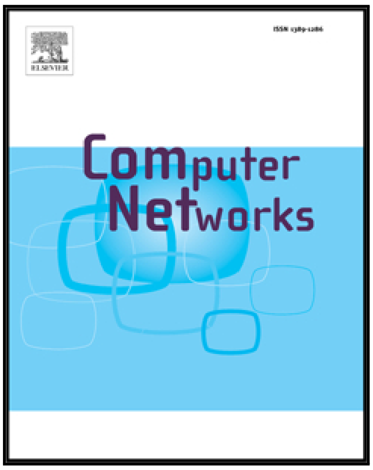


Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues

Alem Čolaković , Mesud Hadžialić

PII: S1389-1286(18)30524-3
DOI: 10.1016/j.comnet.2018.07.017
Reference: COMPNW 6547

To appear in: *Computer Networks*

Received date: 15 December 2017
Revised date: 18 May 2018
Accepted date: 9 July 2018

Please cite this article as: Alem Čolaković , Mesud Hadžialić , Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.07.017

Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues

Alem Čolaković[a,*], Mesud Hadžialić[b]

[a]*University of Sarajevo, Faculty of Traffic and Communications, Zmaja od Bosne 8, Sarajevo, Bosnia and Herzegovina*

[b]*University of Sarajevo, Faculty of Electrical Engineering, Zmaja od Bosne 8, Sarajevo, Bosnia and Herzegovina*

ARTICLE INFO

Article history:

Received 15 December 2017
Received in revised form 18 May 2018

Keywords:

IoT (Internet of Things)
IoT vision
IoT features
IoT enabling technologies
Open issues and challenges
Future research direction

ABSTRACT

IoT (Internet of Things) is a new paradigm which provides a set of new services for the next wave of technological innovations. IoT applications are nearly limitless while enabling seamless integration of the cyber-world with the physical world. However, despite the enormous efforts of standardization bodies, alliances, industries, researchers and others, there are still numerous problems to deal with in order to reach the full potential of IoT. These issues should be considered from various aspects such as enabling technologies, applications, business models, social and environmental impacts. In focus of this paper are open issues and challenges considered from the technological perspective. Just for clarification, we put in light different visions that stand behind this paradigm in order to facilitate a better understanding of the IoT's features. Furthermore, this exhaustive survey provides insights into the state-of-the-art of IoT enabling and emerging technologies. The most relevant among them are addressed with some details. The main scope is to deliver a comprehensive overview of open issues and challenges to be tackled by future research. We provide some insights into specific emerging ideas in order to facilitate future research. Also, this paper brings order in the existing literature by classifying contributions according to different research topics.

∗ Corresponding author. *E-mail address*: alem.colakovic@gmail.com (Alem Čolaković)

1. Introduction

IoT (Internet of Things) is based on integrations of various processes such as identifying, sensing, networking, and computation. It enables large-scale of technological innovations and value-added services which personalize users' interaction with various "things". There are numerous IoT applications that can be grouped into various domains such as health, traffic, logistics, retail, agriculture, smart cities, smart metering, remote monitoring, process automation, etc. Despite the enormous progress in different research fields including architectures, standardization, emerging technologies, security, etc. we consider that IoT is still in the nascent stage of its development. This article provides reports on the state of art, current trends and open issues according to the main IoT visions and enabling technologies. We conducted a review of up-to-date reference literature including journal papers, conference's papers, standards, project reports, white papers and reports from industries. Thus, we provide useful guidelines for readers to understand IoT paradigm and open issues in order to provide perspectives for future research and development.

To discuss research trends, we need to understand what IoT really means and to examine its impact on everyday life, industry, and new business models. We are still in nascent stages where everybody is trying to interpret IoT according to their visions and needs [1]. Because of that, there is no universal definition of IoT and existing visions are fuzzy. Also, there are some other terms related to IoT such as IoE (Internet of Everything), WoT (Web of Things), CoT (Cloud of Things), M2M (Machine to Machine), etc. Some authors consider these terms have the same meaning but the majority of authors distinguish these meanings according to particular vision [2]. We do not include deep analysis of different visions but we present some definitions so that the reader can gain an overall view of IoT.

