SDN, an emerging technology in the network domain, aims at separating control and data planes. The control plane consists of the SDN controller (Network Operating System (NOS)) which has the role of network orchestration; most of the computations are done there, which gives it a special importance being the network brain. The data plane consists of the network devices (routers/switches) being responsible for simple matching operations to know how to forward the packets. These simple devices forward to the controller every packet they do not know how to act upon.

SDN is not the first attempt towards separating data forwarding and network strategical computation, and it is not the first trial to softwarize the network functions. The history of programmable networks dates back to the early 90s. Several attempts to apply programmability and automation in the network domain have been conceived (e.g. ATM) [79]. However, SDN is the most promising one. OpenFlow, the first standardized southbound interface, has presented a primary insight onto the network programmability ef-

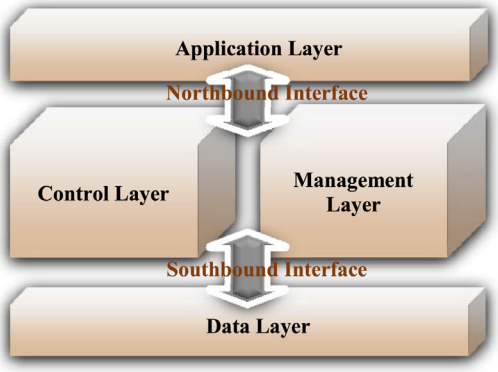


Fig. 2. SDN architecture.

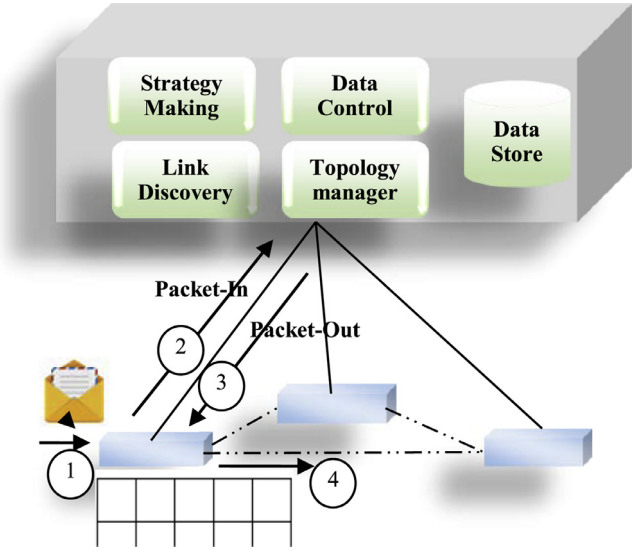


Fig. 3. OpenFlow based flow.

fectiveness. However, limiting SDN to OpenFlow is an inappropriate limitation of the SDN horizons.

The SDN architecture, as presented in the recent IRTF RFC 7426 drafted by the SDN Research Group (SDNRG) [80], consists of four layers: data layer, control layer, management layer, and application layer as shown in Fig. 2. This architecture provides network flexibility, dynamicity, and management capabilities. In this context, the question about how SDN can enable IoT arises.

Therefore, one can argue that it is a bad idea to propose a centralized architecture for this highly scalable network, or that applying the SDN paradigm to it has a retro effect that returns us back to the era where the centralization paradigm was pioneering the telecom domain. However, these assertions are not very accurate. SDN centralized control cannot be compared to a central telecom switch. The SDN centralization is a logical concept more than being a physical one. In this context, the distributed control scheme came to defend this argument [81,82]. Several controllers have enabled control distributiveness into their architecture: Disco [83], Onix [84], ONOS [85], and OpenDaylight [86], etc. In this case, the East/Westbound [87] interfaces are responsible for connecting the distributed controllers' instances. Besides, the southbound interfaces provide the control over the network. OpenFlow is the most known southbound interface. The OpenFlow operational flow is summarized in Fig. 3.

Upon receiving a packet, the switch performs filter matching on the header fields. If there is a corresponding entry in this table, it takes action based on the entry's action part. Otherwise, it forwards the packet to the controller. When it receives the packet from the switch (PacketIn), the controller takes the forwarding decision and downloads the corresponding rule to the switch (PacketOut). The controller basic modules are: topology manager, link manager, decision making, data control, and data storage [88]. The controller learns about the network links (between switches and switches and hosts) using the Link Layer Discovery Protocol (LLDP). The link discovery module provides this information to the topology manager module that is responsible of constructing/updating the network topology database.

On top of the control layer, the application layer resides. The communication between the control and application layers is performed through the northbound interfaces. These interfaces, which give the application access to the network collected data, offer most of the SDN benefits.

The IoT realization is mostly hindered by the Internet management complexity issue preventing the dynamic deployment of new services. The control is fully distributed; so, reconfiguring the network and adding new features will be exhaustive if done in the traditional way. Using SDN, this task becomes much simpler; the control centralization provides the controller with a global view of the network, giving it the power to hide the management complexities and to have more control over the network. QoS guarantee, heterogeneity, security and privacy concerns, communication resilience, and big data management are tasks that can be alleviated by the SDN introduction [89,90].

On the other hand, after revealing its innovative value in the IT domain, the virtualization finds its way into the network domain with the SDN proliferation. NFV and SDN are complementary technologies. SDN with NFV (or SDNv2 [91]) allow the virtualization of the network functions in a way similar to what we have seen in the computing domain; the same network infrastructure can be used by different applications. The network is divided into slices in this case, and each slice has to support certain flow. This allows a fine-grained services categorization and offers a security enhancement solution.

Additionally, NFV plays an important role in the IoT domain [92]. Coupled with SDN, this technology has the capability to handle the IoT requirements in terms of QoS guarantee, traffic engineering, defeating heterogeneity, and providing security services. Additionally, NFV helps to cope with the IoT high scalability challenge [93]. Due to the limited network capacity, the increase in the number of connected devices poses network constraints that cannot be met, especially at peak time load. However, upgrading the existing network infrastructure to support higher capacity is expensive in terms of both OpEx and CapEx. In this context, virtualization provides elasticity that helps in an optimized use of the limited hardware resources at low network load permitting the sharing of the network infrastructure between different service providers and different network services/functions. Additionally, NFV allows to borrow network resources as needed at runtime preventing the waste of resources if designed to handle the peak load [94].

3.2. Cloud computing (X-as a Service)

Cloud computing has permitted advancement in the network and telecommunication domains. Relying on the "pay-as-you-go" paradigm, it enables the reduction of both OpEx and CapEx. In the IT domain, several big companies have built their own cloud systems (e.g. Microsoft [95], Google [96], Apple [97], etc.), and some have exploited it from an economical perspective. Cloud was a revolution in the IT domain and it draws a new line in the telecommunication domain. The idea behind the cloud is to borrow computing facilities from the cloud and to pay as you use the pro-

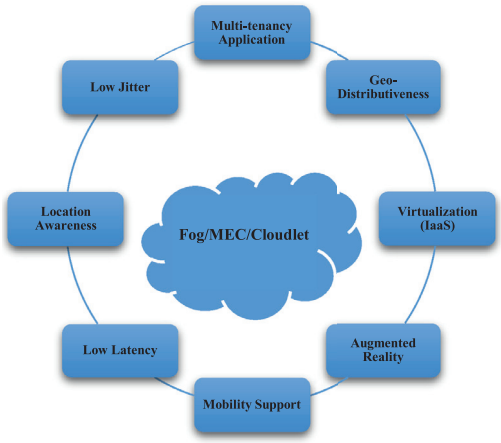


Fig. 4. Common Fog/MEC/Cloudlet features.

vided services. Three main services were provided by the cloud: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).

In the IoT case, the limitations in terms of processing and computing capabilities are more pronounced. Employing cloud computing, in the IoT domain, is beneficial having limited storage and computational power devices. These two revolutionary technologies (cloud and IoT) are fundamental and complementary for the future network era [98]. Different IoT functions have been proposed to be part of the cloud services such as: sensing and actuating as a service [99], sensing cloud [100], sensing as a service [101], building the environment for the Internet of Things as a service (BETaaS) [102], etc.

Another complementary aspect of cloud and IoT is the fact that IoT calls for computation, storage, and communication resources remedy due to the constrained nature of things. On the other hand, the cloud providers need new market domains [103]. Combining IoT and cloud computing brings benefits as well as challenges. Two angles of convergence are presented in [104]: cloud-based and IoT-based. While most of the work discusses cloud-based IoT services, the idea of IoT-centric approach was new. The IoT-centric cloud aims to push cloud functionalities to IoT network edge. This is similar to what is called "fog computing". However, the cloud centric model presents some challenges regarding the cost of transporting the data through the core network, the high latency, and the single point of failure (reliability). Thus, a new way to manage the data is needed while keeping the cloud as a backend.

3.3. Fog computing/MEC/Cloudlet

Rapid mobility patterns, high throughput, reliable sensing, reliable control and actuation, very low latency, big data management, different levels of real-time analytics, and data aggregation are main IoT requirements that cannot be met concurrently by the cloud technology [105]. Low latency, low jitter, mobility support, location awareness, augmented reality, geo-distributiveness, and multi-tenancy applications support (IaaS) are common characteristics provided by edge computing in its different flavors (fog, MEC, and cloudlet) as shown in Fig. 4.

In this context, edge cloud computing was proposed to push the data collection, processing, and analysis to the network edge [106,107]. These edges will not be very powerful nodes; they would just complement the cloud. Essentially, edge computing is about to know which data has to be analyzed at which point (i.e. which data has to stay at the edge and which data has to be pushed to the cloud) [107–109]. Thus, the collaboration between cloud and edge is mandatory [110].

In the shadow of edge computing, comparable new trends aroused (Fig. 5) [111,112]. Fog, cloudlet, and Multi-access Edge Computing (MEC) are three significantly related concepts. In the following, we will try to investigate the subtle differences between these technologies. In this context, the work done in [113] was a good reference for such a comparison.

3.3.1. Fog

Inspired by the natural phenomenon of having fog and clouds where fog are closer to the ground [113], fog computing is meant to be the cloud at the network edge in the IoT networks [114–116].

Fog computing, coined by Cisco in 2012, is an extension of the cloud to the network edge [117]. The fog related characteristics such as low latency, geo-distribution, location awareness, support for mobility, support for ubiquitous access, and support for heterogeneity, present basic requirements for a wide range of IoT services and applications [118]. Additionally, the IoT high scalability imposes federated network management and thus call for new network and data technologies to enable IoT data processing at the network edge [119–121].

In [122], the authors shed light on the relation between fog and cloud. Fog and cloud are complementary technologies and none of them replaces the other. The differentiation between fog and cloud is meant to be in the type of required data and the speed with which data must be processed. Local information can be served by fog nodes and global information can be served by the cloud. The short distance to end users makes the fog distributed platform more suitable for IoT applications while the cloud is relatively farther away [123].

"Why Fog and Why Now?" delay, cognition, agility, and efficiency are defined to be the main reasons for the fog invocation [122]. Additionally, reliability, fault tolerance, and privacy are presented to be fog related benefits [124]. Essentially, cognitive assistance gives rise to distinctive services to be provided by IoT. Cognitive assistance will be the "*killer app*" for mobile computing in the next decade. However, human perception is sensitive to latency. To gain user satisfaction, such applications have to benefit from fog computing emergence to deliver low latency and high-performance processing [125]. Additionally, other innovative applications (e.g. healthcare, smart cars, etc.) will benefit from the fog computing emergence [126,127].

However, the fog nodes distributed pattern imposes new networking issues [128,129]. While the data is centralized at one point in the cloud case, the data nodes are distributed in the fog case. Inducing ways to optimize data correlation between these nodes is critical. Other issues are also encountered in the fog domain such as security and privacy, provisioning and resource management, offloading, charging and accounting, and QoS guarantees in terms of capacity, storage, bandwidth, connectivity, and reliability [130–133].

3.3.2. MEC

An ETSI white paper introduced its Industry Specification Group (ISG) intended to create MEC specifications [134]. This initiative aims at merging the IT and telecom domains to provide cloud-based services at the mobile network edge. In [134], sketches for possible MEC scenarios are presented after listing their benefits and use cases. ETSI is involved in many initiatives such as: NFV, 3GPP, OneM2M, etc. So, it has the incentive to relate new technologies to old ones taking advantage of mature old techniques and providing backward compatibility. In this context, MEC uses cases have been applied to the 3GPP mobile architecture. More recently, MEC solutions have been proposed in the 5G domain [135–137]. Consequently, MEC is one the IoT enablers [138].

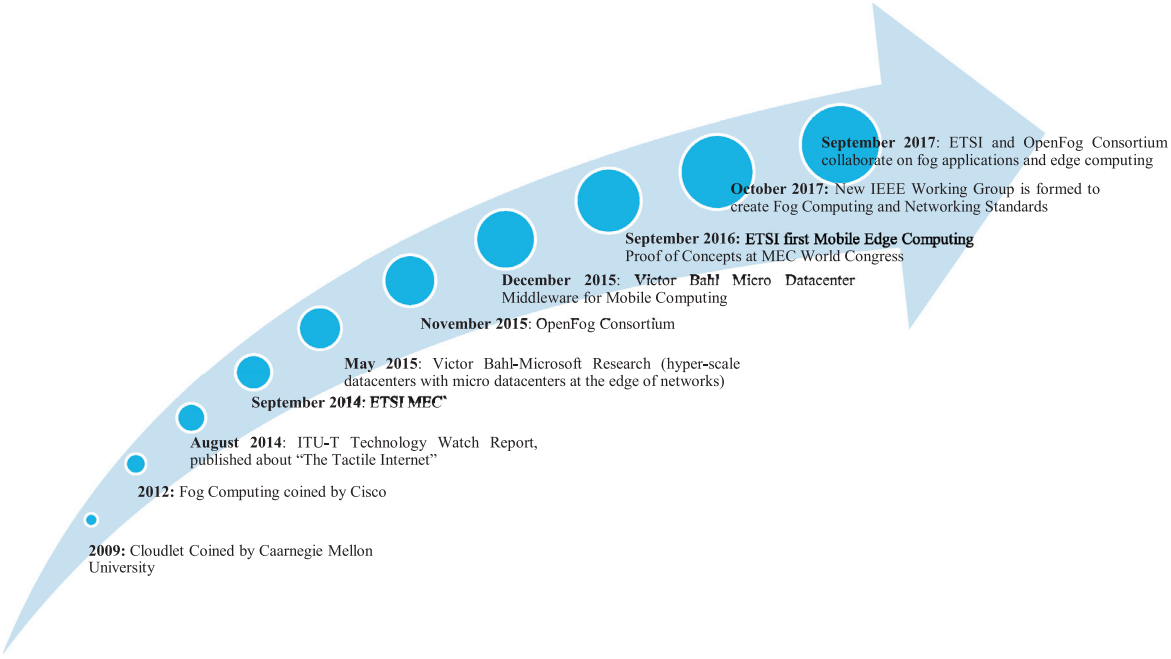


Fig. 5. Fog related technologies timeline.

MEC consists of leveraging edge nodes to enhance mobile devices capabilities. The developers of mobile applications have to account for screen sizes, memory capacity and processing power of different devices, and they must consider the different situations when the processing is done locally or remotely. Handling connection (mobility management) is another issue to deal with. Additionally, while content providers can benefit from giving the MEC's providers insights about users' preferences, it is critical for application developers to protect users' anonymity and privacy. The data synchronization and the mutual trust are the main challenges in this case [139]. Additionally, computation offloading is one of the main MEC challenges having processing and memory limitations [140–143].

3.3.3. Cloudlet

Known also as follow me cloud [144], mobile micro-cloud [145], and mobile cloud computing (MCC), cloudlet, coined by a research group at Carnegie Mellon University, is defined as a small datacenter at the Internet edge [146].

In [147], the mobile edge clouds or cloudlets are considered collocated with the base stations. The authors search to optimize the service migration decision. Their approach is based on the distance between user and base station for simplicity. The optimization problem is formulated using the Markov Decision Process (MDP).

Thus, the main differences between cloudlet and cloud are the rapid provisioning, the fast hand-off, and the cloudlet discovery [148]. Additionally, cloudlets are dispersed at the network edges while the cloud servers are centralized at the core. The cloudlets are managed in an autonomic way while the cloud is managed in an administrative central way. The local edge nodes serve a few number of users giving them augmented reality experience while the cloud case connects a huge number of users [146]. While Cloudlet and MEC were conceived in the mobile domain, the fog computing term is used in the IoT domain.

While cloud computing and edge computing are mainly intended for IoT data processing, storage, and management, there is a need for new networking paradigm to manage the interconnection between the datacenters and/or edge nodes. SDN initially was applied mainly within the datacenters. SDN provided agility and flexibility in deploying and managing the needed network resources for VMs allocation. The need for SDN is more pronounced in the case of distributed cloud nodes (edge computing). In this case, the interconnection and management of the distributed edge nodes call for the SDN manageability. Thus, SDN, NFV, and edge computing can together be employed to handle both IoT data and networks.

3.4. Cellular IoT (5G)

The communication era has witnessed a distinctive evolution; from networks handling analog voice services to fully IP-enabled mobile networks. The first mobile generation (1G) was a revolution supporting user mobility after the fixed telecom network. New services have emerged with newer versions. With the second digital mobile generation (2G), new services and applications have emerged (i.e. text messaging). However, with the third and fourth generations (3G and 4G), distinctive applications have appeared (apple Siri, google glass, etc.) paving the way towards new mobile telecommunication epoch. Cell phones will dominate the future Internet [149]. "Horizon 2020 and beyond" is the tag of the upcoming new era in the telecommunication domain. 5G is not depicted to be an evolution of the previous mobile network generations (2G/3G/4G (LTE)). It is more of a revolution that will change our way of life. 5G is supposed to be the second industrial revolution. Very low latency, high throughput, reliability, security, and high mobility are the characteristics of this upcoming technology [150]. This revolution will enable the cellular IoT paradigm [151]. Main IoT requirements are to be met by this new mobile network. IoT is expected to be integrated in the 5G mobile network [152]. The no cell communication pattern will be supported encompassing the Device-to-Device (D2D) direct communication reducing the signaling and connection time. There is an effort to integrate Machine Type Communication (MTC) into the 3GPP mobile network architecture supporting essentially Human-to-Human (H2H) communication. The mobile network capacity to handle mobile wireless communication makes it suitable for the new emerged communication type. However, the high number of connected devices

Table 4
Software defined (SD) mobile networks.

SD mobile	Summary
SoftCell [156]	Providing fine grained services placing SDN switches at the access points and an SDN controller at the core network.
SoftRAN [153]	Applying SDN to the Access network virtualizing the geo distributed base stations in one virtual big base station allowing for better resources management.
SoftAir [157]	Separating data and control planes. In the data plane reside the SD-RAN (Software Defined Radio Access Network) and the SD-CN (Software Defined Coe Network) and in the control plane resides the SDN controller which runs the network functions applications and services.
SoftNet [158]	Dividing the network in two parts: the core network and the unified access network.
OpenRadio [159]	Providing architecture consisting of two planes: processing plane and decision plane aiming at defining a programmable wireless data plane.
MobileFlow [160]	Introducing the Software Defined Mobile Network (SDMN) that consists of two parts: MobileFlow Forwarding Engine (MFFE) and MobileFlow Controller (MFC).
CellSDN [161]	Defining cell agents allocated with SDN switches able to do some actions (deep packet inspection, header compression, etc.) and a cell operating system on top of which run different applications.

will need a new management paradigm. Overhead in terms of signaling and communicated data must be considered in any mobile network bearing M2M based services.

With the proliferation of smart mobile phones and the dense access to the access nodes, a new paradigm for managing radio access network is needed. The old way adopted in mobile network relies on distributed RAN management. However, the distributiveness has its limitation with high density, high scalability, and low latency requirements. Migrating the control to a centralized entity with a global view of multiple cells will handle better the handover management, power allocation, and interference management. Nevertheless, the decision on downlink allocation per resource block can be given to the local RAN control unit [153]. In this context, applying SDN to the telecom domain has been considered as shown in [154]. Table 4 summarizes the most relevant work done to apply SDN in the mobile network domain.