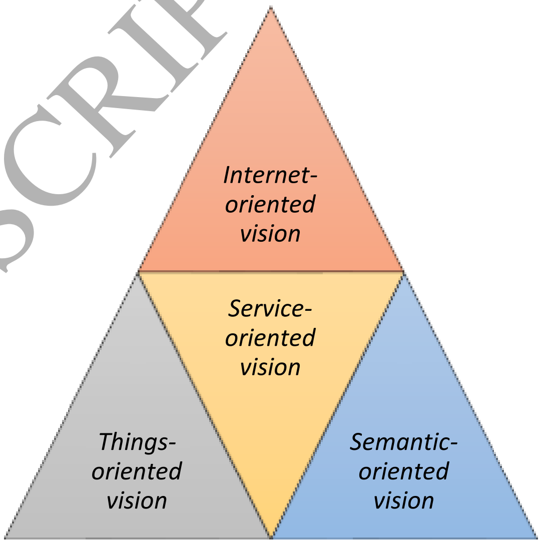
IoT is based on integration of various standards and enabling technologies with different sensing, connectivity, storage, computational, and other capabilities. However, the fragmentation of standards and diversities in deployed technologies produce significant challenges in providing full connectivity of everything [3]-[5]. This causes complex integration challenges [6] as one of the major challenges of IoT development. Numerous standardization organizations, alliances, academics, and industries make an effort on IoT developments, innovation, and standardization but there is still lack of a comprehensive framework with integrated standards under one IoT vision [7], [8]. This causes many challenges that have been identified and discussed in this paper.

Some of the most important challenges that IoT faces are related to traffic loads and various traffic models [9]. Every day more and more devices (things) are being connected to Internet and devices are becoming the major producers and consumers of traffic [10]. This is the reason why traffic requirements arise and we need new traffic models, protocols, network capabilities, security mechanisms, etc. There is a need of simplification and adoption of the current IP (Internet Protocol) architecture in order to enable seamless connectivity and effective management in HetNet (Heterogeneous Networks) environment [6], [11], [12]. Some other challenges related to development of IoT include devices identification, addressing, interoperability, mobility, massive scaling, management, energy efficiency, security, privacy, etc. Also, future deployments of IoT need to fulfill a sustainable smart world with the focus on green IoT enabling technologies which is another major issue [13].

In order to identify and discuss technology-based issues, this paper presents a classification of IoT enabling technologies according to their functionalities. This approach has its value to the research community because it can be used as a starting point for future research. The main objectives are summarized as follows:

- To clarify IoT vision and definitions as well as to provide a comprehensive overview of IoT features.
- To provide an overview of common IoT enabling and emerging technologies according to their functionalities.
- To provide a discussion about IoT open issues and challenges to be tackled by future research.

The remaining of this paper is organized as follows. Section 2 introduces to IoT visions and features according to various perspectives. Section 3 provides a comprehensive overview of IoT enabling technologies which are grouped into four main domains according to their functionalities. Open issues and challenges related to IoT are addressed and discussed in Section 4. Furthermore, we present a literature pool and give some future research hints. Section 5 focus on specific emerging ideas and issues such as modeling and mathematical formulation of IoT systems. The final Section 6 contains concluding remarks.



2. Internet of Things (IoT): visions and features

There are various definitions, outlooks, and visions that stand behind IoT. The early stages of Internet were characterized by WWW (World Wide Web) with linked static HTML (Hyper Text Markup Language) documents. This concept evolved to Web 2.0 which enabled user interaction through social networks, forums, blogs, e-learning platforms, CMS (Content Management Systems), etc. The next step in evolving of Internet is referred as Web 3.0 or Semantic Web. The main goal of Web 3.0 is to make web content and services understandable by devices without human involvement. IoT takes Web 3.0 to a new level by enabling seamless connectivity anytime and anywhere by anyone and anything. It enables to create novel value-added services by dynamically assembling different types of capabilities (sensing, communication, data processing, actuation, etc.) [14].

IoT (Internet of Things), IoE (Internet of Everything), M2M (Machine to Machine), CoT (Cloud of Things), WoT (Web of Things), are related terms that have been used by various authors, standardization bodies (ITU, ETSI, IETF, OneM2M, OASIS, W3C, NIST, etc.), alliances (IERC, IoT-i, IoT-SRA, MCMC, UK FISG, etc.), projects (IoT-A, iCore, CASAGRAS, ETP EPoSS, CERP, etc.), industries (e.g. CISCO, IBM, Gartner, IDC, Bosch, etc.) with the same or different meaning. For example, there is a vision that IoE has more comprehensive meaning than IoT such as CISCO's vision of IoE which is built upon the "four pillars" (building blocks) including people, things, data and process while IoT is only composed of "things". WoT is mostly considered with the similar meaning as IoT while M2M refers to direct communication (without human intervention) between objects (devices). Most of the approaches are based on a technological aspect of IoT paradigm because the same technologies are deployed in most of the cases independently of different visions. However, we have to highlight and other aspects such as social, business, and environment, that effect on IoT development in the future. This multidisciplinary approach is required to overcome any biases of different perspectives of IoT.

Differences in the IoT visions are the result of various approaches to this issue. The most of authors define IoT according to particular aspect and specific interests [1], [2], [15]-[17]. We need to address this challenge to understand IoT concept which will help to facilitate further research. In recent literature, IoT is considered from two [17] or three [16] main perspectives (visions) such as "Internet" oriented, "Thing" oriented and "Semantic" oriented perspective. We consider that the basic concept of Internet is not changing much and it is all about *things* which are changing and becoming smart. Deep research of IoT requires a comprehensive approach and the best way is to put together various perspectives and visions because IoT is not an individual system but integrates several subsystems and technologies. For example, IoT includes sensors, network infrastructure, data analytic tools, etc. upon which various applications and services can be run [18]. All this can be considered according to ITU vision of IoT that enables connectivity with 3A concept: anytime, anywhere, by anyone and anything [19].

Fig. 1. Towards IoT visions

According to *Internet-oriented* vision, IoT is considered as a global infrastructure that enables connectivity between both virtual and physical objects. ITU-T Y.2060 Recommendation defines IoT as a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies [19]. Also, ITU described some technologies deployed in the development of the IoT such as RFID, sensors, smart technologies, nano technology, etc. The similar definition has been provided by ISO/IEC JTC where IoT is defined as an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react [20].

There are some definitions that include only physical aspect (*things-oriented vision*) of IoT. "Things" can be "real world entities" or "virtual entities". For example, Al-Fuqaha A. et al. [5] consider IoT as a technology that enables physical objects to see, hear, think, share information, coordinate decisions and perform jobs. In special IEEE report IoT is defined as "a network of items - each embedded with sensors - which are connected to the Internet." The similar approach is used by OASIS which describes IoT as "a system where the Internet is connected to the physical world via ubiquitous sensors". The most of definitions related to this perspective refers to term M2M. ETSI defines concept named M2M communications as the communication between two or more entities that do not necessarily need any direct human intervention. Also, ETSI provides an architectural model for M2M.