In [155], there is a proposal for a generalized architecture for mobile networks integrating SDN & NFV. Applying SDN in mobile networks is constrained by the ability of this technology to provide a clear path of migration (support co-existence of different generations), security, QoS monitoring, service provisioning, and cost reduction. The main functions to be softwarized are mainly the mobile network control functions, i.e., MME, HSS, PCRF, and S/P-GW. Additional functions include transport, load balancing, security, policy, charging, monitoring, and QoE or resource optimization.

Recently, a 5G operating system (OS) consisting of three levels of control, device controller, edge controller, and orchestrator controller, was proposed in [150]. The device controller encapsulates certain level of intelligence at the device level (machine learning). However, due to the constrained power conditions, this device might call for higher level of control to optimize its power resources. The edge controller is responsible for L2–L3 functions (forwarding routing, QoS provisioning, mobility management, and charging functions). The orchestrator is the highest level of control, it has the role of managing the cloud resources (links, storage, and memory), the allocation, and the provisioning of the VMs. Everything as a service (XaaS) and IoT are the main profiting technologies from the 5G OS conception.

Consequently, new mobile network architecture (5G) with emergence of new technologies such as SDN & NFV and cloud/fog computing will have a major impact on enabling IoT.

3.5. WSN

Wireless Sensor Network (WSN) is one of the utmost IoT application domains. Being able to wirelessly collect data from sensors spread and integrated into different things is an essential IoT requirement. Also having control over these things thanks to embedded actuators is as important. So, WSN is an essential IoT enabler. However, the wireless technology presents many challenges in terms of security due to the ubiquitous network access and in terms of QoS guarantee due to the unpredictable number of connections (mobility) and the environmental influence (interference).

Essentially, routing is one of the obstacles that was tackled widely in the WSN domain. However, conceiving a routing protocol that is energy efficient, supporting load balancing, and dynamically adaptable to network changes, is not a simple task in the distributed traditional way. Centralizing the control at the master and center node levels will be beneficial in terms of both robustness and energy efficiency [162].

From this perspective, SDN has been essentially applied to the wired networks. Indeed, there are many attempts to apply it to the wireless networks [163]. Sensor OpenFlow [164], and SDWN [165,166] are examples of applying OpenFlow/SDN to the WSN domain. The main idea is to enable SDN on the access points through Open vSwitch along with a centralized SDN controller [167]. This controller has the role of managing routing, flow scheduling, and interference management. Additionally, security related functions are assigned to this central controller.

4. Standardization

4.1. IoT standardization

Standardization is key to achieve any new technology's wide adoption. Having disjoint platforms, architectures and protocols undermine their utility. A standardized IoT architecture is key for the IoT wide deployment in addition to the standardization at the communication level [168]. The TCP/IP standard was the enabler of the Internet revolution. Revisiting its architecture, we found that most of its protocols at different layers are not designed for the IoT case. The "things" in IoT might be constrained devices, so the power consumption at different layers must be taken into consideration [169]. Additionally, the IP protocol itself is overwhelmed by the big number of connected things (already IPv4 addresses pool has been exhausted). In addition, the security related protocols, already not widely adopted in the current Internet network due to their expensive cost (overhead), must be revisited as well.

Under the IETF guidance, several working groups (WGs) have been established in the aim of standardizing new IoT protocols or adapting the existing TCP/IP protocol stack to be suitable for IoT (Fig. 6). CoAP, a lightweight HTTP version and CoRE, which is based on the REST web technology for constrained IoT devices, are application layer protocols. DTLS is a security transport layer protocol suitable for constrained devices (running over UDP). Under the RoLL (Routing over Low power and Lossy networks) WG, the IPv6 Routing protocol for Low power and Lossy Networks (RPL) has been developed. In a parallel effort, IEEE has developed the IEEE

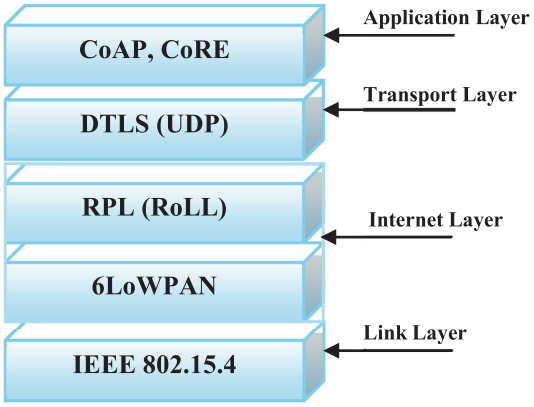


Fig. 6. IoT Protocol stack.

802.15.4, which covers the physical and MAC layers of the TCP/IP stack. The Bluetooth Low Energy (BLE), is another radio communication standard based on IEEE 802.15.1; it is characterized by its low energy and fair data rate, which makes it suitable for some of the IoT applications [170]. The ZigBee alliance builds on top of the IEEE 802.15.4 its own architecture for low power communication network.

However, integrating these protocols in the current Internet infrastructure will not help in overcoming the cited IoT challenges. Perhaps, they will add complexity in terms of management and protocols interoperability. Furthermore, The IoT challenges need to be considered profoundly and correspondent solutions must be engineered harmoniously in one IoT architecture.

4.2. SDN and NFV standardization

The standardization efforts in the SDN and NFV domains are not conducted by a single entity. However, many Standards-Developing Organizations (SDOs), industry consortium, and open development organizations have participated in developing SDN and NFV related standards. The Internet Society (ISOC) has two working groups: IETF and IRTF, that are working on SDN related standards. Interface to routing systems (I2RS) and service function chaining are two groups under the IFTF organization that are working on SDN related specifications. Additionally, IRTF has published an RFC titled "Software-Defined Networking (SDN): Layers and Architecture Terminology" (RFC 7426, January 2015) [80]. The ITU-T has four groups (SG11, SG13, SG15, SG16) working on SDN related projects. Additionally, ETSI was the leader in proposing an NFV standardized architecture. Other open development initiatives like OpenDaylight (under the Linux foundation directory) and Open Platform for NFV (OPNFV) are working on open standards and open source projects that are designed to play an essential role in the business domain [171].

4.3. Edge computing standardization

The Multi-access Edge Computing (MEC) initiative is an Industry Specification Group (ISG) within ETSI that is working on MEC standardization. This initiative aims at developing MEC related specifications mainly the mobile network domain. Doing so, it works to unite the telecom and IT-cloud efforts to enable new applications at the RAN level. On the other hand, the OpenFog consortium, founded by high tech companies and academic institutions (Cisco Systems, Intel, Microsoft, Princeton University, Dell, ARM Holdings), aims at creating a reference architecture to apply fog in the IoT domain.

5. IoT security and privacy: an engineering perspective

The ***security and privacy*** issues hinder the IoT realization. Although, some of the IoT security breaches/vulnerabilities are common with the current Internet network [172], IoT presents new security concerns that make it the "Internet of Vulnerabilities" [173]. Some analysts argue that the security concerns in IoT outweigh its benefits. DY intruder, DoS/DDoS, physical attacks, privacy attacks, eavesdropping, data mining, and traffic analysis are primary IoT attacks [174]. Additionally, new types of attacks related to the constrained things characteristics (low power, low processing, etc.) are IoT specific [175]. Such constraints expose devices to new type of attacks (running out of power, running out of memory, etc.) [176]. Thus, there is a need to propose security solutions that limit the effects of these attacks [177].

In this section, we will review the work done in the IoT security domain. four main security aspects are considered: identity management, authentication, access control, and trustworthiness and privacy. At the end of this section, we will show how SDN/NFV (SDNv2) can be employed to overcome the security challenges in IoT and how it serves in the development of a security embedded architectural solution for IoT.

5.1. Identity management

Practically, what we refer to as being thing identities in IoT, are precisely things identifiers; the identities are more subject-related characteristics (in analogy with the human being case, the identity is the name, last name, birthday, etc.). Usually, in the online systems, we employ identifiers that are a set of uniquely identifiable strings [178,179].

As mentioned before, heterogeneity is one of the IoT challenges. One aspect of this heterogeneity is the presence of different identity schemes in the IoT domain. Device identification is straightforward with RFID; it is performed via the Electronic Product Code (EPC) scheme, which can distinctively recognize "things" from their tags [180]. In ZigBee, devices are identified by their network address, a 16-bit local unique identifier within one ZigBee network. ZigBee also assigns identities to networks via the Personal Area Network Identifier (PAN ID) and the Extended PAN ID(EPID), which are used to refine the identification process [181]. In Bluetooth, devices possess unique UUID identities that are hardcoded into them at manufacturing. The UUID relate to the Device Identification (DI) service record, and a device can have many DIs if it assumes many logical functions. In Wi-Fi (IEEE 802.11), device identification is based on a shared network identifier (SSID) at the access point level on one hand, and on the unique MAC address of the station on the other. As for UMTS, identification is based on the User Services Identity Module, which contains the permanent user's identity (IMSI) and the temporary identifier (TMSI). Finally, in WSN, device identification shifts from being device ID centric to data content identification. The nodes may no longer be identified by their own IDs, but through the data they possess or require. This scheme is referred to as content-based names/addresses [182]. In the Internet, the devices are identified by their IP address (IPv4 or IPv6). In the telecommunication domain, the user equipment is identified by its embedded IMSI code, and the user has a phone number. A summary of the most known device identity schemes is presented in Table 5.

Therefore, having a unified identity scheme is critical to overcome the identity fragmentation in these vertical silos of networks. IPv6 is argued to be the most suitable solution for identification. IPv6 based protocols such GloWBAL, 6LoWPAN, IPsec, and MIPv6 are proposed as solutions to the power related and mobility challenges. Though IP has been the Internet oxygen, it is not obvious that IPv6 will have the same role in the IoT domain. Already, IPv4

Table 5
Device identity schemes.

	Domain of use	Description
IPv4	Internet	32 bits
IPv6	Internet	128 bits
IMSI	Mobile Network	15 digits
Mac Address	Internet	64 bits
Bluetooth Address	Bluetooth Network	48 bits
RFID-EPC	RFID tags	XML
ZigBee-PAN ID	ZigBee Network	16 bits
OneM2M identity	M2M Network	URL

has been depleted and IPv6 adoption is still encumbered in the current Internet. Benefiting from the IP established protocols is key, but we might need to apply new architectural designs and management paradigms [183,184].

In [185], Zhi-Kai Zhang presents a new IoT naming scheme, proceeding from the IoT ITU definition that is based on the ability to connect anything, at any time, from anywhere. There is a proposition of a property-aware name service (PNS). PNS mixes the "what", "where", and "when" aspects of the IoT ITU definition in the object name conception. The object name provided consists of two parts: object name and object location (NV.Obj_Name:: LV.Obj_Location), both containing time stamp information. This scheme needs name resolution and location resolution servers (NRS and LRS), which resembles DNS. The NV and LV parts which provide time-validity checking are compared to the DNSSEC protocol for name based authentication mechanism. The overhead and delay added by the DNSSEC certificates queries make it unsuitable for real-time object name and location resolution. Besides the proposed scheme presents flexibility and interoperability and authentication facilities. In [186], there is a focus on the relation between things and users (owners). Therefore, upon connecting to certain device, you have to be permitted by the devices' owner. In this case, the identity of the thing is related to its owner's identity.

Friese et al. in [187] introduce the Kantara initiative's IDentities of Things (IDoT) discussion group. The discussion group's mission is to identify and analyze the main things identity related issues and to report the existing platforms used or proposed in this context. The authors claim that the name-based scheme (DNS) is not suitable to the IoT case. Regarding the authentication, they stress the importance of context-based authentication and concerning the authorization, they introduce the user-managed access protocol (UMA) on top of the access control framework OAuth.

The work done in [188] presents an IoT architecture and includes the most important technologies used at each level. OpenIDM is proposed for identity management, OpenAM for authentication management, OpenIG for authorization and OpenDG for data accessibility. JSON, REST, OAuth2, LWM2M, DTLS, JS are some of the proposed technologies referred to in this work.

5.2. Authentication

Authentication consists of exchanging identity based information (or credentials) between two parties to confirm the identity authenticity. This service is intended to prevent masquerade and identity spoofing. Cryptography based methods have been established to perform authentication (one way and mutual authentication). However, strong authentication schemes invoke complicated cryptographic operations being computationally expensive. Applying these methods in the IoT domain encompassing a huge set of constrained devices is critical [189]. Some work has considered the emergence of IoT gateways able to handle the computational operations instead of the devices.

In [190], Turkavonic et al. introduce a different perspective of IoT authentication, where the user and the node authenticate themselves directly and not through a gateway. The scheme was presented in a wireless sensor network context, where most of the nodes are of low performance and only few of them are gateway nodes (GWNs) with higher memory and capacity. The GWNs store IDs and keys of all other WSN nodes, and shared keys with users equipped with some sort of a smart card. The authentication step is launched only after the user logs-in and it requests a connection to the node directly. The two parties then share a secret key for subsequent exchanges. Mutual authentication for all three parties is needed in order to safeguard the key exchange session. This scheme is a lightweight yet robust scheme; the authors prove that it provides mutual authentication and key agreement, and security of all passwords. However, the GWNs are required to store IDs and passwords of all WSN nodes and all users, which constitutes a scalability issue for the method, especially that the GWNs are relatively limited in performance and memory.

In [191], a permit code authentication method is proposed. This method is lightweight and can be applied to constrained devices. In [192], a novel continuous authentication scheme is proposed. This scheme uses a public key scheme due to its efficiency in terms of scalability and memory use despite its computational overhead. The public keys are used to generate symmetric keys used as authentication token. The main concept that the proposed scheme introduced is the time factor. So, the generated key is a function of time and the two invoked parties can communicate over a certain period without having to pass into the authentication phase at each time they want to send/receive messages in a short time, which will reduce the overhead in terms of processing, delay and bandwidth consumption.

In [193], there is a proposition of an authentication scheme which relies on an asymmetric authentication method. The ECC algorithm is chosen to generate the private/public keys. In this method, things have their keys generated at the certificate authority (CA) via a secure channel, which is impossible in the ubiquitous IoT network access. The node has to know the public key of each node that it wants to communicate with, and a combination of the other node public key, its private key, and a random nonce are exchanged to do mutual authentication.

Kalra et al. introduced a new feature to cloud server/devices mutual authentication that relies on HTTP cookies and ECC. The protocol is divided into 3 steps. The first step is the registration, where devices subscribe to the server in the cloud by sending their unique identifier. The server would have chosen an elliptic curve, a point G on that curve and a private key. When it receives the identifier, it computes a cookie that is a hash of the unique identifier and the server's private key, encrypts it using ECC and sends it to the device. Whenever a device wants to connect to the server, it sends a hash of the cookie, used by the server to authenticate the device. The server then sends a security parameter to authenticate itself to the device in order to establish the connection. Consequently, they decide on a secret key to be used to encrypt subsequent message exchanges. This is a new technique that relies on cookies and that is independent of device type. However, all devices need to support TCP/IP protocol and HTTP. Furthermore, the secret key is simply XOR-ed with the messages to encrypt them, which is a weak and breakable encryption technique [194].

The RFID technology motivated Kevin Ashton, the British engineer at MIT lab, to launch the Internet of Things term. However, this technology does not provide any kind of authentication and presents many security vulnerabilities. Many authentication schemes have been proposed as shown in [195]. The ECC is chosen for being the most convenient one. This paper surveys the RFID based authentication schemes in IoT in the aim of identifying the best schemes for healthcare environments. The authors compared the performance and the security robustness of different authentication schemes in the literature. The comparison was

done using elliptic curves over F (2163) for key generation. Results showed that all the studied schemes are prone to many attacks. However, three proposals [196–198] were judged to meet the minimum requirements for healthcare IoT applications. The lack of security problem in the RFID domain is tackled in [199]. The EPC code which is widely used in IoT and which is embedded in low power and constrained devices, does not use any cryptographic method, and codes are transmitted in plain text which exposes the authentication process to counterfeit attacks. A lightweight password generation based on XoR is proposed giving some level of security. The RFID technology proved to be efficient in IoT concerning object tagging and identification; especially that it supports all types of objects. Although it offers an edge to IoT, it suffers from many drawbacks, most importantly the lack of security. Aggarwal et al. study this issue in [20], showing advantages and disadvantages of RFID, and propose an improved RFID scheme for IoT. Their method performs authentication at the tag level. The reader sends its ID XOR-ed with a 128-bit random number R and then shifted by the weight of R. The tag used the received value to recover R, apply transformation on it and XOR it with its ID. The resulting value is sent via the reader to the backbone server that is able to authenticate the tag by recovering it from the received value and comparing it to the stored ID. A system is as strong as its weakest link. Therefore, in order to ensure a secure IoT network with RFID, security should be enforced even on the tag reading level. Furthermore, the authors show that the scheme is resistant to many attacks such as replay and disclosure [200].

Shivraj et al. review different techniques used for IoT authentication. They also set forward their own authentication process that relies on the One Time Password (OTP) technique developed with Elliptic Curves Cryptography (ECC). In their design, a PKG unit holds the IDs of all devices and applications in the network. At this stage, nodes acquire their public Keys from PKG and compute their respective private keys. When a connection is to be established between an application and a device, the latter sends the ID of the node they wish to connect to the PKG. The PK automatically generates the corresponding private key out of which it computes a one-time key. This key is sent to both nodes, which validate the connection by comparing the key with each other. The scheme was shown to be more efficient than other existing methods when it comes to the size of the key and the security robustness. The KDC does not store Private and Public keys of devices, it only stores their IDs. Consequently, hacking the KDC does not incur compromising the keys of all devices in the network. However, the OTP adds computational overhead since the KDC is required to compute a new one-time key every time a new connection between devices and applications is to be created [201].

The authors in [202] combined IoT concept with the Federated Identity and Access Management (FIAM) technique to address device authentication. The method was inspired from the web. It is composed of four agents: the device or the thing that was implemented with Arduino, the authorization server implemented in WSO2 that allows the creation of users and OAuth applications, the authorization tool to enable timely access, and the MQTT unit that supports plugins for authorization services. In this scheme, the nodes and the MQTT unit verify each other via the OAuth platform. The proposed framework is a compilation of many existing standards. This system is built with specialized components, which makes it more robust and secure. However, integrating these components might be problematic, which is why the authors faced many concerns during implementation.

The work done in [203] approaches the two-steps authentication scheme used in today's business transactions. Instead of using a verification code sent to the mobile phone, the authors propose the use of a smart card for generating keys on the devices directly. Having credentials and keys at the same place and issued by the same party might have security issues. The proposed scheme tries to separate data and encryption keys. This method provides high security. The need to have smart cards makes this method impractical.

The authors in [204] present a dynamic adaptive authentication scheme for IoT (DAoT). This scheme switches between key establishment (KE), message authentication code and the TLS handshake based on the energy level of the constrained device. This scheme allows energy saving. An evaluation of the effectiveness of the proposed scheme is done using the Crypto++, a TestCrypt benchmark tool. The energy consumption is measured using an energy cost model that gives an estimation of the energy cost of each cycle. The results show that ideal amount of energy cost savings by DAoT. And even if the state of devices changes, DAoT can adjust the cost gap in stabilized state by feedback control scheme. Dynamic adaptation of the authentication method to the energy level of the device.

The architecture proposed in [205] lacks the autonomy of things, which is a main concept in the Internet of Things. Bai et al. revisit the issue of the integration of IoT in Cloud computing, in the aim of providing data online that can be accessed anywhere at any time. The architecture is composed of three islands connected via MPLs tunnels. The first island consists of users; IoT enabled smart card (ISC) per user, and readers. The ISC assigns a unique identifier to each user and transmits data to readers periodically. The information collected by the readers is relayed to a smart gateway that filters data and sends it to the authentication island. The latter is in charge of verifying the identity of users and integrity of data. The authors use X.509 version 3 certificates based on ECC to achieve authentication at four levels: user's authentication, mobile device authentication, smart card and cloud server authentication. When authentication is complete, data is sent to the cloud server and stored in the cloud. This technique works with different IoT applications and devices and overcomes the protocol/vendor specific limitations. Furthermore, the different levels of authentication provide a robust security design. The ISC card is attached to users, however, this scheme might not scale if identities were given to all things [205].