Some approaches include a combination of two or all three perspectives. IETF describes the term IoT along with definition for "*Internet*" and "*things*". IAB (The Internet Architecture Board) defines IoT in RFC 7452 [21] as a trend where many embedded devices employ communication services offered by the Internet protocols. If we use a definition of "*Internet*" as world-wide network based on TCP/IP, and if we consider "*things*" as a semantically various objects, then IoT means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols [22]. From this perspective, WoT is the term used by W3C to define IoT from the application and Web technologies perspective: "The Web of Things is essentially about the role of Web technologies to facilitate the development of applications and services for the Internet of Things. This includes sensors, actuators, physical objects tagged with a bar code or NFC as well as their virtual representation. An example of relevant Web technology is HTTP which is used for accessing RESTful services and for naming objects as a basis for linked data and rich descriptions. Also, JavaScript APIs (Application Programming Interfaces) is web technology used for virtual objects to act as proxies for real-world objects". This perspective of IoT is used by Chen et al. [23] who define IoT as an *intelligent network* which connects all things to the Internet for the purpose of exchanging information and communicating with the information sensing devices in accordance with agreed protocols. Whitmore et al. [24] define the IoT as a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective. In Oxford Dictionary IoT is defined as the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data [25].

Instead of including a specific definition, some definition approaches include descriptions and list of requirements. For example, OneM2M present an exhaustive list of M2M/IoT system requirements as well as functional roles and standards related to architecture, interfaces, security, communication, etc. The National Institute of Standards and Technology (NIST) give a description of IoT rather than a formal definition. There are many other approaches to define IoT but some basic characteristics of these definitions are common. IoT require a new "technology stack" that includes various hardware and software embedded in the objects. Also, understanding of this paradigm requires considering many other aspects such as applications, social impact, business models, environmental issues, etc. We can signify that a comprehensive perspective is needed to understand IoT paradigm. For providing our definition we introduce a *service-oriented* vision which put IoT services in the focus while it includes all perspectives mentioned above (Fig. 1). Based on these considerations we highlight common characteristics of IoT (Fig. 2) and we can define Internet of Things (IoT) as the inter-networking paradigm enabled by technology stack which provides a seamless connectivity between physical and virtual objects to facilitate the development of intelligent services and applications with self-configuring capabilities. The technology stack is a combination of various technologies that enable these processes as well as to provide a seamless connectivity anytime and anywhere by anyone and anything.

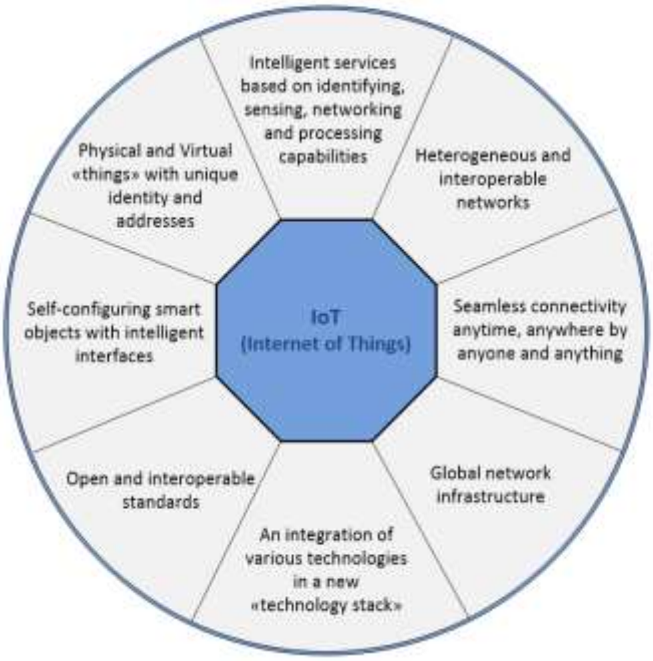
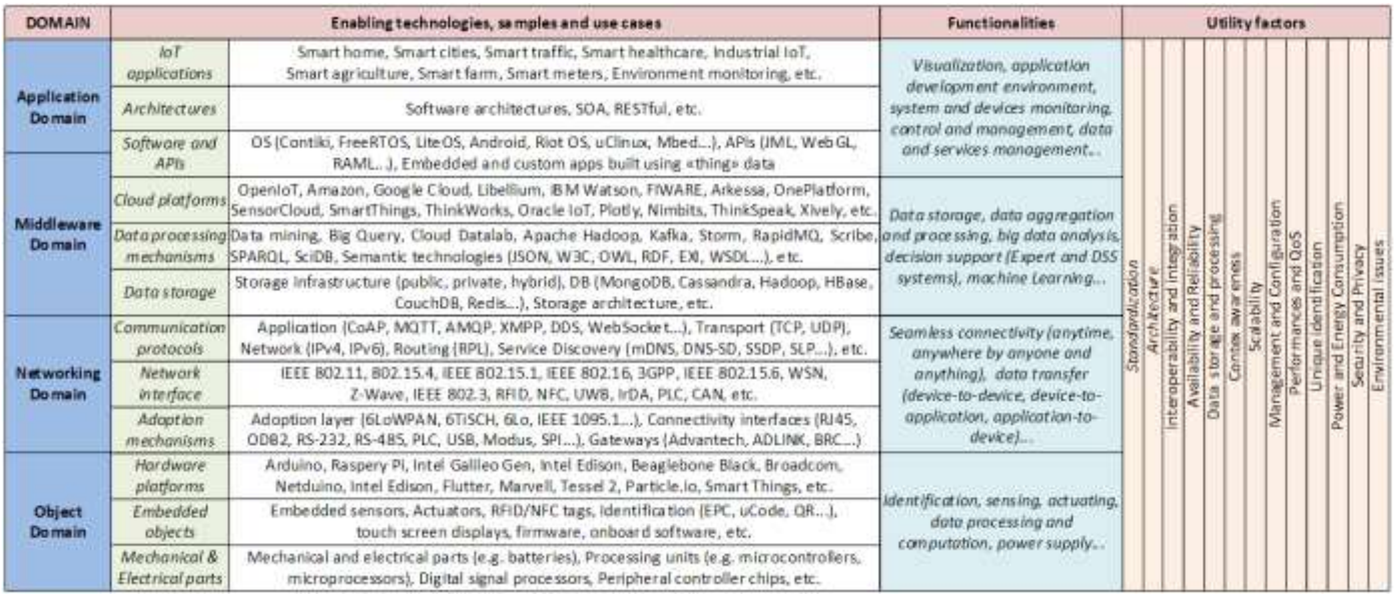

Intelligent services based on identifying, sensing, networking and processing capabilities
Heterogeneous and interoperable networks
Seamless connectivity anytime, anywhere by anyone and anything
Global network infrastructure
An integration of various technologies in a new «technology stack»
Open and interoperable standards
Self-configuring smart objects with intelligent interfaces
Physical and Virtual «things» with unique identity and addresses
IoT (Internet of Things)

Fig. 2. Towards IoT features

3. IoT enabling technologies

IoT systems are comprised of functional blocks to facilitate various utilities to the system such as sensing identification, actuation, communication, and management [26]. Therefore, IoT enabling technologies can be summarized into several categories such as: sensing technologies, identification and recognition technologies, hardware, software and cloud platforms, communication technologies and networks, software and algorithms, positioning technologies, data processing solutions, power and energy storage, security mechanisms, etc. For the purpose of this paper, we present IoT enabling technologies according to functional blocks composed of four main domains as shown on Table I. This classification is used to provide an overview of open issues and challenges clearly and concisely. All these domains (system layers) include various hardware, software, and technologies with specific functionalities and capabilities. Incorporating these domains into the IP architecture enables full deployment of the IoT technologies. IoT platforms enable easy integration of various IoT enabling technologies. These platforms can be defined as an intelligent layer that connects the things to the network and abstract applications from the things with the goal to enable the development of services [27]. They provide a framework for connecting things to the various networks and applications. There are various IoT platforms such as hardware and cloud platforms which can be used to increase productivity, usability, and flexibility of IoT applications as well as to decrease time and cost of the developing process.