In [206], Sungchul et al. propose an authentication scheme for RESTful web services in the IoT. This approach considers that each IoT object is presented by a unique URI. The REST being stateless presents some issues at the authentication level. The proposed method utilizes the ID-based encryption.

A comparison of the most used authentication methods: password, token, smart card and biometric is done in [207]. The comparison shows that although the biometric based one is the most secure one to authenticate human beings, it lacks applicability in the IoT domain. The smart card based method is the second secure one to authenticate its owner based on different applications. Then, the token-based authentication scheme is more secure than the password based one that is considered as the least secure one. The authors stated that there is a need to investigate the impact and the challenges in adopting any of the existing authentication schemes in the IoT domain. Table 6 summarizes the advantages and disadvantages of these methods.

5.3. Access control

Access control is a very critical part of the IoT security scheme. Guaranteeing authorized access to the collected data is an important task. Access control was mainly tackled in the web of things context [208]. Frameworks such as: OAuth [209], Shiro [210], and LDAP [211] have been proposed to manage the things roles description and access rights. Access management in IoT is a strongly related task to the identity management one. Having a unique identity, the thing can be granted access to the appropriate resources.

Table 6
Authentication schemes.

Authentication scheme	Advantages	Disadvantages
Public/Private Keys	Scalability	Complexity and computing overhead
Symmetric Key	Simplicity where same key is used for en/decryption	Scalability
Biometric	Simplicity	Availability and applicability
Identity Card	Robustness	Scalability
Passwords	Simplicity	Scalability and maintainability

Thus, the gateway layer in the IoT architecture will play a key role in the identity and access management process [212].

However, the high scalability of the IoT network makes the discretionary access control (DAC) configured per user or device used in today's web based applications not suitable to the IoT case. This calls for alternative scalable solutions. Mandatory access control (MAC) which was used in Operating system domains can be applied with the SDN integration in the IoT domain.

5.4. Privacy and trustworthiness

Privacy, a term related to Personal Identifiable Information (PII), is the ability to decide who can see our private data. Having our private assets connected to the Internet, privacy is a very important requirement in the IoT case. On the other hand, trustworthiness is a measure of how much a service or communicated data can be trusted. Having constrained devices prone to diverse attacks and third-party applications, a trustworthiness model is needed to protect our devices and data from a malicious exploitation.

In [213], a model, that relates trustworthiness to privacy, is proposed. This formal model can be used in an automated security framework to evaluate trustworthiness and guarantee the data privacy. In the RERUM consortium report [214], a model of the trustworthiness of IoT services is proposed. This model relies on a measure of reputation that helps in deciding if we can rely on certain service or not. The logs of the trustworthiness level can be used for notification in case of drastic changes (e.g. attack). In [215,216], Nitti et al. consider the social Internet of things. In this case, the data provided by the users are considered as services that need to be trusted. Thus, their model consists of measuring the trustworthiness of the users by asking their friends. The distributed evaluation framework is shown to be able to isolate malicious peers. In [217], a reference architecture for improving security and privacy of IoT applications is proposed. The authors consider the IoT applications as being the entities that need to be trusted by the IoT devices and thus an evaluation of the users' rating for these apps is presented.

5.5. SDN and NFV based security for IoT

SDN presents some security issues due to some of its characteristics such as the centralization one that makes it vulnerable to DoS attack per example [218]. However, its improvements in terms of providing an architectural based security solution overweight its disadvantages [219]. SDN provides a global view of the network thanks to the control centralization and thus the monitoring and consistency verification tasks become straightforward ones. Furthermore, the mitigation of some attacks (e.g. DoS, DDoS, etc.) become easier [220–223]. Thus, flow-based security schemes can be implemented dynamically at the network edge [224,225].

In [226], the first network access control (NAC) using SDN through the use of multiple flow tables in the OpenFlow v1.3 protocol is proposed. It is shown that there is a reduction of 72% in terms of packets exchange compared to the captive portal approach and up to 80% reduction in terms of authentication delay.

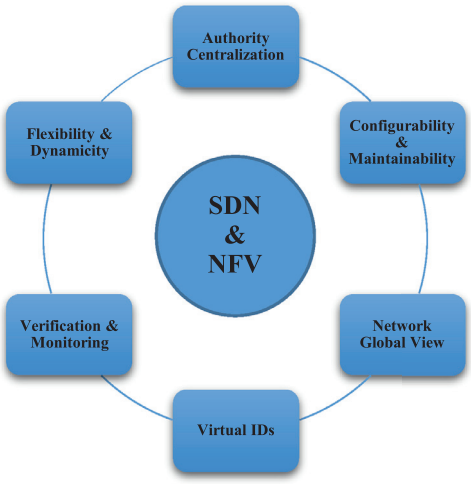


Fig. 7. SDN & NFV security benefits.

Additionally, due to the virtualization integration, the isolation of flows become seamless. Therefore, the identity management on top of the heterogeneous identity islands needs a decision centralization guaranteeing the uniqueness of control. The authentication function was traditionally accompanied with central entities (PKI Servers, CAs, etc.) providing keys, authentication certificates, and related security services. The access control task is also accompanied with central authority managing the access permissions and roles. Above and beyond, SDN provides flexibility and agility in configuring and modifying security rules which makes this network evolvable and updatable. Dynamicity of the IoT applications and services call for easily configurable security rules and policies [227].

Indeed, as summarized in Fig. 7, SDN and NFV bring novel benefits to the network security domain and especially in the IoT large scale network case. Having a global view of the network with periodically collected statistics, the SDN controller can detect abnormal behaviors and isolate the concerned flows or nodes thanks to the virtualization techniques. Moreover, SDN presents flexibility and dynamicity in configuring the corresponding rules at the data plane level. Additionally, the network functions are softwarized and thus intelligence can be easily implemented at the controller level for intrusion detection. Therefore, having multiple applications that might modify the data plane rules, verification of rules' consistency can be implemented to avoid network error.

5.6. Challenges

Applying SDN and virtualization in IoT brings its own security concerns: concerns about device bootstrapping, identity management, key management, and authorization. Device bootstrapping and key management should be standardized in the future to provide a common management interface to facilitate secure device configuration, thus enabling large-scale IoT deployment [228].

After revising the work done in the IoT security domain, we found that most of the work presents limitations. The proposed

IoT architectures lack the integrated approach to security. Adding security solutions after the fact will be costly and has historically proven ineffective. Therefore, the high IoT scalability demands automated security solutions [229–231].

No matter how robust are added security measures, a secure infrastructure is a prerequisite. The underlying IP based infrastructure is by itself vulnerable, starting from the IP spoofing attack to more significant vulnerabilities [232]. In this context, applying SDN and NFV can alleviate several of the IoT security challenges. However, as SDN brings benefits in terms of security management, it poses new security challenges. The centralization of the intelligence, at the controller level, makes the SDN controller a single point of failure. Particularly, if the controller is hijacked, the attacker gains control of the network. Moreover, the controller is prone to DDoS attack where the switches can be maliciously programmed to flood the controller with OpenFlow packet-in messages. On the other hand, the switches can also be hijacked, and thus inconsistent rules can be added compromising the network availability. Additionally, SDN allows third party applications which makes the network prone to malicious application attacks. Thus, unauthenticated applications and northbound interfaces can employ the controller to compromise the network consistency and availability [233].

6. IoT Big Data: a management perspective

It is not about "things"; it is about data. Effectively, the IoT innovative value lays on a collected data foundation [234]. The ***IoT "Big Data"*** is about 3 V's: Volume, Variety, and Value [235,236]. To an extent, we can say that there is no IoT without the sense of data. It is not about the size of collected/generated data; it is more about the diversity, heterogeneity, dispersity of this data. Having the data shared between different entities poses security and privacy concerns [237,238].

Handling the IoT "Big Data" in a global IoT architecture is evident. In this context, the integration of data interoperability in a general IoT architecture is key [239]. Managing this data calls for advanced data technologies. Cloud computing related aspects are expected to play an essential role in this context [239]. Additionally, SDN is expected to improve IoT big data applications [240].

6.1. Cloud computing based IoT solutions

Different cloud-based IoT architectures have been proposed in the literature. A typical cloud based IoT architecture is proposed in [241]. This architecture consists of three layers: the sensor layer, the cloud central layer, and the application layer. A sensor bridge connects the sensors to the cloud. An IoT framework is proposed in [242]. This framework consists of three layers: device layer, central hub layer and cloud layer. Essentially, the device has two principal parts: the micro-controller (i.e. Raspberry Pi, Arduino) and the communication component which allows its connection to the network. The central hub layer presents a kind of gateway that is a middle point between devices and cloud layer. The cloud layer consists of three subcomponents: web server, web application and database. In [243], the authors consider IMS (IP Multimedia Subsystem) as being the solution to integrate IoT and cloud. Their proposed architecture consists of three layers: The IoT device layer, the IMS core network, and the cloud layer. Most of the needed services (Naming, communication, management, etc.) are supported by IMS. Mobile Cloud Computing is principally introduced to overcome the mobile devices incapability in terms of storage and computation [244,245]. Mobile cloud computing an integration of mobile and cloud computing domains. It is a platform where both storage and processing are leveraged to a third party the cloud outside the mobile phone [246].

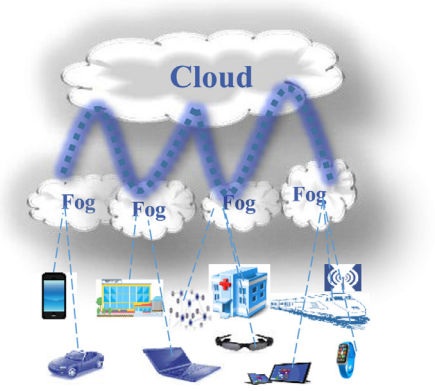


Fig. 8. Fog tiered architecture.

Thus, the principles to build an IoT cloud system are summarized in seven points in [247]: enabling virtualization, enabling emulation and simulation of IoT units, enabling monitoring, dynamic provisioning, enabling softwarization, providing software-defined elasticity, and providing elasticity at the different levels. The proposed software-defined machine (SDM) consists of three hardware and software layers: vertical domain application and middleware, general purpose OS, and hardware layer. To meet these requirements, new cloud management means have to be introduced. SDN, which will be revisited in detail as an enabler technology for IoT in Section 7, has retrieved its precious management role in the datacenter and cloud domains [248].

Software defined units are proposed to be the base of an IoT cloud system. Integrating SDN in a cloud system provides elasticity, dynamicity, automated provisioning, policy-based configuration, fine-grained resource consumption, self-service model, and API encapsulation of IoT resources and capabilities. The main component is the IoT unit encapsulating functional (storage, computation, communication) and non-functional (security, configuration, quality) aspects. These fine-grained and modular units compose more complex components on demand [249]. In [250], SDN is shown to enable processing of the IoT data at the network level. Consequently, the number of packets sent over Internet to the cloud decrease.

Cloud networking and cloud inter-networking with interoperability across different providers and platforms are provided through an overlay layer of federation management. OpenDOVE is used as a cloud orchestrator in [251]. Thus, open source cloud networking tools such as OpenStack, OpenDaylight, and Open vSwitch are used to manage cloud systems [252].

6.2. Fog computing/MEC/Cloudlet based IoT solutions

The distributed set of mobile devices impose a geo-distributed set of data. Additionally, the ***IoT high scale*** makes the centralization of data a critical mission. Consequently, a distributed set of fog nodes is required.

The proposed fog model in [253] follows the fog tier architecture design (presented in Fig. 8) adding the notion of IaaS interface between cloud and fog and defining a PaaS programming model for the fog layer. The proposed model separates or differentiates logical and physical entities. The fog applications are not deployed at the fog nodes, despite the mobile fog application is an ensemble of processes running on the computing nodes in cloud, fog or end devices. The application design consists principally of APIs and events handlers supporting the main fog functions (receiving, sending messages/notifications).

The authors in [254] shed the light on some heterogeneous use cases that call for the fog computing application. The authors

choose different use cases where fog nodes characteristics (e.g. mobility) are different. The authors add a new dimension to the big data Vs, the geo-distribution one that calls for fog integration. In this context, a high-level fog software architecture is described. This platform consists of four components: the devices, the abstraction layer, the orchestration layer (sense, analyze, plan and execute) and a northbound APIs that connect the orchestration layer to the application layer.

The integration of fog and cloud is proposed in [255,256]. The proposed IoT fog-based architecture consists of: analytics layer, virtualization layer, reconfiguration layer, and hardware layer. The fog nodes can be reconfigured to meet the different applications requirements.

Therefore, SDN, presenting management facilities, can be employed to deploy fog/MEC/cloudlet nodes [257–260]. In [261], a software defined fog node based distributed blockchain cloud architecture for IoT is proposed. The presented architecture aims at implementing distributed security scheme at the network edge level. In [262], a software defined fog-based architecture is proposed. Similarly, virtualization helps in facilitating the deployment of the fog nodes [263–265].

6.3. Challenges

The cloud-related solutions handle the IoT Big Data management (storage, processing, and analysis). However, the IoT data need to be contextually analyzed to extract useful insights from this data. Consequently, data from different cloud/edge nodes need to be collected for this aim. While SDN can be employed for interconnecting the datacenters and the edge nodes, the interconnection of the data nodes needs special protocols and networking paradigm (e.g. Information Centric Network (ICN)).

Furthermore, the fact that data need to be stored at different locations, the decision where to put which data needs to implement intelligence at the application level. Moreover, the security of the communicated data and the management of the access control to this data is a challenge that needs to be considered in any cloud/edge-based solution.

7. IoT heterogeneity: a middleware perspective

7.1. IoT gateway

Owing to the massive ***heterogeneity*** in the IoT domain and the presence of vertically integrated domains and applications, the call for a gateway layer is crucial [266]. Thus, the IoT gateway has to perform multiple functions such as: protocols translation (NATing [267]), service chaining, security related functions (firewall, authentication, access control, etc.), data mining, QoS management, mobility and handover management, and routing and forwarding packets (Fig. 9) [268].

In [269], Datta et al. propose a OneM2M based IoT gateway. This gateway consists of a OneM2M middle node performing mainly three functions: data analysis, resources discovery, and device management. The authors propose a fog computing architecture based on the OneM2M standard. The vehicular networks use case is shown as a direct application, where the gateways are fog enabled and deployed on the Road Side Units (RSUs) providing the consumer centric services such as data analytics and semantics, and vehicles discovery and management. Besides, the IoT gateway plays an initial role providing services and resources discovery. The Distributed Hash Table (DHT) and Distributed Geographic Table (DGT) algorithms employed in the P2P networks are used to discover neighbors and services in [270]. Applying cloud/fog computing paradigm to the gateway layer is key to handle data related services. BETaaS (Building the Environment for the Internet

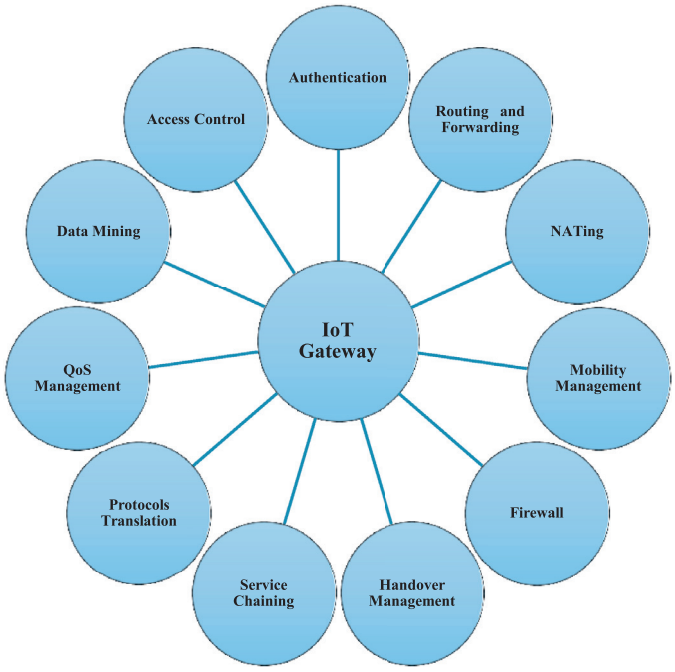


Fig. 9. IoT gateway **Function.**

of Things as a service) is presented in [271]. The authors try to employ virtualization on top of the BETaaS gateways, so each VM can run certain applications. However, the need for high processing computations cannot be met by the edge nodes presenting power and computing resources limitations. Therefore, the migration to the cloud is necessary for certain complicated tasks. Benefits of edge mining reducing the traffic between edge and core are presented in [272]. Data trimming is one of the Cloud of Things (CoT) challenges. In [273,274], a smart gateway functional architecture is presented. Main tasks of this smart gateway are: collecting, preprocessing, filtering and reconstructing data into more valuable one, uploading only necessary data to the cloud, tracking IoT objects and sensors' activities, tracking IoT power constrained nodes energy consumption, security and privacy of the data, and overall services monitoring and management [275].

Use of mobile phones as IoT gateways having the capability of transferring the data over wide area networks has been proposed in the literature [276,277]. In [278], Datta et al. have proposed a gateway having the role of translating the data requests/replies collected from the sensors and transmitted to the mobile applications. The access to data can be done in two ways: polling request to the gateway or registering to the gateway for notifications. The gateway is mounted on a Google Application Engine (GAE). The user is presented by its mobile application profile. Thus, the gateway functionalities, the scalability concerns, and the security issues have to be considered extensively. In [279], Datta et al. have proposed a mobile application to Connect and Control Things (CCT). This application uses the mobile phone to connect and control M2M devices through a gateway. This gateway translates the different technologies. The authors deploy the proposed application on a GAE where the messages are transported via HTTP. Future extension to support other messaging protocols is necessary. These messages contain SenML (Sensor Markup Language) based data. An SenML extension to support actuation messages is proposed. The SenML [280] is an ongoing standardization work that defines a standard format of the sensor measurements.

However, closeness and hardware dependence limit the gateway's capability to support dynamic IoT network features. Virtualization migration from the ICT world to the network domain

will have an impact on the networking functions deployment [281]. Now, the current IP packets are processed by multiple middle boxes (e.g. load balancer, firewalls, etc.), if special forwarding paradigm has to take place. However, the middle boxes closed infrastructure incur complicated management and configuration tasks. SDN & NFV are coming to hide these complexities making the networking functions software based tasks, that can be deployed anywhere and on any hardware. Thus, the management and configuration tasks become easier and maintainable [282]. IoT gateways, meant to be deployed in big numbers, have to benefit from the SDN & NFV paradigm to be easily manageable. Intelligence and service chaining are other features acquired integrating SDN & NFV in the IoT gateway layer. The smart IoT gateways have to perform networking and data related functions. The integration of all functions in hyper-convergent smart boxes with SDN & NFV and cloud integration is proposed in [283]. Open vSwitch is proposed as being an intelligent edge in [284]. The proposition of an intelligent gateway is done in [285,286]. An extended MQTT queuing method is integrated into this gateway to support an enhanced QoS management mechanism.

With the introduction of these revolutionary technologies, service chaining becomes a straightforward task [287]. Dynamic network service chaining built on top of software-defined edges is tackled in [288]. These edges are deployed in a datacenter as software engines running on virtual machines. An emulation is done using Mininet as proof of concept; Pox (SDN controller) is used to configure the switches/routers edge nodes with the correspondent rules. In this setup, the authors use hybrid switches which support both SDN and legacy network functionalities.

In [289], an edge-computing platform for IoT gateways, called Paradrop, is presented. This platform is characterized by the dynamicity, the management through OpenFlow, the supported APIs and security functions. In [290], the SDG-pro (software-defined gateways programming framework) for cloud IoT system is presented. In this framework, software defined gateways are provisioned and deployed dynamically on edge nodes by IoT controller units in the cloud. This approach allows the “everything as code” paradigm to deal with the IoT network dynamicity and scalability.

The work done in [291] tackles the IoT gateway problems. The authors claim that today’s IoT solutions depend on closed application-layer gateways. The authors compare the today’s IoT application specific gateway to having a browser for each website, which is not an intelligible solution. Their proposed architecture consists of having a smartphone as an IoT gateway. The used communication technology is BLE where the smartphone is the master node and the peripheral things are the slaves’ nodes. Each slave node sends beacons periodically to notice its presence to the nearer master and the master has the role to establish the connection between slaves. The smartphone can forward the IPv6 packets from the peripheral nodes, if supported. If not, it has to act as a proxy to translate the different packets to IPv6 format. Several questions can be posed concerning the security, privacy, trust, user incentive, and reliability.