IoT enabling technologies can be considered from various aspects (utility factors) which we used to provide insights into the open issues and challenges.



DOMAIN	Enabling technologies, samples and use cases		Functionalities	Utility factors
Application Domain	*IoT applications*	Smart home, Smart cities, Smart traffic, Smart healthcare, Industrial IoT, Smart agriculture, Smart farm, Smart meters, Environment monitoring, etc.	*Visualization, application development environment, system and devices monitoring, control and management, data and services management…*	Standardization Architecture Interoperability and integration Availability and Reliability Data storage and processing Context awareness Scalability Management and Configuration Performances and QoS Unique identification Power and Energy Consumption Security and Privacy Environmental issues
	Architectures	Software architectures, SOA, RESTful, etc.		
	Software and APIs	OS (Contiki, FreeRTOS, LiteOS, Android, Riot OS, uClinux, Mbed…), APIs (JML, WebGL, RAML…), Embedded and custom apps built using «thing» data		
Middleware Domain	*Cloud platforms*	OpenIoT, Amazon, Google Cloud, Libellium, IBM Watson, FIWARE, Arkessa, OnePlatform, SensorCloud, SmartThings, ThinkWorks, Oracle IoT, Plotly, Nimbits, ThinkSpeak, Xively, etc.	*Data storage, data aggregation and processing, big data analysis, decision support (Expert and DSS systems), machine Learning…*	
	Data processing mechanisms	Data mining, Big Query, Cloud Datalab, Apache Hadoop, Kafka, Storm, RapidMQ, Scribe, SPARQL, SciDB, Semantic technologies (JSON, W3C, OWL, RDF, EXI, WSDL…), etc.		
	Data storage	Storage infrastructure (public, private, hybrid), DB (MongoDB, Cassandra, Hadoop, HBase, CouchDB, Redis…), Storage architecture, etc.		
Networking Domain	*Communication protocols*	Application (CoAP, MQTT, AMQP, XMPP, DDS, WebSocket…), Transport (TCP, UDP), Network (IPv4, IPv6), Routing (RPL), Service Discovery (mDNS, DNS-SD, SSDP, SLP…), etc.	*Seamless connectivity (anytime, anywhere by anyone and anything), data transfer (device-to-device, device-to-application, application-to-device)…*	
	Network interface	IEEE 802.11, 802.15.4, IEEE 802.15.1, IEEE 802.16, 3GPP, IEEE 802.15.6, WSN, Z-Wave, IEEE 802.3, RFID, NFC, UWB, IrDA, PLC, CAN, etc.		
	Adoption mechanisms	Adoption layer (6LoWPAN, 6TiSCH, 6Lo, IEEE 1095.1…), Connectivity interfaces (RJ45, ODB2, RS-232, RS-485, PLC, USB, Modus, SPI…), Gateways (Advantech, ADLINK, BRC…)		
Object Domain	*Hardware platforms*	Arduino, Raspery PI, Intel Gallileo Gen, Intel Edison, Beaglebone Black, Broadcom, Netduino, Intel Edison, Flutter, Marvell, Tessel 2, Particle.io, Smart Things, etc.	*Identification, sensing, actuating, data processing and computation, power supply…*	
	Embedded objects	Embedded sensors, Actuators, RFID/NFC tags, Identification (EPC, uCode, QR…), touch screen displays, firmware, onboard software, etc.		
	Mechanical & Electrical parts	Mechanical and electrical parts (e.g. batteries), Processing units (e.g. microcontrollers, microprocessors), Digital signal processors, Peripheral controller chips, etc.		

Table I. IoT enabling technologies and functional blocks

3.1. Application domain

IoT has a huge potential for developing intelligent applications in almost every vertical market such as smart home, smart healthcare, smart transportation, etc. For example, there are many IoT applications that have been already successfully implemented for smart traffic systems, fleet tracking solutions, control of logistics chain, smart cities, smart metering, industrial automation, collision avoidance systems in cars, energy efficiency, smart buildings/homes/offices, environment monitoring, etc. IoT applications provide a set of functionalities and capabilities which can be grouped according to domain of utilization into four areas: monitoring (devices condition, environment state, notifications, alert, etc.), control (control of devices functions), optimization (device performances, diagnostics, repair, etc.) and autonomy (autonomous operations). A survey by Gluhak A. et al. [28] presents facilities for practical aspects of IoT.

Application domain manages application services that are usually provided through the IoT middleware layer. Therefore, software and APIs can be mapped to the application or middleware domain. However, we grouped IoT enabling technologies according to their functionalities and based on this consideration we included software (including OS) and APIs to this layer. For enabling functionalities of application domain there are some common embedded operating systems in use such as TinyOS, Contiki, LiteOS, Android, Riot OS, etc. These systems support low-power Internet communication and they require very few kilobytes of RAM. The SDKs (Software Development Kit) for these operating systems provides a software framework for various microcontroller firmware's to be run on IoT devices. SDK framework supports application programming by using various programming languages such as c, C++, C#, Java, etc. Another important building block of IoT systems are software platforms that enable integration of IoT objects with network technologies by using various communication protocols. These platforms provide an appropriate APIs or they are used in various environments for monitoring and controlling purposes [29]. Also, there are some platforms that provide other functionalities such as a development of services independently of hardware, data storage, and analytics, etc. Examples of these Cloud-based platforms are AWS IoT Platform, IBM Bluemix Platform, Microsoft Azure, Google Cloud, Platform, ThingWorx, Xively, etc. (Table I).

Key issues in developing IoT applications are related to deployment in various use cases, availability, management, reliability, interoperability, scalability (large-scale deployment and integration), security (authentication, access control, configuration management, antivirus protection, cryptography, etc.), and privacy. Research challenges include creating algorithms and schemes to present, analyze and process data collected by sensors. One of the major challenges related to incorporating IoT objects on the IoT web-based architecture is difficulty in extending existing approaches such as SOA (Service Oriented Architecture) [30]. Many IoT applications rely on REST (Representational State Transfer) or *RESTful* to provide interoperability but still, there are several issues to overcome. Some of technological developments and issues in the IoT application domain context have been envisioned in [17].

3.2. Middleware domain

We consider IoT middleware as a system constrained by software and infrastructure which is designed to be the intermediary between IoT objects and application layer. In this domain, we grouped technologies that provide functionalities such as aggregating, filtering and processing received data from the IoT devices, information discovery, machine learning, predictive modeling and providing access control to the devices for applications. Some literature uses other meanings of IoT middleware such as an approach that include applications in this domain. As we mentioned before, some IoT middleware provide OS and API management while enabling IoT applications communicating over heterogeneous interfaces.

The number of connected objects increases as well as raw data (unstructured data) that needs to be managed and processed. Huge amounts of data, including real-time data, are collected from heterogeneous sources such as sensors, smart objects as well as social networks and the web. Data and services are fragmented across many entities including data storage and processing units. Semantic web technologies such as RDF (Resource Description Framework) are developed as a model for data interchange on the Web to facilitate data merging. Message formats can be classified into text-based and binary-based. After conversion data into internal object structure, it is then ready for processing and visualization [31]. The most used text-based encodings are XML and JSON and these formats provide human-readable data. Binary messaging formats such as PBF (Protocol Buffers), Colfer, Protostaff Java object serialization, AMF (Adobe's Action Message Format) and Kryo reduce message size and because of that are mostly used to encode object graphs. Also, there are some encoding techniques to convert text-based messages to binary-based messages such as EXI (Efficient XML Interchange), BSON, BJSON, UBJSON. These encoding techniques provide message size reduction and improve their processing.