In [292], different approaches used for conceptualizing an IoT middleware have been presented. These approaches are compared in terms of the challenges that can overcome; these challenges are mainly: interoperability, trust, scalability, mobility, heterogeneity abstraction, spontaneous events, random topology, multiplicity, unknown data-point availability, security/privacy, actuation conflicts, bootstrapping, extensibility, modularity, and real-world integration. The analysis shows that there is no approach that can tackle and overcome all the challenges. Additionally, some challenges: trust, actuation conflicts, and bootstrapping, are not solved yet by any middleware approach.

The work done in [100] introduces the device-centric approach comparing it to the data-centric approach that relies on collecting and providing data without caring about devices ’identity. IoT-A, SENSEI, FI-WARE, BETaaS, IoT6, etc.: all these projects aim to provide IoT cloud based architectures where the main scope is the data (data-centric). However, in [100], the purpose is to provide or deploy sensing and actuating cloud services. So, the user can provision services despite of asking for data (service-centric).

Table 7 shows the different approaches used in conceiving an IoT middle ware. These approaches can be categorized in four types: device centric (where the focus is on the device itself, so it has its own identity), user centric (where the device identity is related to the owner identity), data centric (where the data has to be identified), and service centric (where everything is served as a service (XaaS)). Each of these approaches has its advantages and disadvantages.

7.2. Challenges

Applying SDN and NFV to design an IoT gateway presents many advantages: programmability, management flexibility, configurability, etc. However, being controlled by an SDN controller, the gateway needs to communicate with the controller to populate its forwarding table which makes the controller a single point of failure. In case of connection failure, the gateway cannot operate in standalone mode for an extended period of time while maintaining correctness of the rules. This hints at the need for hybrid gateways that can operate in two modes (SDN and/or non SDN).

Furthermore, employing cloud/edge computing techniques for data management at the gateway level pose new challenges. The data distributiveness calls for new data-based networking paradigm. Taking the decision of which data need to be processed and analyzed at the gateway level and which need to be transported to the cloud is another challenge that calls for data classification and tagging at the device level.

8. IoT scalability: an architectural perspective

Having billions of things connected to the Internet in the future network, the network architecture needs to be rethought. Many IoT architectures have been proposed in the literature (Table 8). This situation is similar to have multiple remote controls (for managing different types of devices the DVD, TV, AC, etc.) all functioning the same way, but no one can replace the other [303]. For enabling the IoT wide deployment, we need a common agreed upon architecture as the case of the TCP/IP Internet architecture. The architectural diversity and heterogeneity and the absence of interoperability between these different architectures devalorized their utility [304]. SDN is intended to overcome this heterogeneity providing a common control layer on top of these different IoT architectural silos. In the following, we will review the most known IoT architectures and the most recent work applying SDN & NFV in a generalized IoT architecture. The layered representation of these different architectures is summarized in Fig. 10.

8.1. iCore

The iCore project defines three main levels in its framework: the virtual object level (VO), the composite virtual object level (CVO), and the service logic level. These levels aim at abstracting the heterogeneity at the physical object layer and provide cognitive services to ensure reliability [305].

As part of the iCore project, [306] presents a distributed framework for IoT. This framework consists of four modules embedded in IoT daemon: the virtual object layer (VOL), the composite virtual object layer (CVOL), the service layer (SL) and the security management (SM) module. This framework tends to provide interoperability between different IoT application domains. Mainly, each

Table 7
Middleware IoT approaches.

Approach	Description	Advantages	Disadvantages
Device-centric	The devices are identified and connected to the network.	Connectivity and security management	Scalability and heterogeneity
User-centric	The focus is on the device-user relationship; the device's identity is based on the owner's identity.	Scalability and management facility	Lack of M2M type of communications
Data-centric	The focus is on data; the data will be identified, labeled, and classified without caring about user or device identity.	Big data handling and Interoperability	Added complexity (e.g. data classification)
Service-centric	The focus is on the services; services are provided to registered users upon request.	Scalability and interoperability	Reliability

Table 8
IoT Architectures Initiatives.

Architecture	Description	Partnership
IoT-A [293]	A proposed IoT Architecture Reference Model (ARM) under the F7 European project.	Alcatel Lucent (Belgium, France), CEA (France), CFR (Italy), CSE (Greece), FhG IML (Germany), Hitachi (UK), IBM (Switzerland), NEC (UK), NXP (Germany, Belgium), SAP (Germany), Siemens (Germany), Sapienza University of Rome (Italy), University of St. Gallen (Switzerland), University of Surrey (UK), University of Würzburg (Germany), VDI/VDE-IT (Germany), VTT (Finland).
IoT6 [294]	A 3-year F7 European research project for researching the IPv6 potential for IoT.	Mandat International (Switzerland), Ericsson (Serbia), RunMyProcess (France), University College of London (UK), University of Murcia (Spain), Vienna University of Technology (Austria), University for Applied Sciences Western Switzerland (Switzerland), University of Luxembourg (Luxembourg), KAIST (S. Korea).
iCore [295]	An IoT project aiming at abstracting the heterogeneity and representing the different user/stakeholders view. Cognitive context awareness, reliability, and energy efficiency are main goals of the conceived solution.	12 industrial partners from which 8 are leading ICT manufacturers (Alcatel, Bell labs, Atos, Fiat, Siemens, Software AG, Telecom Italia, Thales), 5 SMEs (Zigpos, Ambient, Arago, Innotec, M3S, Trilogis), 4 universities (Delft University of Technology, University of Surrey, University of Piraeus, KAIST), and 5 research centers (Create-Net, JRC, TNO, VTT, Wuxi SensingNet Industrialization Research institute)
OneM2M [296]	A service layer abstraction to overcome the vertical heterogeneity while ensuring compatibility with older M2M architectures.	8 of the world leading ICT's companies (Arib, ETSI, Atis, CCSA, TIA, TSDSI, TTA, TTC), 6 global fora and SDOs (Broadband Forum, CEN, CENELEC, Global Platform, Next Generation M2M Consortium, OMA) and over 200 companies in all industry sectors.
IoTDM [297]	IoT data Broker for oneM2M based infrastructure	Committed by Cisco, ETRI, Echelon, Technicolor (it is part of the Lithium ODL version)
FIWARE [298]	Provides a set of APIs to develop IoT applications	Independent Open Community
BUTLER [299]	uBiquitous, secUre inTernet-of-things with Location and contExt-awaReness project to enable development of secure and assistant life applications.	INNO, Ericsson (Spain), Telecom Italia, GEMALTO, CEA, CWC, FBConsulting, ISMB, I Home Lab, ST, University of Luxembourg, K.U. Leuven, TST, Jacobs University, ZIGPOS, Maya Technologies, Banco Santander, Santander City Council, Tecnalia
COMPOSE [300]	Collaborative Open Market to Place Objects at your Service	5 Industrial partners (IBM (Israel), INNOVA (Italy), U-HOPPER (Italy), CELLNEX (Spain), EVRYTHNG (UK)), 4 research Institutes (BDIGITAL (Spain), BSC-CNS (Spain), Fokus (Germany), Create-Net (Italy)), 2 universities (Open University (UK), University of Passau (Germany)), and one standardization body (W3C).
IEEE Project P2413 [301]	No new architecture but a high-level description to enable cross-domain applications and compatibility between different architectures.	BroadBand Tower, Cisco Systems, Emerson, EPRI, Finger Food Studios, Hitach, Honeywell International, Huawei Technologies, Infocomm Development Authority (IDA), Intel, Kaspersky Lab, Korea Electronics Technology Institute (KETI), NIST, Qualcomm Inc., Renesas, Rockwell Automation, Schneider Electric, Senslytics, Siemens AG, SIGFOX, STMicroelectronics, Toshiba Corporation, Wipro, Yokogawa Electric Corporation, ZTE.
TRESCIMO [302]	Testbeds for Reliable Smart City Machine to Machine Communications (TRESCIMO) is a project under the European Union's FP7, Future Internet Research and Experimentation initiative.	EUR, TUB, Fraunhofer, CSIR, UCT, ABS, ESKOM, I2CAT

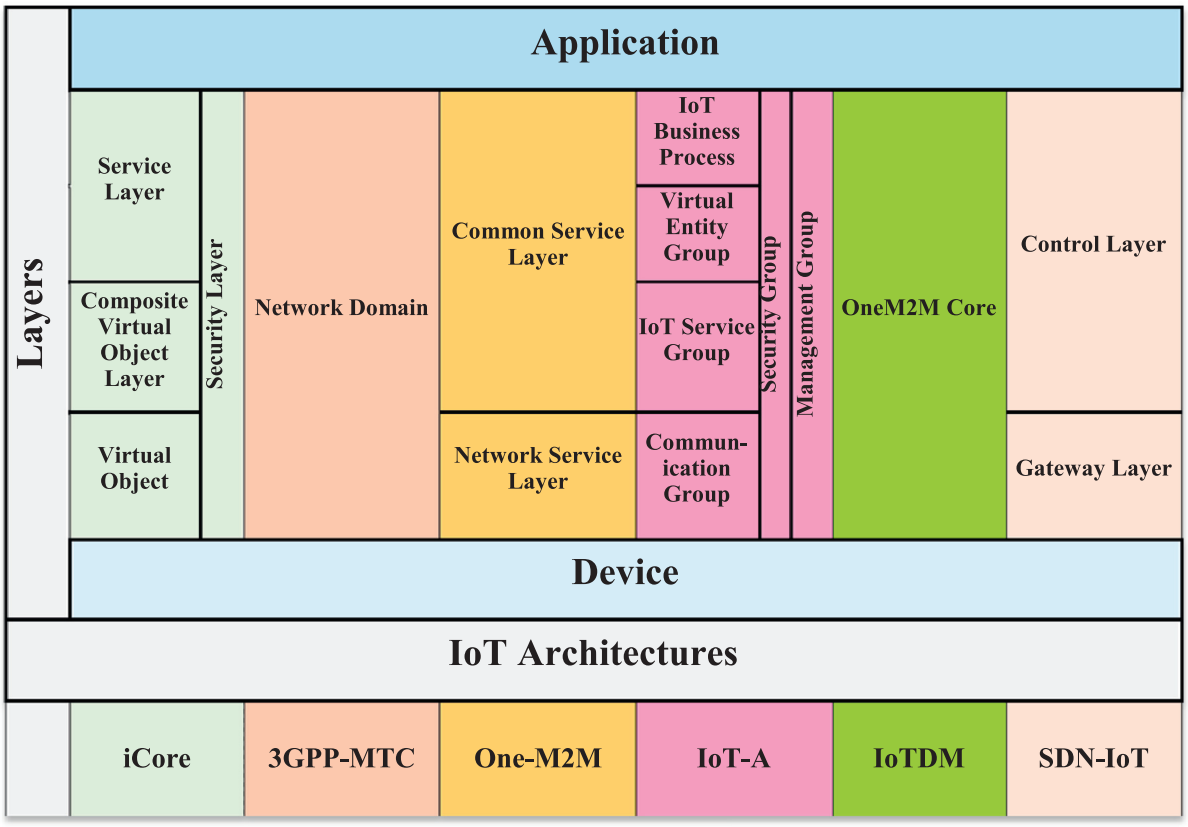


Fig. 10. IoT layered architectures.

object must run this daemon and some layers can be omitted due to power and processing limitations.

The fact that an integration of the proposed layers has to be performed in the IoT devices, this architecture presents scalability and interoperability limitations. IoT solutions are already there, so imposing change in the present devices is an impractical solution.

8.2. 3GPP MTC architecture

Taleb et al. in [307] present the 3GPP MTC architecture. 3GPP is the 3rd Generation Partnership Project alliance grouping the Alliance for Telecommunications Industry Solutions (ATIS), the China Communications Standards Association (CCSA), the Open Mobile Alliance (OMA), IEEE and the European Telecommunication Standards Institute (ETSI), the Association of Radio Industries and Businesses (ARIB), the Telecommunications Standards Development Society (TSDSI), the Telecommunications Technology Association (TTA), and the Telecommunication Technology Committee (TTC) as organizational partners. This Machine Type Communication (MTC) initiative aims at introducing the M2M communication into the mobile network supporting initially the Human-to-Human (H2H) communication. The presented architecture consists mainly of three domains: the device domain, the network domain, and the user application domain. The device domain is where heterogeneity resides; this heterogeneity is in terms of supported communication protocols, device capabilities (power, processing, and storage), and supported security measures. The network domain is mainly the mobile core network (e.g. EPS in the LTE case) [308].

Kunz et al. in [309] present the main requirements, use cases, and key issues over the successive 3GPP MTC releases (10, 11, and 12). New features are intended to be added with new releases. Essentially, in the 5G era, the MTC surely has to be supported and new capabilities will be added as this new network provides revolutionary features [310].

8.3. OneM2M

OneM2M is an M2M based architecture aiming to provide an IoT middleware [311]. OneM2M intends to combat the fragmentation by implementing a horizontally deployed middleware service layer above the different vertical M2M silos networks and applications. Swetina et al. in [312] introduce the OneM2M standard. Essentially, the OneM2M architecture consists of three layers: Network Service Layer (NSL), Common Service Layer (CSL), and the Application Service Layer (ASL). These layers are presented by three types of entities: Network Service Entity (NSE), Common Service Entity (CSE), and the Application Service Entity (ASE). Five node types are included in the OneM2M functional architecture: Infrastructure Node (IN), Middle Node (MN), Application Service Node (ASN), Application Dedicated Node (ADN), and Non-OneM2M Node (NoN). These nodes are separated into two categories: CSE enabled and Non CSE enabled. These nodes essentially reside in two domains; The field domain contains the IN which presents the provider services and in the field domain reside the MN which is typically a gateway, the ASN which is oneM2M device, the ADN which is a constrained oneM2M device not presenting service providing capability, and the non OneM2M device which is normally a network device providing the underlying network services (location service, management service, and triggering service) [313].

In a myriad of M2M architectures and solutions, there is a need to retrieve a common middleware layer to combat the fragmentation and provide interoperability between these different silos. The global standardization initiative is launched in July 2012. Then,

the first version is released in December 2014 with ten specifications published online. These specifications tackle the main services provided by the CSL such as: registration, security, service charging and accounting, subscription and notification, discovery, group management, location, network service exposure and service triggering, application and service layer management, communication management, data management and repository, and device management [314].

Husain et al. in [315] describe how the OneM2M architecture is meant to use the underlying networks services (and more precisely when the underlying network is a 3GPP mobile one). Three services mainly can be provided by underlying networks through the network service entities (NSE): triggering, discovery, and management. One of the standardized infrastructures is the 3GPP one. Mainly an AE in the field domain has to have an IP connection with the AE in the infrastructure domain to establish a connection and performs one of the four operations: Create, Retrieve, Update, Notify, and Delete. This IP connectivity can be served by the 3GPP MTC network. The ASN in the field domain is similar to a user equipment in the user plane and the infrastructure node is similar to an SCS in the control plane. The MTC architecture presents some services that can overlap with those provided by OneM2M. Therefore, it is necessary to do the mapping between these services and one of them is the identification one. The used identifiers in the MTC case are the external ID (M2M-Ext-ID or MSISDN) and the Trigger-Recipient-ID of the target CSE.

The work done in [316] aims at integrating the lightweight management protocol (LWOMA) into the OneM2M architecture. The identity management and the object registration are two key parts in any IoT management scheme. Mostly, the authors approach IoT from a web-based perspective, using unique resource identifiers (URI) for identifying the things. Additionally, they extend the CoRE (constrained restful environment) capabilities to legacy devices and integrate the proposed scheme into the OneM2M standard architecture. However, URIs used in the web context present some limitations in the IoT case where we have big number of resources.

In [317], there is a proposition of OneM2M based smart city architecture consisting of things as ADN interacting with a gateway presenting an MN that aggregates data and bridge the non-smart things to the infrastructure node deployed in a cloud system. In a smart city domain, multiple gateways are deployed, and they have to be registered to the central smart city central cloud instance. The integration of the M3 data management framework [318] and crowdsourcing use case for smart city is discussed for providing smart services.

The work done in [319] tackles the issue of data interoperability. Most of the standardization efforts focus on one of the two aspects of interoperability: data and communication. The current version of OneM2M does not include the data semantic integration. The idea in this work was to integrate the data ontology concept in the OneM2M architecture.

8.4. IoT-A

The IoT-A architecture consists of seven longitudinal groups: device group, communication group, IoT service group, virtual entity group, IoT business process management group, and application group, and two transversal groups: security group, and management group as shown [320]. Thus, IoT-A provides an abstract architecture model and does not define in detail the main functionalities. This will conduct in different implementations posing interoperability issues.

8.5. IoT6

The IoT6 architecture focuses on three groups of the IoT-A architecture: the communication group, the business process management group, and the security group. In [321], the IoT6 architecture is presented. This architecture consists of six groups: the communication group, the resources and services group, the process automation group, the applications group, the management group, and the security group. This IPv6 based architecture employs the IPv6 inherited benefits (unique addressing, no need for NAT, etc.) and standards (6LowPAN, CoAP, GloWbal). It provides functionalities such as: mobility, multi-protocols interoperability among heterogeneous things, intelligence distribution, cloud computing and mobile phone network integration, ubiquitous access, and management capabilities. This architecture is not detached from previous IoT architectures (IoT-A, FI-WARE, OneM2M, etc.) but it extends them. Focusing on the communication layer, it provides functionalities provided at higher layers in other architectures in a complex way. It complements the existing architectures supporting IPv6 to resolve the IoT identification challenge. This architecture consists of three domains: the IPv6 compliant and non-compliant things (the non-compliant things have to be connected to proxy or gateway) domain, the IPv6 local area network domain, and the IPv6 wide area network domain for connecting different LANs. The discovery service is provided through “digrectories”; these digrectories have multiple interfaces: JSON, DNS, etc. and have to be connected to a digcovery core that applies the ontology principles to overcome the heterogeneity challenge.

The focus on IPv6 as IoT enabler is understandable in the identification context. However, the interoperability between different existent identification schemes adds complexity to the IoT ubiquitous network [322].

8.6. IoTDM

This module was integrated firstly in the Lithium OpenDaylight version. It consists of applying SDN to the OneM2M architecture. Having the data collected and analyzed by a central entity coping with the different access technology heterogeneity is key to enable the OneM2M deployment. This project consists of integrating a OneM2M core in the ODL controller. This core acts as an IoT data broker. The OneM2M core is connected to different devices using different protocols.

Thus, this project shows that OneM2M and SDN are two complementary concepts. In this context, employing SDN & NFV to deploy the OneM2M architecture will accelerate the IoT realization [323].

8.7. Software defined IoT architectures

“Is SDN the De-Constraining Constraint of the Future Internet?” [324]. While the current network technologies are considered revolutionary relative to what preceded, their endurance is limited by the rigidity of the current network infrastructure. In today’s network, the configuration is done through low-level policies configured manually (via CLI). SDN came to hide the management complexity and allow for innovative applications and network services to meet the IoT requirements [325,326].

Omnes et al. in [327] discuss the benefits of employing SDN & NFV in a general IoT architecture. While SDN permits dynamic configuration of the data plane policies and rules, the NFV allows the virtualization of resources lowering CapEx and OpEx. The authors defined main requirements for a general IoT architecture such as QoS guarantee, common service layer, new access network mentality, and big data management.

A restful software defined IoT architecture is proposed in [328]. This architecture consists of several modules: northbound Application Programming Interfaces (APIs), southbound APIs, processor, and database. The southbound interfaces deal with different protocols: HTTP, COAP, etc. The control plane consists of the processor and the database where the nodes state and information are collected. The southbound interface, which interconnects the control and the application planes, is principally REST based.

Describing the usefulness of SDN to enable agility, flexibility, and dynamicity to overcome the today's IT problems, Tadinada in [329] introduces the Freescale SDN products: VortiQa Open Network Director and VortiQa Open Network Switch. Two use cases of SDN OF switches are presented. The first use case is where Open vSwitch acts as an IoT gateway managed by a cloud based SDN controller. The second use case is where an Open vSwitch is mounted on eNodeB to offload data from the Evolved Packet Core (EPC) network, providing better user experience and decreasing OpEx and CapEx. The main functions assigned to the IoT gateway are: forwarding data between end devices, protecting devices from external attacks, providing QoS guarantee, authenticating and authorizing the end devices, transferring data in a secure way between gateways (IPsec/tunneling), and managing access control and queuing. Therefore, the eNodeB Open vSwitch aims to separate the voice from the data packets making the data packets not traversing the EPC network.

In [330], an SDN based architecture for home automation is proposed. Today, a big number of home devices are connected to the Internet. The management of these devices in a traditional way is unpractical and unviable in some cases. The authors propose the Majord'home management platform. In the proposed architecture: CO is the connected object, coCO is the community of connected objects, VO the virtual object, and Avatar is the user representation to manage its VOs. The Internet Service Provider (ISP) plays the role of the Majordomo: a software that allows managing the user's objects (i.e. the client home objects) through virtualization. The Majord'home architecture consists of user manager, VO manager, coCO manager, network manager, and application manager.

Extending the work done in [330], Boussard et al. propose a generalization of the CO, VO, Avatar, coCO, and coVO definitions to any smart environment: A CO now is not just a home device connected to the Internet, it is an entity that can generate, receive or impact the data flow in the network, the VO is an abstract view of this entity, the coCO as before a community of connected objects, the coVO is a community of the virtual objects in other words it is an abstraction of the coCO, and Avatar presents the manager of the CO through VO. The proposed SDN architecture consists of three horizontal layers and one vertical layer. The data layer consists of all NE and COs that can receive and generate data without performing any forwarding/routing functions, the control layer is composed of two sub-levels; level 1 consists of the network controller and the CO controller and level 2 consists of the coVO controller, and on top of these layers resides the application layer. The management layer consists of different managers (network manager, VO manager, application manager), all encompassed in the Operation Support System(OSS). The control, application, and management layers compose the "majordomo". As proof of concept, they tested the proposed architecture with two Majord'homes (Bob and Alice homes). Each one has an Open vSwitch to which the home appliances are connected. A coVO controller, residing at the ISP side, controls the Majord'home gateways. Scalability, auto configuration, and security and privacy issues are to be tackled in future work [331].

In [332], a proposition of an IoT architecture that employs both SDN and distributed data service (DDS) is presented. While SDN is used to guarantee data agility, flexibility, and mobility handling, DDS is introduced for big data management. The publish/subscribe paradigm has shown its usefulness in the Wireless Sensor Network (WSN) case. This data-centric approach makes the data an addressable entity. In the IoT domain, this concept is needed because IoT applications and services rely mostly on the analysis of the collected data. This architecture consists of three domains: the M2M domain where a gateway connects the heterogeneous set of devices, the network domain that includes different access networks (3G, LAN, etc.), and the application domain that includes the IoT applications.

In [333], there is a proposition of a Software Defined Infrastructure (SDI) manager, which consists of two essential components: the cloud computing controller (OpenStack), and the network controller (FlowVisor)). The main roles of the cloud computing controller are the collection of the users' descriptions and the management of the computing resources. On the other hand, the network controller has the role of managing the network resources, collecting network topology information, and interacting with the Open vSwitches to configure their forwarding tables. The FlowVisor layer is added to permit slicing of the network and the attachment of each slice to a certain controller.

The Idea of Network Operating System (NOS) was depicted to hide the heterogeneity in the network domains. NOS allows the deployment of different applications over a set of different network devices. In [334], the authors propose an operating system for IoT extending the ONOS SDN controller to support SDN-WISE, a protocol that extends the SDN capabilities to WSN. SoftINTERNET a new initiative for a future software defined Internet. This architecture aims to provide both connectivity and management in a software defined way coping with the heterogeneity and complexity of the future Internet [335].

The trial to invoke SDN in the IoT domain is challenged by the delay imposed by the communication between switch and controller. A pre-emptive flow installation algorithm is proposed in [336]. In [337], there is a proposition of a software defined solution to overcome the heterogeneity challenge in the IoT networks. This solution consists of having an IoT controller which communicates with the things that have integrated IoT agents permitting them to request communication. These communication requests are collected by the IoT controller which builds a full view of the network and calculates the forwarding rules. These forwarding rules are communicated to the SDN controller which downloads them in the forwarders (switches/routers). This solution builds an overlay network on top of the heterogeneous networks and allows the interworking between them. However, the proposed solution presents some limitations such as the integration of the IoT agents, the routing protocol, the forwarding rules formulation, the identity schemes heterogeneity, and the scalability.

Considering the scalability, management, and security IoT issues, the proposed architecture in [338] consists of three layers: the physical layer, the middleware/control layer, and the data service layer. The physical layer consists of different types of connected devices. The middleware/control layer consists of software defined blocks: Software Defined Security (SDSec), Software Defined Storage (SDStore), Internet of Things Controller (IoT-C), and Software Defined Controller (SDN-C). When the data is received from the network gateway, a data collector process it; authentication is performed by the SDSec component, if the authentication check succeeds the data is tagged by a positive (P) flag (otherwise a flag N). Then, the data is passed to the IoT controller that has the role to compute the path to the destination, the forwarding rules are forwarded to the SDN-C which downloads them into the network switches.

Hu in [339] discusses the IIoT need for traffic engineering. Three phases of management are implemented in a centralized cloud based controller: topology computation, admission control, and allocation optimization. The centralization of management is shown

to have a good impact in terms of packet loss implementing an alternative route mechanism.

Employing the SDN concept, Lee et al. in [340] show that is feasible to obtain interoperability between devices from different manufacturers. Auto configuration and recognition are integrated into the proposed solution. Using the Open vSwitch as a gateway, this architecture ensures a dynamic configuration and management of home networks. The home devices are identified using their unique MAC addresses. The configuration related information is kept in a database connected and managed by the SDN controller. An implementation of this architecture is done using Mininet and OpenDaylight with the home devices as hosts.

Two virtualization levels are defined in [341]: the network level and the end-user level. At the network level, there are two cases. The first case is where physical resources are in the same physical location; in this case, virtualization aims to partition the resources between different logical functions. The second case is where physical entities are at different locations; in this case, two virtualization functions are invoked: moving the logical function (migration) and having the physical resources at different places. Virtualization at the network and the end-user levels calls for specialized functions. The virtual sensor, the virtual cell management, and the software defined controlled wireless networks are presented as use cases that implement these virtualizations functionalities. Thus, SDN coupled with NFV can enable management flexibility in the IoT domain [342].

The work done in [343] presents a Web of Things SDN based architecture. The web technologies, facilitating the development mission, have some limitations in terms of security, things management (rebooting), and the data management. Therefore, putting SDN on top of the resource based Web architecture helps in hiding the security and management complexities. This architecture is composed of three layers: the access layer where the things are connected to WoT gateways, the control layer consisting of the resource databases and the control functions, and the application layer.

8.8. Challenges

Many proposals have been established for conceiving a widely adopted IoT infrastructure. However, the added functions complexities prevent their application. Even though the abstraction layers are promising, as the case of the OneM2M architecture, the techniques to deploy such layers need to be specified. In this context, SDN is a way to re-think the network functions deployment. Softwarization grants the dynamicity and the support of heterogeneity. The deployment of an SDN gateway is the solution to overcome the orthogonal diversity of IoT infrastructures. The reviewed architectures in this section show the benefits of applying SDN in facilitating the management network functions to cope with the high scalability challenge. Proposing a single central control can cope with the management issues. However, the centralization poses new challenges in terms of latency, availability, throughput, etc. Additionally, when we talk about a network with billions of connected things, the data management should be considered as well as the control layer design.

9. Limitations and future research directions

9.1. Limitations

Based on the review presented in this paper, we can list some of the limitations of the current IoT solutions:

Lack of Interoperability: different solutions have been proposed to overcome the different IoT challenges. However, most of them do not consider the existing IoT solutions and this makes the adoption of the new solutions a complicated task. Interoperability between the different IoT solutions (devices, architectures, protocols, etc.) helps in revealing the IoT value in enabling innovative applications. Therefore, in the network domain, adopting new solutions is not a straightforward task. Proposing a pure SDN based solutions per example is not realistic and thus the consideration of the hybrid case is key.

Lack of Realizability: scalability is one of the IoT main challenges. Most of the IoT challenges rise from the high scale of the IoT network which introduces new QoS and security issues. However, the realization of the high scale is not easy both from theoretical and practical perspectives.

Lack of Compatibility: having thousands of published papers in the IoT domain, few of them propose new schemes that can be integrated in the current network infrastructure. However, other proposals are meant to be standalone solutions that repose on new networking schemes.

Lack of Security: security is not an issue that can be treated independently. Security has to be designed and built in each layer of the IoT solutions (from the device layer to the application layer). IoT security is not only about securing the network and data it goes beyond that to attacks which can target the human health or life.

9.2. Recommendations

Based on the presented limitations, we believe that there are important directions that have to be considered in the future IoT research studies:

Build on top of the existing solutions: one of the most important challenges of any new proposed IoT solution is its interoperability with existing solutions. Thus, the future work has to consider the compliance of any new solution with the IoT standards and its interoperability with similar existing IoT platforms.

Consider different challenges when building an IoT solution: building an IoT solution for a specific challenge might result in a partial solution. Thus, it is essential for future work to define the main challenges that have to be considered in any IoT solution.

Real implementation: having plenty of position papers in the IoT domain, there is a need for real implementations that show the effectiveness of the proposed solutions. Additionally, real testbeds need to be implemented to test the correctness and effectiveness of the proposed solutions. Simulators that allow to model and test the different proposed architectures, protocols, and algorithms need to be developed.

Consider data and network related aspects: when IoT data related research focuses on data analysis the network related research focuses on how to connect things to the Internet. However, some applications present critical requirements in terms of network resources; thus, we need to rethink the data networking issue and where data analytics related functions have to be implemented.

Standardization: the interoperability between the different IoT solutions call for well-defined IoT standards. Therefore, the IoT standardization efforts at different levels (communication protocols, architectures, data management, e.g.) need to be correlated. Standards are key not only for compatibility and interoperability aims. Perhaps, the lack of standardization can invoke many security issues.

Actually, the IoT devices are not meant to communicate only with one device (i.e. gateway, switch, router). Instead, the IoT devices will communicate with many other IoT devices and thus standard D2D communication protocols are required. However, the standardization need to cover different IoT aspects and not only the communication one. The IoT devices will generate different types of data and thus interoperability at the data level is essential

to reduce data analysis complexity and enable innovative IoT applications. Besides, new regulations are needed to define the data ownership policies to protect data privacy and security [344].

SDN, NFV, and cloud/edge computing integration: as discussed in this paper, the application of SDN and NFV can alleviate many of the IoT challenges. SDN coupled with NFV provide flexibility and dynamicity that help in overcoming the management complexity, aggravated by the high scalability of the IoT network. Additionally, SDN, enabling the programmability of the network functions, can cope with the IoT heterogeneity challenge. Furthermore, SDN and NFV can help in alleviating main IoT security concerns (e.g. DoS, DDoS, etc.). On the other hand, edge computing coupled with SDN can help in managing the IoT big data. However, the integration of these technologies need special consideration. In addition to the standardization efforts, developing real testbeds of the proposed solutions is key for their real deployment.

IoT involves many parties: IoT devices manufacturers, network services providers, data services providers, and applications developers. The IoT devices manufacturers need to monitor their devices for maintenance and management purposes. Additionally, some IoT devices manufactures provide cloud-based services to store, process, and connect the devices' collected data. In this context, SDN and cloud computing can hide the complexity of IoT devices and data management. Amazon, for example, has developed the Amazon Web Services (AWS) for IoT [345]. The AWS IoT services allow to manage the IoT devices through deployed applications in a cloud environment. In addition, it permits the management and the analysis of the collected data. On the other hand, the network services providers have to guarantee good QoS level and secure communication over their deployed networks. Thus, integrating SDN helps in managing both QoS and security in the highly scalable IoT network. Software based gateways help in overcoming the IoT network management complexity. Cisco, for example, has developed a softwarized IoT gateway integrating Cisco IOx (i.e. Cisco IOS software with fog) to enable flexible IoT networks management and real-time IoT applications [346]. Besides, OpenDaylight has integrated the IoTDM module as a plugin ever since its lithium release. This module permits the connection of the devices, directly or through a gateway, to the SDN controller. In this case, the developed applications on top of the controller are responsible for managing the IoT devices and ensuring QoS and security. Furthermore, data service providers need to consider analyzing data at the network edge. For this aim, for example, Microsoft has developed an IoT framework for implementing data analytics at the network edge [347]. Besides, application developers have to implement intelligence at the application level to get insights from the collected data. As an example, IBM has developed a cognitive system called IBM Watson for IoT data intelligence [348].

As a result, IoT data and network management requires the federation of all the involved parties' efforts to have a global IoT architecture integrating the most recent data and network enabling technologies.

10. Conclusion

The network and telecommunication networks are in continuous evolution. Internet of Things is expected to take advantage of this evolution to be widely deployed. While some IoT applications are already there, its wide realization still encumbered by many challenges such as the high scalability and management complexity, the heterogeneity and interoperability support, the big data handling, and the security and privacy guarantee. These main challenges need new architectural and design based solutions to be handled. In this paper, we presented SDN & NFV, cloud and fog computing, and 5G as the main enablers of the IoT evolution. Many architectural solutions have been conceived in the IoT domain, but no one has gained a global acceptance and adoption. We believe that SDN is a solution that combats the heterogeneity and can serve in unifying the vision of a global IoT architecture. While the work in this domain is still in its early stages, we presented the most recent work applying SDN & NFV in an SDN based IoT architecture.

Acknowledgements

Research funded by the AUB University Research Board, the Lebanese National Council for Scientific Research, and TELUS Corp., Canada.

References

[1] K. Ashton, That 'internet of things' thing, RFiD J. 22 (7) (Jul. 2009) 97–114.
[2] M. Walport, The Internet of Things: making the most of the second digital revolution a report by the UK Government Chief Scientific Adviser, 2014. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.
[3] S. DuBravac, The Internet of Things: evolution or revolution?, 2015. Available online at: http://www.biztositasiszemle.hu/files/201506/aig_white_paper_iot_english_tcm2538-677834.pdf.
[4] D. Evans, The Internet of Things: how the next evolution of the internet is changing everything, CISCO White Paper 1 (2011) 14.
[5] https://en.wikipedia.org/wiki/Metcalfe%27s_law.
[6] R. Want, S. Dustdar, Activating the Internet of Things [Guest editors' introduction], Computer 48 (9) (Sept. 2015) 16–20.
[7] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, D. Aharon, The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute, 2015.
[8] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, A. Marrs, Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy, 12, McKinsey Global Institute, San Francisco, CA, May 2013.
[9] A. Taivalsaari, T. Mikkonen, Cloud technologies for the internet of things: defining a research agenda beyond the expected topics, in: 2015 41st Euromicro Conference on Software Engineering and Advanced Applications, Funchal, Madeira, Portugal, 2015, pp. 484–488.
[10] F. Graur, Dynamic network configuration in the Internet of Things, in: 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, 2017, pp. 1–4.
[11] Developing Solutions for IoT. Intel White Paper, 2014.
[12] B. Edson, Get Started with the Internet of Things in Your Organization. Introducing the Microsoft Azure Internet of Things Suite, Microsoft Corp, 2015.
[13] Libelium - Connecting Sensors to the Cloud. [Online]. Available: http://www.libelium.com/. [Accessed: November 2017].
[14] OpenMTC. [Online]. Available: http://www.openmtc.org/index.html#openmtc. [Accessed: November 2017].
[15] Internet of Things (IoT) - Cisco. [Online]. Available: http://www.cisco.com/c/en/us/solutions/internet-of-things/iot-products/solutions.html. [Accessed: November 2017].
[16] Hewlett Packard Enterprise (HPE). [Online]. Available: https://www.hpe.com/us/en/home.html. (Accessed: November 2017).
[17] Internet of Things | Dell United States. [Online]. Available: http://www.dell.com/en-us/work/learn/internet-of-things-solutions. [Accessed: November 2017].
[18] Internet of Things (IoT) Solutions and Services | AT&T Business. [Online]. Available: https://www.business.att.com/enterprise/Portfolio/internet-of-things/. [Accessed: November 2017].
[19] IoT - InterDigital. [Online]. Available: http://www.interdigital.com/iot/. [Accessed: November 2017].
[20] IBM Watson Internet of Things (IoT). [Online]. Available: http://www.ibm.com/internet-of-things/. [Accessed: November 2017].
[21] D. Zeng, S. Guo, Z. Cheng, The web of things: a survey, J. Commun. 6 (Jan. (6)) (2011) 424–438.
[22] K.S. Lee, M. Bae, H. Kim, Future of IoT networks: a survey, Appl. Sci. 7 (10) (2017).
[23] O.B. Sezer, E. Dogdu, A.M. Ozbayoglu, Context aware computing, learning and big data in Internet of Things: a survey, IEEE Internet Things J. PP (99) (2018) 1–27.
[24] U. Deniz Ulusar, F. Al-Turjman, G. Celik, An overview of Internet of things and wireless communications, in: 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, 2017, pp. 506–509.
[25] M. Alaa, A.A. Zaidan, B.B. Zaidan, M. Talal, M.L.M. Kiah, A review of smart home applications based on Internet of Things, J. Netw. Comput. Appl. 97 (Supplement C) (November 2017) 48–65.
[26] S. Li, L. Da Xu, S. Zhao, The internet of things: a survey, Inf. Syst. Front. 17 (2) (Oct. 2010) 243–259.
[27] J. Latvakoski, A. Iivari, P. Vitic, B. Jubeh, M.B. Alaya, T. Monteil, Y. Lopez, G. Talavera, J. Gonzalez, N. Granqvist, A survey on M2M service networks, Computers 3 (4) (Nov. 2014) 130–173.

[28] E. Borgia, The Internet of Things vision: key features, applications and open issues, Comput. Commun. 54 (Dec. 2014) 1–31.
[29] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Networks 54 (15) (Oct. 2010) 2787–2805.
[30] H.B. Pandya, T.A. Champaneria, Internet of things: survey and case studies, in: Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, AP, India, 2015, pp. 1–6.
[31] S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, A vision of IoT: applications, challenges, and opportunities with china perspective, Internet Things J., IEEE 1 (4) (Aug. 2014) 349–359.
[32] P. Gaur, M.P. Tahiliani, Operating systems for IoT devices: a critical survey, in: Region 10 Symposium (TENSYMP), Sanur, Bali island, Indonesia, 2016, pp. 33–36.
[33] M. Razzaque, M. Milojevic-Jevric, A. Palade, S. Clarke, Middleware for Internet of Things: a Survey, IEEE Internet Things J. 3 (1) (Feb. 2016) 70–95.
[34] I. Yaqoob, E. Ahmed, I.A.T. Hashem, A.I.A. Ahmed, A. Gani, M. Imran, M. Guizani, Internet of Things architecture: recent advances, taxonomy, requirements, and open challenges, IEEE Wirel. Commun. 24 (3) (2017) 10–16.
[35] G. GardaŠević, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović, M. Radonjić, The IoT architectural framework, design issues and application domains, Wirel. Pers. Commun. 92 (1) (2017) 127–148 01/01.
[36] I. Mashal, O. Alsaryrah, T. Chung, C. Yang, W. Kuo, D.P. Agrawal, Choices for interaction with things on Internet and underlying issues, Ad Hoc Networks 28 (May 2015) 68–90.
[37] H. Derhamy, J. Eliasson, J. Delsing, P. Priller, A survey of commercial frameworks for the Internet of Things, in: 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 2015, pp. 1–8.
[38] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things security and forensics: challenges and opportunities, Future Gener. Comput. Syst. 78 (Part 2) (January 2018) 544–546.
[39] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: a survey, J. Netw. Comput. Appl. 88 (Supplement C) (June 2017) 10–28.
[40] J. Granjal, E. Monteiro, J. Silva, Security for the Internet of Things: a survey of existing protocols and open research issues, IEEE Commun. Surv Tutorials 17 (3) (Jan. 2015) 1294–1312.
[41] J. Pescatore, Securing the Internet of Things Survey, SANS Institute, Jan. 2014.
[42] D. Christin, A. Reinhardt, P.S. Mogre, R. Steinmetz, Wireless sensor networks and the internet of things: Selected challenges, in: Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze, Hamburg, Germany, 2009, pp. 31–34.
[43] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Networks 76 (Jan. 2015) 146–164.
[44] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, Commun. Surv. Tutorials, IEEE 17 (4) (Nov. 2015) 2347–2376.
[45] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, Commun. Surv. Tutorials, IEEE 15 (3) (Jul. 2013) 1389–1406.
[46] A. Rajandekar, B. Sikdar, A survey of MAC layer issues and protocols for machine-to-machine communications, Internet Things J., IEEE 2 (2) (Apr. 2015) 175–186.
[47] T. Salman, R. Jain, A survey of protocols and standards for Internet of Things, Adv. Comput. Commun. 1 (1) (March 2017).
[48] I. Ishaq, D. Carels, G.K. Teklemariam, J. Hoebeke, F.V.D. Abeele, E.D. Poorter, I. Moerman, P. Demeester, IETF standardization in the field of the internet of things (IoT): a survey, J. Sens. Actuator Networks 2 (2) (Apr. 2013) 235–287.
[49] S. Bera, S. Misra, A.V. Vasilakos, Software-defined networking for Internet of Things: a survey, IEEE Internet Things J. 4 (6) (Dec. 2017) 1994–2008.
[50] S.K. Tayyaba, M.A. Shah, O.A. Khan and A.W. Ahmed, "Software Defined Network (SDN) based Internet of Things (IoT): a road ahead," pp. 15:1–15:8, 2017.
[51] N. Bizanis, F.A. Kuipers, SDN and Virtualization solutions for the Internet of Things: a survey, IEEE Access 4 (2016) 5591–5606.
[52] M. Nitti, V. Pilloni, G. Colistra, L. Atzori, The virtual object as a major element of the Internet of Things: a survey, EEE Commun. Surv. Tutorials 18 (2) (2015) 1228–1240.
[53] N.A. Jagadeesan, B. Krishnamachari, Software-defined networking paradigms in wireless networks: a survey, ACM Comput. Surv. (CSUR) 47 (2) (Jan. 2015) 27.
[54] K. Sood, S. Yu, Y. Xiang, Software defined wireless networking opportunities and challenges for Internet of Things: a review, IEEE Internet Things J. 3 (4) (Aug. 2016) 453–463.
[55] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (Sept. 2013) 1645–1660.
[56] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing, J. Netw. Comput. Appl. 67 (May 2016) 99–117.
[57] L. Atzori, A. Iera, G. Morabito, Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm, Ad Hoc Networks 56 (Supplement C) (March 2017) 122–140.
[58] M. Roberto, A. Biru, D. Rotondi, Towards a definition of the Internet of Things (IoT), IEEE Internet Initiative, May 2015.
[59] "Overview of the Internet of Things." ITU, June 15, 2012. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060.
[60] G.M. Lee, J. Park, N. Kong, N. Crespi, The Internet of Things–Concept and Problem Statement, Internet Research Task Force, July 2011.
[61] Cisco Systems, "What is the Internet of Everything?", http://internetofeverything.cisco.com/vas-public-sector-infographic/.
[62] Cisco Systems, The Internet of Everything, Global Private Sector Economic Analysis, 2013. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf.
[63] I. Bojanova, G. Hurlburt, J. Voas, Imagineering an internet of anything, Computer (6) (Jun. 2014) 72–77.
[64] "Internet of Things (IOT) /M2M". Study paper. http://tec.gov.in/pdf/Studypaper/IOT_M2M_Study_Paper.pdf.
[65] ETSI TS 102 689 V1.2.1 (2013-06) Machine-to-Machine communications (M2M); M2M service requirements, 2013.
[66] M. Alam, R.H. Nielsen, N.R. Prasad, The evolution of M2M into IoT, in: Communications and Networking (BlackSeaCom), 2013 First International Black Sea Conference on, Batumi, Georgia, Jul. 2013, pp. 112–115.
[67] P. Goncalves, J. Ferreira, P. Pedreiras, D. Corujo, Adapting SDN datacenters to support Cloud IIoT applications, in: 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxemburg, Sep. 2015, pp. 1–4.
[68] P.C. Evans, M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, GE White Paper, Nov. 2012.
[69] A. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, in: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, Jun. 2015, p. 54.
[70] Industrial Internet Consortium. [Online]. Avialable: http://www.iiconsortium.org/. [Accessed: November 2017].
[71] D. Dujovne, T. Watteyne, X. Vilajosana, P. Thubert, 6TiSCH: deterministic IP-enabled industrial internet (of things), Commun. Mag., IEEE 52 (12) (Dec. 2014) 36–41.
[72] E. Fleisch, "What is the Internet of Things? – An Economic Perspective", Auto-ID Labs White Paper WP-BIZAPP-053, Jan. 2010.
[73] A. Iera, G. Morabito, L. Atzori, The social Internet of Things, in: Cloud Engineering (IC2E), 2015 IEEE International Conference on, Tempe, AZ, USA, Mar. 2015, p. 1.
[74] Y. Kim, Y. Lee, Automatic generation of social relationships between Internet of Things in smart home using SDN-based home cloud, in: Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on, Gwangiu, South Korea, Mar. 2015, pp. 662–667.
[75] L. Atzori, A. Iera, G. Morabito, From "smart objects" to "social objects": The next evolutionary step of the internet of things, Commun. Mag., IEEE 52 (1) (Jan. 2014) 97–105.
[76] *Standardized Machine-to-Machine (M2M) Software Development Platform. (PG: PLS. set in roman)*, Interdigital White Paper, Oct. 2012.
[77] A.M. Alberti, D. Singh, Internet of Things: perspectives, challenges and opportunities, in: *Proceeding of: International Workshop on Telecommunications (IWT 2013)*, Santa Rita do Sapucaí, Minas Gerais, Brazil, 2013, pp. 1–6.
[78] M.H. Miraz, M. Ali, P.S. Excell, R. Picking, A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT), in: Internet Technologies and Applications (ITA), Wrexham, North Wales, UK, 2015, pp. 219–224.
[79] N. Feamster, J. Rexford, E. Zegura, The road to SDN: an intellectual history of programmable networks, ACM SIGCOMM Comput. Commun. Rev. 44 (2) (Apr. 2014) 87–98.
[80] RFC 7426. https://tools.ietf.org/html/rfc7426.
[81] L. Zuccaro, F. Cimorelli, F.D. Priscoli, C.G. Giorgi, S. Monaco, V. Suraci, Distributed control in virtualized networks, Proc. Comput. Sci. 56 (Dec. 2015) 276–283.
[82] M. Bouet, K. Phemius, J. Leguay, Distributed SDN for mission-critical networks, in: 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 2014, pp. 942–948.
[83] K. Phemius, M. Bouet, J. Leguay, Disco: distributed multi-domain sdn controllers, in: 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 2014, pp. 1–4.
[84] T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, S. Shenker, Onix: a distributed control platform for large-scale production networks, OSDI 10 (Oct. 2010) 1–6.
[85] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, G. Parulkar, ONOS: towards an open, distributed SDN OS, in: Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, Chicago, IL, USA, Aug. 2014, pp. 1–6.
[86] J. Medved, A. Tkacik, R. Varga, K. Gray, OpenDaylight: towards a model-driven SDN controller architecture, in: A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on, Sydney, Australia, Jun. 2014, pp. 1–6.
[87] M. Jarschel, T. Zinner, T. Hossfeld, P. Tran-Gia, W. Kellerer, Interfaces, attributes, and use cases: a compass for SDN, IEEE Commun. Mag. 52 (6) (June 2014) 210–217.
[88] F. Wang, H. Wang, B. Lei, W. Ma, A research on high-performance SDN controller, in: Cloud Computing and Big Data (CCBD), 2014 International Conference on, Huangshan, Anhui, China, 2014, pp. 168–174.
[89] H. Sandor, B. Genge, G. Sebestyen-Pal, Resilience in the internet of things: the software defined networking approach, in: Intelligent Computer Communication and Processing (ICCP), 2015 IEEE International Conference on, Cluj–Napoca, Romania, 2015, pp. 545–552.
[90] J. Rak, Resilience of future internet communications, in: Resilient Routing in Communication Networks, Springer International Publishing, 2015, pp. 45–83.

[91] Time for an SDN Sequel? Scott Shenker Preaches SDN Version 2. [Online]. Available: https://www.sdxcentral.com/articles/news/scott-shenker-preaches-revised-sdnsdnv2/2014/10/. [Accessed: Novmeber 2017].

[92] M. Ahmad, J.S. Alowibdi, M.U. Ilyas, vIoT: a first step towards a shared, multi--tenant IoT Infrastructure architecture, in: 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, 2017, pp. 308–313.

[93] I. Miladinovic, S. Schefer-Wenzl, A highly scalable iot architecture through network function virtualization, Open J. Internet Things (OJIOT) 3 (1) (2017) 127–135.

[94] Why elastic scalability matters in network functions virtualization, Feb 24, 2015. By Martin Taylor https://www.metaswitch.com/blog/why-elastic-scalability-matters-in-network-functions-virtualization Available Accessed: May 2018.

[95] Microsoft Azure Cloud Computing Platform & Services. [Online]. Available: https://azure.microsoft.com/en-us/. [Accessed: May 2018].

[96] Google Cloud Computing, Hosting Services & APIs | Google Cloud. [Online]. Available: https://cloud.google.com/. [Accessed: May 2018].

[97] iCloud. [Online]. Available: https://www.icloud.com. [Accessed: May 2018].

[98] S.M. Babu, A.J. Lakshmi, B.T. Rao, A study on cloud based Internet of Things: CloudIoT, in: Communication Technologies (GCCT), 2015 Global Conference on, Thuckalay, Kanya Kumari District, India, 2015, pp. 60–65.

[99] S. Distefano, G. Merlino and A. Puliafito, "Sensing and actuation as a service: a new development for Clouds," *Network Computing and Applications (NCA), 2012 11th IEEE International Symposium on*, pp. 272–275.

[100] S. Distefano, G. Merlino, A. Puliafito, A utility paradigm for IoT: the sensing Cloud, Pervasive Mob. Comput. 20 (Jul. 2015) 127–144.

[101] X. Sheng, J. Tang, X. Xiao, G. Xue, Sensing as a service: challenges, solutions and future directions, IEEE Sens. J. 13 (10) (2013) 3733–3741.

[102] BETaaS – Community. [Online]. http://www.betaas.com/. [Accessed: November 2017].

[103] A. Botta, W. de Donato, V. Persico, A. Pescapé, On the integration of Cloud Computing and Internet of Things, in: Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, Barcelona, Spain, 2014, pp. 23–30.

[104] A.R. Biswas, R. Giaffreda, IoT and cloud convergence: opportunities and challenges, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, Seoul, Korea (South), 2014, pp. 375–376.

[105] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero, M. Nemirovsky, Key ingredients in an IoT recipe: fog computing, cloud computing, and more fog computing, in: 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, Greece, 2014, pp. 325–329.

[106] G.I. Klas, "Edge Cloud to Cloud Integration for IoT," 2016.

[107] A. Noronha, R. Moriarty, K. Connell, N. Villa, Attaining IoT value: how to move from connecting things to capturing insights: gain an edge by taking analytics to the edge, Cisco Anal. Brief (2014).

[108] J. Pan, J. McElhannon, Future edge cloud and edge computing for Internet of Things applications, IEEE Internet Things J. PP (99) (2018) 1–27.

[109] E. Ahmed, A. Ahmed, I. Yaqoob, J. Shuja, A. Gani, M. Imran, M. Shoaib, Bringing computation closer toward the user network: is edge computing the solution? IEEE Commun. Mag. 55 (11) (November 2017) 138–144.

[110] S.K. Sharma, X. Wang, Live data analytics with collaborative edge and cloud processing in wireless IoT networks, IEEE Access 5 (2017) 4621–4635.

[111] M. Satyanarayanan, The emergence of edge computing, Computer 50 (1) (Jan. 2017) 30–39.

[112] A.C. Baktir, A. Ozgovde, C. Ersoy, How can edge computing benefit from software-defined networking: a survey, use cases, and future directions, IEEE Commun. Surv. Tutorials 19 (4) (2017) 2359–2391, Fourthquarter.

[113] G.I. Klas, Fog Computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium, ETSI MEC and Cloudlets, 2015. http://yucianga.info/wp-content/uploads/2015/11/15_11_22-_Fog_computing_and_mobile_edge_cloud_gain_momentum_Open_Fog_Consortium-ETSI_MEC-Cloudlets_v1_1.pdf.

[114] P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on fog computing: architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (Supplement C) (November 2017) 27–42.

[115] E.M. Tordera, X. Masip-Bruin, J. Garcia-Alminana, A. Jukan, G. Ren, J. Zhu and J. Farre, "What is a Fog Node A Tutorial on Current Concepts towards a Common Definition," arXiv preprint arXiv:1611.09193, 2016.

[116] I. Stojmenovic, Fog computing: a cloud to the ground support for smart things and machine-to-machine networks, in: Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian, Melbourne, Australia, 2014, pp. 117–122.

[117] E. Marín-Tordera, X. Masip-Bruin, J. García-Almiñana, A. Jukan, G. Ren, J. Zhu, Do we all really know what a fog node is? Current trends towards an open definition, Comput. Commun. 109 (Supplement C) (September 2017) 117–130.

[118] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 2012, pp. 13–16.

[119] L.M. Vaquero, L. Rodero-Merino, Finding your way in the fog: towards a comprehensive definition of fog computing, ACM SIGCOMM Comput. Commun. Rev. 44 (5) (Oct. 2014) 27–32.

[120] S. Yang, "IoT Stream Processing and Analytics in The Fog," arXiv preprint arXiv:1705.05988, 2017.

[121] A.V. Dastjerdi, R. Buyya, Fog Computing: helping the Internet of Things realize its potential, Computer 49 (8) (Aug. 2016) 112–116.

[122] M. Chiang, "Fog Networking: An Overview on Research Opportunities," arXiv preprint arXiv:1601.00835, 2016.

[123] T.H. Luan, L. Gao, Z. Li, Y. Xiang and L. Sun, "Fog Computing: Focusing on Mobile Users at the Edge," arXiv preprint arXiv:1502.01815, 2015.

[124] Y. Liu, J.E. Fieldsend, G. Min, A framework of fog computing: architecture, challenges, and optimization, IEEE Access 5 (2017) 25445–25454.

[125] M. Satyanarayanan, Z. Chen, K. Ha, W. Hu, W. Richter, P. Pillai, Cloudlets: at the leading edge of mobile-cloud convergence, in: Mobile Computing, Applications and Services (MobiCASE), 2014 6th International Conference on, Austin, Texas, United States, 2014, pp. 1–9.

[126] M. Oppitz, P. Tomsu, Fog Computing, in: Inventing the Cloud Century, Springer, 2018, pp. 471–486.

[127] F.A. Kraemer, A.E. Braten, N. Tamkittikhun, D. Palma, Fog computing in healthcare–a review and discussion, IEEE Access 5 (2017) 9206–9222.

[128] S. Yu, M. Liu, W. Dou, X. Liu, S. Zhou, Networking for big data: a survey, IEEE Commun. Surv. Tutorials 19 (Firstquarter (1)) (2017) 531–549.

[129] Y. Sahni, J. Cao, S. Zhang, L. Yang, Edge mesh: a new paradigm to enable distributed intelligence in Internet of Things, in *IEEE Access* 5 (2017) 16441–16458.

[130] M. Abdelshkour, IoT, from Cloud to Fog Computing, March 2015. http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing.

[131] J. Ni, K. Zhang, X. Lin and X. Shen, "Securing fog computing for Internet of Things applications: challenges and solutions," in *IEEE Commun. Surv. Tutorials*, vol. PP, no. 99, pp. 1.

[132] R. Mahmud, R. Kotagiri, R. Buyya, in: Fog Computing: A Taxonomy, Survey and Future Directions, Internet of Everything, 2018, pp. 103–130.

[133] S. Yi, C. Li, Q. Li, A survey of fog computing: concepts, applications and issues, in: Proceedings of the 2015 Workshop on Mobile Big Data, Hangzhou, China, 2015, pp. 37–42.

[134] M. Patel, B. Naughton, C. Chan, N. Sprecher, S. Abeta, A. Neal, Mobile-Edge Computing Introductory Technical White Paper, White Paper, Mobile-edge Computing (MEC) industry initiative, September 2014.

[135] B.P. Rimal, D. Pham Van, M. Maier, Mobile-edge computing versus centralized cloud computing over a converged FiWi access network, IEEE Trans. Network Serv. Manage. 14 (3) (Sept. 2017) 498–513.

[136] 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.

[137] Y. Mao, C. You, J. Zhang, K. Huang, K.B. Letaief, A survey on mobile edge computing: the communication perspective, IEEE Commun. Surv. Tutorials 19 (4) (Fourthquarter 2017) 2322–2358.

[138] X. Sun and N. Ansari, "Mobile Edge Computing Empowers Internet of Things," arXiv preprint arXiv:1709.00462, 2017.

[139] G.A. Lewis, Mobile computing at the edge (keynote), in: Proceedings of the 1st International Conference on Mobile Software Engineering and Systems, Hyderabad, India, 2014, pp. 69–70.

[140] S. Shahzadi, M. Iqbal, T. Dagiuklas, Z.U. Qayyum, Multi-access edge computing: open issues, challenges and future perspectives, J. Cloud Comput. 6 (1) (2017) 30 12/21.

[141] E. Ahmed, M.H. Rehmani, Mobile edge computing: opportunities, solutions, and challenges, Future Gener. Comput. Syst. 70 (Supplement C) (May 2017) 59–63.

[142] P. Mach, Z. Becvar, Mobile edge computing: a survey on architecture and computation offloading, IEEE Commun. Surv. Tutorials 19 (thirdquarter (3)) (2017) 1628–1656.

[143] S. Ranadheera, S. Maghsudi and E. Hossain, "Mobile edge computation offloading using game theory and reinforcement learning," arXiv preprint arXiv:1711.09012, 2017.

[144] T. Taleb, A. Ksentini, Follow me cloud: interworking federated clouds and distributed mobile networks, IEEE Network 27 (5) (Sep. 2013) 12–19.

[145] S. Wang, K. Chan, R. Urgaonkar, T. He, K.K. Leung, Emulation-based study of dynamic service placement in mobile micro-clouds, in: Military Communications Conference, MILCOM 2015–2015 IEEE, Tampa, FL, USA, 2015, pp. 1046–1051.

[146] M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, The case for VM-based cloudlets in mobile computing, IEEE Pervasive Comput. 8 (4) (Oct. 2009) 14–23.

[147] S. Wang, R. Urgaonkar, M. Zafer, T. He, K. Chan, K.K. Leung, Dynamic service migration in mobile edge-clouds, in: IFIP Networking Conference (IFIP Networking), Toulouse, France, 2015, pp. 1–9.

[148] K. Ha, M. Satyanarayanan, OpenStack for Cloudlet Deployment, School of Computer Science Carnegie Mellon University Pittsburgh, 2015.

[149] S. Keshav, Why cell phones will dominate the future internet, ACM SIGCOMM Comput. Commun. Rev. 35 (2) (Apr. 2005) 83–86.

[150] D. Soldani, A. Manzalini, Horizon 2020 and beyond: on the 5G operating system for a true digital society, Veh. Technol. Mag., IEEE 10 (1) (Mar. 2015) 32–42.

[151] E.T. Dresden, N. Vodafone, A Choice of Future m2m Access Technologies for Mobile Network Operators, Cellular IoT White Paper, 2014.

[152] T. Maksymyuk, S. Dumych, M. Brych, D. Satria, M. Jo, An IoT based monitoring framework for software defined 5G mobile networks, in: Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication, 2017, p. 105.

[153] A. Gudipati, D. Perry, L.E. Li, S. Katti, SoftRAN: software defined radio access network, in: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, Hong Kong, China, 2013, pp. 25–30.

[154] G. Hampel, M. Steiner, T. Bu, Applying software-defined networking to the telecom domain, in: Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on, Turin, Italy, 2013, pp. 133–138.

[155] J. Costa-Requena, J. Llorente Santos, V. Ferrer Guasch, K. Ahokas, G. Premsankar, S. Luukkainen, I. Ahmad, M. Liyanage, M. Ylianttila, O. Lopez Perez, SDN and NFV integration in generalized mobile network architecture, in: Networks and Communications (EuCNC), 2015 European Conference on, Paris, France, 2015, pp. 154–158.

[156] X. Jin, L.E. Li, L. Vanbever, J. Rexford, Softcell: scalable and flexible cellular core network architecture, in: Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, Santa Barbara, CA, USA, 2013, pp. 163–174.

[157] I.F. Akyildiz, P. Wang, S. Lin, SoftAir: a software defined networking architecture for 5G wireless systems, Comput. Networks 85 (Jul. 2015) 1–18.

[158] H. Wang, S. Chen, H. Xu, M. Ai, Y. Shi, SoftNet: a software defined decentralized mobile network architecture toward 5G, IEEE Network 29 (2) (Mar. 2015) 16–22.

[159] M. Bansal, J. Mehlman, S. Katti, P. Levis, Openradio: a programmable wireless dataplane, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 2012, pp. 109–114.

[160] K. Pentikousis, Y. Wang, W. Hu, Mobileflow: toward software-defined mobile networks, IEEE Commun. Mag. 51 (7) (Jul. 2013) 44–53.

[161] Li, Xin Jin1 Li Erran, L. Vanbever and J. Rexford, "Cellsdn: Software-defined cellular core networks," 2013.

[162] Z. Han, W. Ren, A novel wireless sensor networks structure based on the SDN, Int. J. Distrib. Sens. Netw. (2014).

[163] J. Schulz-Zander, C. Mayer, B. Ciobotaru, S. Schmid, A. Feldmann, OpenSDWN: programmatic control over home and enterprise WiFi, in: Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research, Santa Clara, CA, USA, 2015, p. 16.

[164] T. Luo, H. Tan, T.Q. Quek, Sensor OpenFlow: enabling software-defined wireless sensor networks, Commun. Lett., IEEE 16 (11) (Nov. 2016) 1896–1899.

[165] S. Costanzo, L. Galluccio, G. Morabito, S. Palazzo, Software defined wireless networks: unbridling sdns, in: 2012 European Workshop on Software Defined Networking, Darmstadt, Germany, 2012, pp. 1–6.

[166] A. Mahmud, R. Rahmani, Exploitation of OpenFlow in wireless sensor networks, in: Computer Science and Network Technology (ICCSNT), 2011 International Conference on, 1, Dec. 2011, pp. 594–600.

[167] B. Trevizan de Oliveira, C. Borges Margi, L. Batista Gabriel, TinySDN: enabling multiple controllers for software-defined wireless sensor networks, EEE Lat. Am. Trans. 13 (11) (Nov. 2015) 1–6.

[168] S. Shen, M. Carugi, An evolutionary way to standardize the Internet of Things, J. ICT 2 (2014) 87–108.

[169] A. Aijaz, Cognitive machine-to-machine communications for Internet-of-Things: a protocol stack perspective, Internet Things J., IEEE 2 (2) (Apr. 2015) 103–112.

[170] J. Nieminen, C. Gomez, M. Isomaki, T. Savolainen, B. Patil, Z. Shelby, M. Xi, J. Oller, Networking solutions for connecting bluetooth low energy enabled machines to the internet of things, Network, IEEE 28 (6) (Nov. 2014) 83–90.

[171] W. Stallings, Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud, Addison-Wesley Professional, 2015.

[172] C. Kolias, A. Stavrou, J. Voas, Securely Making "Things" Right, Computer 48 (9) (Sep. 2015) 84–88.

[173] M.A. Jan, P. Nanda, X. He, Z. Tan, R.P. Liu, A robust authentication scheme for observing resources in the internet of things environment, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, China, 2014, pp. 205–211.

[174] M. Abomhara, G.M. Koien, Security and privacy in the Internet of Things: current status and open issues, in: Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, Aalborg, Denmark, 2014, pp. 1–8.

[175] H. Zhang, How to disinfect and secure the Internet of Things, Network Secur. 2016 (9) (September 2016) 18–20.

[176] Y. Lee, W. Lee, G. Shin and K. Kim, "Assessing the Impact of DoS attacks on IoT Gateway, Advanced Multimedia and Ubiquitous Engineering. MUE 2017, FutureTech 2017, Lect. Notes Electr. Eng., vol 448.", pp. 252–257.

[177] D. Barrera, I. Molloy and H. Huang, "IDIoT: securing the Internet of Things like it's 1994," arXiv preprint arXiv:1712.03623, 2017.

[178] Identifier Survey - DG - Identities of Things - Kantara Initiative. [Online]. Available: https://kantarainitiative.org/confluence/display/IDoT/Identifier+Survey. [Accessed: November 2017].

[179] V.G. Cerf, Secure identities, Internet Comput., IEEE 15 (4) (Jul. 2011) 96.

[180] J.Y. Lee, W.C. Lin, Y.H. Huang, A lightweight authentication protocol for Internet of Things, in: Next-Generation Electronics (ISNE), 2014 International Symposium on, Kwei-Shan Tao-Yuan, Taiwan, 2014, pp. 1–2.

[181] An Overview of ZigBee Networks A guide for implementers and security testers. [Online]. Available: https://www.mwrinfosecurity.com/system/assets/849/original/mwri-zigbee-overview-finalv2.pdf. [Accessed:: November 2017].

[182] Chapter 7: Naming & Addressing. [Online]. Available: http://hscc.cs.nthu.edu.tw/~sheujp/lecture_note/sensys-ch7-naming_09.pdf. [Accessed: November 2017].

[183] C. Tseng, S. Chen, Y. Yang, L. Chou, C. Shieh, S. Huang, IPv6 operations and deployment scenarios over SDN, in: Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific, Taiwan, National Chiao Tung University, 2014, pp. 1–6.

[184] A.J. Jara, L. Ladid, A. Skarmeta, The Internet of everything through IPv6: an analysis of challenges, solutions and opportunities, J. Wirel. Mob. Netw. Ubiq. Comput. Dependable Appl. 4 (Sep. 2013) 97–118.

[185] Zhi-Kai Zhang, M.C.Y. Cho, Zong-Yu Wu, S.W. Shieh, Identifying and authenticating IoT objects in a natural context, Computer 48 (8) (Aug. 2015) 81–83.

[186] D. van Thuan, P. Butkus and D. van Thanh, "A user centric identity management for Internet of Things," In *IT Convergence and Security (ICITCS), 2014 International Conference on*, Beijing, China, pp. 1–4.

[187] I. Friese, J. Heuer, N. Kong, Challenges from the Identities of Things, 2014 Discussion group within Kantara Initiative.

[188] The Identity of Things (IDoT): Access Management (IAM) Reference Architecture for the Internet of Things (IoT), Forgerock White Paper, 2015. https://www.forgerock.com/app/uploads/2015/05/fr_whitepaper-idot-letter.pdf.

[189] H. Kim, A. Wasicek, B. Mehne, E.A. Lee, A secure network architecture for the internet of things based on local authorization entities, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, 2016, pp. 114–122.

[190] M. Turkanović, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Networks 20 (Sep. 2014) 96–112.

[191] A. Park, H. Kim, J. Lim, A framework of device authentication management in IoT environments, in: IT Convergence and Security (ICITCS), 2015 5th International Conference on, Kuala Lumpur, Malaysia, 2015, pp. 1–3.

[192] O.O. Bamasag, K. Youcef-Toumi, Towards continuous authentication in internet of things based on secret sharing scheme, in: Proceedings of the WESS'15: Workshop on Embedded Systems Security, Amsterdam, Netherlands, 2015, p. 1.

[193] F. Chu, R. Zhang, R. Ni, W. Dai, An improved identity authentication scheme for internet of things in heterogeneous networking environments, in: 2013 16th International Conference on Network-Based Information Systems, Gwangju, Korea, 2013, pp. 589–593.

[194] S. Kalra, S.K. Sood, Secure authentication scheme for IoT and cloud servers, Pervasive Mob. Comput. 24 (Dec. 2015) 210–223.

[195] D. He, S. Zeadally, An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography, Internet Things J., IEEE 2 (1) (Feb. 2015) 72–83.

[196] M. Farash, Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography, J. Supercomput. 70 (2) (Nov. 2014) 987–1001.

[197] Z. Zhao, A secure RFID authentication protocol for health care environments using elliptic curve cryptosystem, J. Med. Syst. 38 (5) (May 2014) 1–7.

[198] Z. Zhangand, Q. Qi, An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography, J. Med. Syst. 38 (5) (May 2014) 1–7.

[199] J. Lee, W. Lin, Y. Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics (ISNE), Kwei-Shan Tao-Yuan, Taiwan, 2014, pp. 1–2.

[200] R. Aggarwal, M.L. Das, RFID security in the context of internet of things, in: Proceedings of the First International Conference on Security of Internet of Things, Kollam, India, 2012, pp. 51–56.

[201] V. Shivraj, M. Rajan, M. Singh, P. Balamuralidhar, One-time password authentication scheme based on elliptic curves for Internet of Things (IoT), in: Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, Riyadh, Saudi Arabia,, 2015, pp. 1–6.

[202] P. Fremantle, B. Aziz, J. Kopecky, P. Scott, Federated identity and access management for the Internet of Things, in: Secure Internet of Things (SIoT), 2014 International Workshop on, Wroclaw, Poland, 2014, pp. 10–17.

[203] M.A. Crossman, H. Liu, Study of authentication with IoT testbed, in: Technologies for Homeland Security (HST), 2015 IEEE International Symposium on, Waltham, MA, USA, 2015, pp. 1–7.

[204] Y. Kim, S. Yoo, C. Yoo, DAoT: dynamic and energy-aware authentication for smart home appliances in Internet of Things, in: *2015 IEEE International Conference on Consumer Electronics (ICCE)*,, Las Vegas, NV, USA, 2015, pp. 196–197.

[205] T. Bai, S.A. Rabara, Design and development of integrated, secured and intelligent architecture for Internet of Things and cloud computing, in: Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, Rome, Italy, 2015, pp. 817–822.

[206] S. Lee, J. Jo, Y. Kim, Method for secure RESTful web service, in: Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on, Las Vegas, NV, USA, 2015, pp. 77–81.

[207] J. Torres, M. Nogueira, G. Pujolle, A survey on identity management for the future network, Commun. Surv. Tutorials, IEEE 15 (2) (Jan. 2013) 787–802.

[208] S.W. Oh, H.S. Kim, Study on access permission control for the Web of Things, in: 2015 17th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, South Korea, 2015, pp. 574–580.

[209] OAuth 2. [Online]. Available: http://oauth.net/2/. [Accessed: November 2017].

[210] Apache Shiro | Simple. Java. Security. [Online]. Available: http://shiro.apache.org/. [Accessed: November 2017].

[211] RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map. [Online]. Available: https://tools.ietf.org/html/rfc4510. [Accessed: November 2017].

[212] P. Mahalle, S. Babar, N.R. Prasad, R. Prasad, Identity management framework towards internet of things (IoT): roadmap and key challenges, in: International Conference on Network Security and Applications, Chennai, India, 2010, pp. 430–439.

[213] J. Daubert, A. Wiesmaier, P. Kikiras, A view on privacy & trust in IoT, in: 2015 IEEE International Conference on Communication Workshop (ICCW), London, 2015, pp. 2665–2670.

[214] D. Ruiz, et al. Modelling the trustworthiness of the IOT RERUM Deliverable D3.3 April 2016.

[215] M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social Internet of Things, in: 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications – (PIMRC), Sydney, NSW, 2012, pp. 18–23.

[216] M. Nitti, R. Girau, L. Atzori, Trustworthiness management in the social Internet of Things, in: *IEEE Transactions on Knowledge and Data Engineering*, 26, May 2014, pp. 1253–1266.

[217] I.D. Addo, S.I. Ahamed, S.S. Yau, A. Buduru, A reference architecture for improving security and privacy in Internet of Things applications, in: 2014 IEEE International Conference on Mobile Services, Anchorage, AK, 2014, pp. 108–115.

[218] K.S. Sahoo, B. Sahoo, A. Panda, A secured SDN framework for IoT, in: 2015 International Conference on Man and Machine Interfacing (MAMI), Bhubaneswar, India, 2015, pp. 1–4.

[219] R. Vilalta, et al., Improving security in Internet of Things with software defined networking, in: 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1–6.

[220] K. Kalkan, S. Zeadally, Securing Internet of Things (IoT) with Software Defined Networking (SDN), IEEE Commun. Mag. PP (99) (2017) 1–7.

[221] N. Bindra, M. Sood, Is SDN the real solution to security threats in networks? A security update on various SDN models, Indian J. Sci. Technol. 9 (32) (2016).

[222] T. Xu, D. Gao, P. Dong, H. Zhang, C.H. Foh, H.C. Chao, Defending against new-flow attack in SDN-based Internet of Things, IEEE Access 5 (2017) 3431–3443.

[223] M.E. Ahmed, H. Kim, DDoS attack mitigation in Internet of things using software defined networking, in: 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), San Francisco, CA, 2017, pp. 271–276.

[224] A. Sivanathan, D. Sherratt, H.H. Gharakheili, V. Sivaraman, A. Vishwanath, Low-cost flow-based security solutions for smart-home IoT devices, in: 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bangalore, 2016, pp. 1–6.

[225] P. Bull, R. Austin, E. Popov, M. Sharma, R. Watson, Flow based security for IoT Devices using an SDN gateway, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, 2016, pp. 157–163.

[226] M. Baird, B. Ng, W. Seah, WiFi network access control for IoT connectivity with software defined networking, in: Proceeding MMSys'17 Proceedings of the 8th ACM on Multimedia Systems Conference, Taipei, 2017, pp. 343–348.

[227] P. Massonet, L. Deru, A. Achour, S. Dupont, A. Levin, M. Villari, End-To-End security architecture for federated cloud and IoT networks, in: 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, 2017, pp. 1–6.

[228] S.L. Keoh, S.S. Kumar, H. Tschofenig, Securing the internet of things: a standardization perspective, Internet Things J., IEEE 1 (3) (Jun. 2014) 265–275.

[229] M. Mohsin, Z. Anwar, F. Zaman, E. Al-Shaer, IoTChecker: a data-driven framework for security analytics of Internet of Things configurations, Comput. Secur. 70 (Supplement C) (September 2017) 199–223.

[230] Y. Li, F. Björck, H. Xue, IoT architecture enabling dynamic security policies, in: Proceedings of the 4th International Conference on Information and Network Security, Kuala Lumpur, Dec. 2016, pp. 50–54.

[231] M. Ge, J.B. Hong, W. Guttmann, D.S. Kim, A framework for automating security analysis of the internet of things, J. Netw. Comput. Appl. 83 (Supplement C) (April 2017) 12–27.

[232] S.M. Bellovin, Identity and Security, IEEE Secur. Privacy 8 (2) (May 1992) 88.

[233] A. Feghali, R. Kilany, M. Chamoun, SDN security problems and solutions analysis, in: 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), Paris, 2015, pp. 1–5.

[234] R.D. Sriram, A. Sheth, Internet of Things perspectives, IT Profess. 17 (3) (2015) 60–63.

[235] I. Yaqoob, I.A.T. Hashem, A. Gani, S. Mokhtar, E. Ahmed, N.B. Anuar, A.V. Vasilakos, Big data: from beginning to future, Int. J. Inf. Manage. 36 (6) (December 2016) 1231–1247 Part B.

[236] J. Fritsch, C. Walker, The problem with data, in: Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, London, UK, 2014, pp. 708–713.

[237] R.H. Weber, Internet of Things—need for a new legal environment? Comput. Law Secur. Rev. 25 (6) (2009) 522–527.

[238] C. Perera, R. Ranjan, L. Wang, S.U. Khan, A.Y. Zomaya, Big data privacy in the Internet of Things era, IT Prof. 17 (3) (May 2017) 32–39.

[239] A. Gyrard, S.K. Datta, C. Bonnet, K. Boudaoud, A Semantic Engine for Internet of Things: Cloud, Mobile Devices and Gateways, in: Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015 9th International Conference on, Blumenau, Brazil, 2015, pp. 336–341.

[240] M.A. Alqarni, Benefits of SDN for Big data applications, in: 2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), Irbid, 2017, pp. 74–77.

[241] C. Cecchinel, M. Jimenez, S. Mosser, M. Riveill, An architecture to support the collection of big data in the Internet of Things, in: 2014 IEEE World Congress on Services, Anchorage, AK, USA, 2014, pp. 442–449.

[242] F. Anon, V. Navarathinarasah, M. Hoang, C. Lung, Building a framework for Internet of Things and Cloud computing, in: Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), Taipei, Taiwan, 2014, pp. 132–139.

[243] K. Chang, C. Chen, J. Chen, H. Chao, Internet of things and cloud computing for future internet, in: Security-Enriched Urban Computing and Smart Grid, Hualien, Taiwan, 2011, pp. 1–10.

[244] T. Shon, J. Cho, K. Han, H. Choi, Toward advanced mobile cloud computing for the Internet of Things: current issues and future direction, Mobile Networks Appl. 19 (3) (Jun. 2014) 404–413.

[245] S. Dey, Mobile cloud applications: opportunities, challenges and directions, in: Proceedings of the First International Workshop on Mobile Cloud Computing & Networking, Bangalore, India, 2013, pp. 1–2.

[246] A. Alzahrani, N. Alalwan, M. Sarrab, Mobile cloud computing: advantage, disadvantage and open challenge, in: Proceedings of the 7th Euro American Conference on Telematics and Information Systems, Valparaiso, Chile, 2014, p. 21.

[247] H. Truong, S. Dustdar, Principles for engineering IoT Cloud systems, Cloud Comput., IEEE 2 (2) (Mar. 2015) 68–76.

[248] R.R. Krishnan, N. Figueira, Analysis of data center SDN controller architectures: technology and business impacts, in: Computing, Networking and Communications (ICNC), 2015 International Conference on, Anaheim, California, USA, 2015, pp. 104–109.

[249] S. Nastic, S. Sehic, D. Le, H. Truong, S. Dustdar, Provisioning Software-defined IoT Cloud Systems, in: Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, Barcelona, Spain, 2014, pp. 288–295.

[250] M.T. Kakiz, E. Öztürk, T. Çavdar, A novel SDN-based IoT architecture for big data, in: 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, 2017, pp. 1–5.

[251] A. Levin, K. Barabash, Y. Ben-Itzhak, S. Guenender, L. Schour, Networking architecture for seamless cloud interoperability, in: 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, USA, 2015, pp. 1021–1024.

[252] K. Bakshi, Network considerations for open source based clouds, in: 2015 IEEE Aerospace Conference, Big Sky, MT, USA, 2015, pp. 1–9.

[253] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, B. Koldehofe, Mobile fog: a programming model for large-scale applications on the internet of things, in: Proceedings of the second ACM SIGCOMM Workshop on Mobile Cloud Computing, Hong Kong, China, 2013, pp. 15–20.

[254] F. Bonomi, R. Milito, P. Natarajan, J. Zhu, Fog computing: a platform for internet of things and analytics, in: Big Data and Internet of Things: A Roadmap For Smart Environments, Springer International Publishing, 2014, pp. 169–186.

[255] A. Munir, P. Kansakar and S.U. Khan, "IFCIoT: integrated fog cloud IoT architectural paradigm for future internet of things," arXiv preprint arXiv:1701.08474, 2017.

[256] A. Munir, P. Kansakar, S.U. Khan, IFCIoT: Integrated Fog Cloud IoT: a novel architectural paradigm for the future Internet of Things, IEEE Consum. Electr. Mag. 6 (3) (July 2017) 74–82.

[257] C. Li, Z. Qin, E. Novak, Q. Li, Securing SDN infrastructure of IoT–fog networks from MitM attacks, IEEE Internet Things J. 4 (5) (Oct. 2017) 1156–1164.

[258] M. Özçelik, N. Chalabianloo, G. Gür, Software-defined edge defense against IoT-based DDoS, in: 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, 2017, pp. 308–313.

[259] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, M. Rovatsos, Fog orchestration for Internet of Things Services, IEEE Internet Comput. 21 (2) (2017) 16–24.

[260] T. Subramanya, L. Goratti, S.N. Khan, E. Kafetzakis, I. Giannoulakis, R. Riggio, A practical architecture for mobile edge computing, *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, November 2017.

[261] P.K. Sharma, M.Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access PP (99) (2018) 115–124.

[262] S. Tomovic, K. Yoshigoe, I. Maljevic, I. Radusinovic, Software-defined fog network architecture for IoT, Wirel. Pers. Commun. 92 (1) (2017) 181–196 01/01.

[263] H. Gupta, S.B. Nath, S. Chakraborty and S.K. Ghosh, "SDFog: A Software Defined Computing Architecture for QoS Aware Service Orchestration over Edge Devices," arXiv preprint arXiv:1609.01190, 2016.

[264] R. Morabito, Virtualization on Internet of Things edge devices with container technologies: a performance evaluation, IEEE Access 5 (2017) 8835–8850.

[265] D. Roca, J.V. Quiroga, M. Valero, M. Nemirovsky, Fog function virtualization: a flexible solution for IoT applications, in: 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, 2017, pp. 74–80.

[266] B. Kang, H. Choo, An experimental study of a reliable IoT gateway, ICT Express (April 2017). Available online.

[267] G. Kim, J. Kim, S. Lee, An SDN based fully distributed NAT traversal scheme for IoT global connectivity, in: Information and Communication Technology Convergence (ICTC), 2015 International Conference on, Jeju Island, Korea, 2015, pp. 807–809.

[268] V. Gazis, M. Görtz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger, E. Vasilomanolakis, A survey of technologies for the Internet of Things, in: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015, pp. 1090–1095.

[269] S.K. Datta, C. Bonnet and J. Haerri, "Fog computing architecture to enable consumer centric Internet of Things services," In *2015 International Symposium on Consumer Electronics (ISCE)*, Madrid, Spain, pp. 1.

[270] S. Cirani, L. Davoli, G. Ferrari, R. Léone, P. Medagliani, M. Picone, L. Veltri, A scalable and self-configuring architecture for service discovery in the internet of things, Internet Things J., IEEE 1 (5) (Oct. 2014) 508–521.

[271] deSantos Francisco Javier Nieto, S.G. Villalonga, Exploiting local clouds in the internet of everything environment, in: 2015 23rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, Turku, Finland, 2015, pp. 296–300.

[272] E. Gaura, J. Brusey, M. Allen, R. Wilkins, D. Goldsmith, R. Rednic, Edge mining the internet of things, Sensors J., IEEE 13 (10) (Oct. 2013) 3816–3825.

[273] M. Aazam, I. Khan, A.A. Alsaffar, E. Huh, Cloud of Things: integrating Internet of Things and cloud computing and the issues involved, in: *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST)* Islamabad, Pakistan, 14th–18th January, 2014, pp. 414–419.

[274] M. Aazam, P.P. Hung, E.N. Huh, Smart gateway based communication for cloud of things, in: Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on, Singapore, 2014, pp. 1–6.

[275] M. Aazam, E. Huh, Fog computing and smart gateway based communication for Cloud of Things, in: Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, Barcelona, Spain, 2014, pp. 464–470.

[276] S. Seol, Y. Shin, W. Kim, Design and realization of personal IoT architecture based on mobile gateway, Int. J. Smart Home 9 (11) (2015) 133–144.

[277] S. Dey, A. Mukherjee, H.S. Paul, A. Pal, Challenges of using edge devices in IoT computation grids, in: Parallel and Distributed Systems (ICPADS), 2013 International Conference on, Seoul, Korea, 2013, pp. 564–569.

[278] S.K. Datta, C. Bonnet, N. Nikaein, An iot gateway centric architecture to provide novel m2m services, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, Seoul, Korea (South), 2014, pp. 514–519.

[279] S.K. Datta, C. Bonnet, N. Nikaein, CCT: connect and control things, in: 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP, Singapore, 2014, pp. 21–24.

[280] C. Jennings, J. Arkko and Z. Shelby, "Media types for sensor markup language (SENML)," 2012.

[281] R. Morabito, N. Beijar, Enabling data processing at the network edge through lightweight virtualization technologies, in: 2016 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops), London, 2016, pp. 1–6.

[282] A. Manzalini, R. Minerva, F. Callegati, W. Cerroni, A. Campi, Clouds of virtual machines in edge networks, Commun. Mag., IEEE 51 (7) (Jul. 2013) 63–70.

[283] J. Kim, Designing multi-level connectivity for IoT-enabled SmartX Boxes, in: 2015 International Conference on Information Networking (ICOIN), Siem Reap, Cambodia, 2015, pp. 462–463.

[284] J. Pettit, Open vSwitch and the Intelligent Edge, 2014 *OpenStack Summit*.

[285] S.K. Datta, C. Bonnet, Smart M2M gateway based architecture for M2M device and Endpoint management, in: Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), Taipei, Taiwan, 2014, pp. 61–68.

[286] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, M. Mohammadi, Toward better horizontal integration among IoT services, Commun. Mag., IEEE 53 (9) (Sep. 2015) 72–79.

[287] J. Blendin, J. Ruckert, N. Leymann, G. Schyguda and D. Hausheer, "Position paper: Software-defined Network Service Chaining," pp. 109–114.

[288] F. Callegati, W. Cerroni, C. Contoli, G. Santandrea, Dynamic chaining of Virtual Network Functions in cloud-based edge networks, in: Network Softwarization (NetSoft), 2015 1st IEEE Conference on, London, UK, 2015, pp. 1–5.

[289] D. Willis, A. Dasgupta, S. Banerjee, ParaDrop: a multi-tenant platform to dynamically install third party services on wireless gateways, in: Proceedings of the 9th ACM Workshop on Mobility in the Evolving Internet Architecture, Maui, HI, USA, 2014, pp. 43–48.

[290] S. Nastic, H. Truong, S. Dustdar, SDG-Pro: a programming framework for software-defined IoT cloud gateways, J. Internet Serv. Appl. 6 (1) (Oct. 2015) 1–17.

[291] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, P. Dutta, The Internet of Things has a gateway problem, in: Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications, Santa Fe, NM, USA, 2015, pp. 27–32.

[292] G. Fersi, Middleware for Internet of Things: a study, in: 2015 International Conference on Distributed Computing in Sensor Systems, Fortaleza, Brazil, 2015, pp. 230–235.

[293] IoT-A. [Online]. Available: http://www.iot-a.eu/. [accessed: November 2017].

[294] Welcome to IoT6.eu | IoT6.eu. [Online]. Available: http://iot6.eu/. [Accessed: November 2017].

[295] iCore. [Online]. Available: http://www.iot-icore.eu/. [Accessed: November 2017].

[296] oneM2M - Home. [Online]. Available: http://www.onem2m.org/. [Accessed: November 2017].

[297] Iotdm:Main - OpenDaylight Project. [Online]. Available: https://wiki.opendaylight.org/view/IoTDM:Main. [Accessed: November 2017].

[298] Home - FIWARE. [Online]. Available: https://www.fiware.org/. [Accessed: November 2017].

[299] Butler. [Online]. Available: http://www.iot-butler.eu/. [Accessed: November 2017].

[300] COMPOSE Project | Collaborative Open Market to Place Objects at your Service. [Online]. Available: http://www.compose-project.eu/. [Accessed: November 2017].

[301] IEEE-SA - Internet of Things - The IEEE Standards Association. [Online]. Available: http://standards.ieee.org/innovate/iot/. [Accessed: November 2017].

[302] H. Madhoo, A. Khatri, T. Willemse, D. Oosthuizen, L. Coetzee, Future Internet concepts for demand management, in: Domestic Use of Energy (DUE), 2015 International Conference on, Cape Town, South Africa, 2015, pp. 19–26.

[303] S. Krco, B. Pokric, F. Carrez, Designing IoT architecture(s): a European perspective, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, Seoul, Korea (South), 2014, pp. 79–84.

[304] G. Fortino, C. Savaglio, C.E. Palau, J.S. de Puga, M. Ganzha, M. Paprzycki, M. Montesinos, A. Liotta and M. Llop, "Towards Multi-layer Interoperability of Heterogeneous IoT Platforms: The INTER-IoT Approach," pp. 199–232.

[305] iCore. [Online]. Available: www.iot-icore.eu. [Accessed: November 2017].

[306] C. Sarkar, A. Uttama Nambi SN, R. Prasad, A. Rahim, R. Neisse, G. Baldini, DIAT: a scalable distributed architecture for IoT, IEEE Internet Things J. 3 (2) (Jun. 2015) 230–239.

[307] T. Taleb, A. Kunz, Machine type communications in 3GPP networks: potential, challenges, and solutions, Commun. Mag., IEEE 50 (3) (Mar. 2012) 178–184.

[308] 3GPP TR 23.888 V11.0.0 (2012-09). [Online]. Available: http://www.qtc.jp/3GPP/Specs/23888-b00.pdf. [Accessed: November 2017].

[309] A. Kunz, H. Kim, L. Kim, S.S. Husain, Machine type communications in 3GPP: from release 10 to release 12, in: 2012 IEEE Globecom Workshops, Anaheim, California, USA, 2012, pp. 1747–1752.

[310] C. Bockelmann, N. Pratas, H. Nikopour, K. Au, T. Svensson, C. Stefanovic, P. Popovski and A. Dekorsy, "Massive Machine-type Communications in 5G: Physical and MAC-layer Solutions," arXiv preprint arXiv:1606.03893, 2016.

[311] M. Pticek, V. Cackovic, M. Pavelic, M. Kusek, G. Jezic, Architecture and functionality in M2M standards, in: Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on, Opatija, Croatia, 2015, pp. 413–418.

[312] J. Swetina, Guang Lu, P. Jacobs, F. Ennesser, JaeSeung Song, Toward a standardized common M2M service layer platform: introduction to oneM2M, Wireless Commun., IEEE 21 (3) (Jun. 2014) 20–26.

[313] http://www.onem2m.org/images/files/deliverables/TS-0001-Functional_Architecture-V1_13_1.pdf.

[314] ATIS Member Briefing: oneM2M Finalizes First Release, January 2015. http://www.atis.org/newsroom/images/atis-member-onem2m-briefing.pdf.

[315] S. Husain, A. Kunz, J. Song, T. Koshimizu, Interworking architecture between oneM2M service layer and underlying networks, in: 2014 IEEE Globecom Workshops (GC Wkshps), Austin, Texas, USA, 2014, pp. 636–642.

[316] S.K. Datta, C. Bonnet, A lightweight framework for efficient M2M device management in oneM2M architecture, in: Recent Advances in Internet of Things (RIoT), 2015 International Conference on, Singapore, 2015, pp. 1–6.

[317] S.K. Datta, C. Bonnet, Internet of Things and M2M Communications as Enablers of Smart City Initiatives, in: Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, Cambridge, UK, 2015, pp. 393–398.

[318] M3 Framework: Architecture - SWoT: Semantic Web of Things. [Online]. Available: https://www.ussm.gov/m3/#.V7yiTyh97D4. [Accessed: November 2017].

[319] M.B. Alaya, S. Medjiah, T. Monteil, K. Drira, Toward semantic interoperability in oneM2M architecture, Commun. Mag., IEEE 53 (12) (Dec. 2015) 35–41.

[320] M. Bauer, "Introduction to the Architectural Reference Model for the Internet of Things," First Reference Model White Paper. IOT—i The Internet of Things Initiative. [Online] Available: http://ww.iot—a.eu/[Accessed 14 July 2016].

[321] The Big Shift to IPv6-Based IoT is on the Roll! -IoT6. [Online]. Available: https://iot6.eu/sites/default/files/imageblock/ipv6-forum.pdf. [Accessed: November 2017].

[322] Deliverable D1.4 Updated Version of IoT6 Architecture and SOA specifications. [Online]. Available: http://iot6.eu/sites/default/files/IoT6%20-%20D1.4_0.pdf. [Accessed: November 2017].

[323] IoTDM Overview - OpenDaylight Project - OpenDaylight Wiki. [Online]. Available: https://wiki.opendaylight.org/view/IoTDM_Overview#Block_Diagram. [Accessed: November 2017].

[324] J. Crowcroft, M. Fidler, K. Nahrstedt, R. Steinmetz, Is SDN the de-constraining constraint of the future internet, ACM SIGCOMM Comput. Commun. Rev. 43 (5) (Nov. 2013) 13–18.

[325] A.L. Valdivieso Caraguay, A. Benito Peral, L.I. Barona Lopez, L.J. García Villalba, SDN: evolution and opportunities in the development IoT applications, Int. J. Distrib. Sens. Netw. 2014 (May 2014).

[326] H. Huang, J. Zhu and L. Zhang, "An SDN_based management framework for IoT devices," In *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET*, Limerick, Ireland, pp. 175–179.

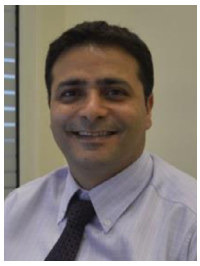
[327] N. Omnes, M. Bouillon, G. Fromentoux, O. Grand, A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges, in: Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, Paris, France, 2015, pp. 64–69.

[328] Z. Wen, X. Liu, Y. Xu, J. Zou, A RESTful framework for Internet of things based on software defined network in modern manufacturing, Int. J. Adv. Manuf. Technol. 84 (1-4) (Apr. 2016) 1–9.

[329] V.R. Tadinada, Software defined networking: redefining the future of internet in IoT and Cloud Era, in: Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, Barcelona, Spain, 2014, pp. 296–301.

[330] M. Boussard, D.T. Bui, R. Douville, N. Le Sauze, L. Noirie, P. Peloso, R. Varloot, M. Vigoureux, The Majord'Home: a SDN approach to let isps manage and extend their customers' home networks, in: 10th International Conference on Network and Service Management (CNSM) and Workshop, Rio de Janeiro, Brazil, 2014, pp. 430–433.
[331] M. Boussard, D.T. Bui, L. Ciavaglia, R. Douville, M. Le Pallec, N. Le Sauze, L. Noirie, S. Papillon, P. Peloso, F. Santoro, Software-Defined LANs for Interconnected Smart Environment, in: Teletraffic Congress (ITC 27), 2015 27th International, Ghent, Belgium, 2015, pp. 219–227.
[332] A. Hakiri, P. Berthou, A. Gokhale, S. Abdellatif, Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications, Commun. Mag., IEEE 53 (9) (Sep. 2015) 48–54.
[333] T. Lin, J. Kang, H. Bannazadeh, A. Leon-Garcia, Enabling SDN applications on software-defined infrastructure, in: 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 2014, pp. 1–7.
[334] A.G. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, S. Palazzo, Towards a software-defined network operating system for the IoT, in: Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, Milan, Italy, 2015, pp. 579–584.
[335] A. Galis, J. Rubio-Loyola, S. Clayman, L. Mamatas, S. Kukliński, J. Serrat, T. Zahariadis, Software enabled future internet–challenges in orchestrating the future Internet, in: International Conference on Mobile Networks and Management, Springer International Publishing, 2013, pp. 228–244.
[336] P. Bull, R. Austin, M. Sharma, Pre-emptive Flow Installation for Internet of Things Devices within Software Defined Networks, in: Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, Rome, Italy, 2015, pp. 124–130.
[337] P. Martinez and A. Skarmeta, "Empowering the Internet of Things with Software Defined Networking," FP7 European Research Project on the Future Internet of Things, 2014.
[338] Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, M. Vouk, A. Rindos, SDIoT: a software defined based internet of things framework, J. Ambient Intell. Hum. Comput. 6 (4) (Aug. 2015) 453–461.
[339] P. Hu, A system architecture for software-defined industrial Internet of Things, in: 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, Quebec, Canada, 2015, pp. 1–5.
[340] M. Lee, Y. Kim, Y. Lee, A home cloud-based home network auto-configuration using SDN, in: Networking, Sensing and Control (ICNSC), 2015 IEEE 12th International Conference on, Taipei, Taiwan, 2015, pp. 444–449.
[341] E. Patouni, A. Merentitis, P. Panagiotopoulos, A. Glentis, N. Alonistioti, Network Virtualisation Trends: virtually anything is possible by connecting the unconnected, in: Future Networks and Services (SDN4FNS), 2013 IEEE SDN for, Trento, Italy, 2013, pp. 1–7.
[342] M. Ojo, D. Adami, S. Giordano, A SDN-IoT architecture with NFV implementation, in: 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1–6.
[343] Q. Xiaofeng, L. Wenmao, G. Teng, H. Xinxin, W. Xutao, C. Pengcheng, WoT/SDN: web of things architecture using SDN, Communications, China 12 (11) (Nov. 2015) 1–11.
[344] IoT Standardization: Why should you care, Sep 8, 2017. Available Accessed: May 2018 http://nicolaswindpassinger.com/iot-standardization-care .
[345] AWS IoT Services Overview - Amazon Web Services. [Online]. Available: https://aws.amazon.com/iot/. [Accessed: May 2018].
[346] Internet of Things (IoT) - Cisco. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html#~stickynav=1. [Accessed: May 2018].
[347] IoT Edge | Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us/services/iot-edge/. [Accessed: May 2018]
[348] IBM Watson Internet of Things (IoT). [Online]. Available: https://www.ibm.com/internet-of-things. [Accessed: May 2018].

Ola Salman received her M.E. degree in Computer and Communications Engineering from the Lebanese University in 2013. In September 2014, she joined the PhD accelerated track program in the Electrical and Computer Engineering (ECE) department at the American University of Beirut (AUB). Her research interests are in the area of Information Security and Networks, Software Defined Networks, Edge Computing, Artificial Intelligence, and Internet of things. In 2017, she received the CNRS-L/AUB doctoral scholarship award from the Lebanese National Council for Scientific Research (CNRS) in recognition of her research work.



Imad H. Elhajj received his Bachelor of Engineering in Computer and Communications Engineering, with distinction, from the American University of Beirut in 1997 and the M.S. and Ph.D. degrees in Electrical Engineering from Michigan State University in 1999 and 2002, respectively. He is currently an Associate Professor with the Department of ECE at AUB. Imad received Best Research Paper Award at the Third International Conference on Cognitive and Behavioral Psychology (CBP), Best Paper award at the IEEE Electro Information Technology Conference in June 2003, and at the International Conference on Information Society in the 21st Century in November 2000. Dr. Elhajj is recipient of the Teaching Excellence Award at the American University of Beirut, June 2011, the Kamal Salibi Academic Freedom Award, 2014, and the most Outstanding Graduate Student Award from the ECE Department at Michigan State University, April 2001.

Ali M. Chehab received his Bachelor degree in EE from AUB in 1987, the Master's degree in EE from Syracuse University in 1989, and the PhD degree in ECE from the University of North Carolina at Charlotte, in 2002. From 1989 to 1998, he was a lecturer in the ECE Department at AUB. He rejoined the ECE Department at AUB as an Assistant Professor in 2002, and became a Full Professor in 2014. He received the AUB Teaching Excellence Award in 2007. He teaches courses in Programming, Electronics, Digital Systems Design, Computer Organization, Cryptography, and Digital Systems Testing. His research interests include: Wireless Communications Security, Cloud Computing Security, Multimedia Security, Trust in Distributed Computing, Low Energy VLSI Design, and VLSI Testing. He has more than 180 publications. He is a senior member of IEEE and a senior member of ACM.

Ayman Kayssi studied electrical engineering and received the BE degree, with distinction, in 1987 from the American University of Beirut (AUB), and the MSE and PhD degrees from the University of Michigan, Ann Arbor, in 1989 and 1993, respectively. In 1993, he joined the Department of Electrical and Computer Engineering (ECE) at AUB, where he is currently a full professor. From 2004 to 2007, he served as chairman of the ECE Department at AUB. He teaches courses in electronics and in networking, and has received AUB's Teaching Excellence Award in 2003. His research interests are in information security and networks, and in integrated circuit design and test. He has published more than 200 articles in the areas of security, networking, and VLSI. He is a senior member of IEEE, and a member of ACM, ISOC, and the Beirut OEA.