The most common solutions with IoT middleware functionalities rely on Cloud computing. Cloud platforms enable IoT services development and data processing independently of the hardware platform. There are many commercial and open source platforms (Table I) that can be evaluated according to gateway support, application protocol support, programming language, etc. Platforms such as Apache Hadoop, Apache Spark, Apache Kafka, Apache Storm, Apache Ambari, Apache HBase, Spark Streaming, Druid, Open TSDB, etc. can be deployed to build an efficient and scalable IoT platform. In paper [32] some survey has been done with comparisons of these platforms.

It is very important to ensure the high level of security and privacy that include mechanisms such as authentication, access control, configuration management, antivirus protection, cryptography, etc. The most recent research is focused on cross-domain solutions to improve security and data quality levels [192]. Also, in the focus of research community are paradigms known as Fog computing, MCC (Mobile Edge Computing), MCC (Mobile Cloud Computing), and Cloudlet. These computing systems based on these paradigms distributes some resources, processes, and services to data centers which are closer to the edge of the network to improve IoT system performances (e.g. response time, throughput, energy efficiency) as well as to provide better security and privacy. They include several mechanisms similar to Cloud computing but deployed at edge nodes that are located between IoT devices and Cloud infrastructure. According to this, they can be considered as a part of IoT middleware.

3.3. Network domain

Network domain includes hardware, software, technologies and protocols that enable connectivity between objects, and between objects and global infrastructure (e.g. Internet). IETF RFC 7452 [21] outlines the framework of IoT communication models with following variations: *Device-to-Device Communications, Device-to-Cloud Communications, Device-to-Gateway Model, Back-End Data-Sharing Model*. Recommendation ITU-R M.2083-0 [33] highlights the importance of key capabilities in different usage scenarios. IoT systems use an extreme diversity of communication technologies that need to be interoperable in order to meet IoT requirements. Also, it is more and more difficult to meet traffic requirements while the volume of traffic increases. *ITU-T Y.2060 Recommendation* [19] highlights some high-level requirements for networks to support IoT such as identification-based connectivity, autonomic networking, autonomic services provisioning, location-based capabilities, security, privacy, quality, plug and play, manageability. Other open issues related to this domain are interoperability, scalability, reliability, mobility management, routing, coverage, resource usage control and management, self-configuration, energy efficiency, spectrum flexibility, bandwidth, latency, etc. These issues will be described in the following Section of this paper.

IoT protocol stack based on TCP/IP reference model with the most common protocols is presented in Fig. 3. Various protocols need to interoperate thus we need to use appropriate communication system architecture. Several IoT communication architectures have been proposed by authors and projects [34]. However, there is still problem of interoperability between various network technologies. Maria.R.P. et al. [35] consider that the standardized approach based on latest developments is the only way to the future development of IoT. Developing new IoT-based protocols and architectures will play an important role in the following years.

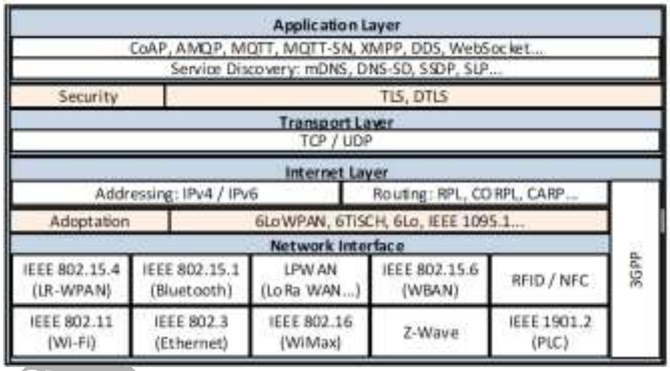


Fig. 3. IoT protocol stack

Application layer protocols used in traditional Internet services are not the corresponding option for IoT due to constraints of LLNs (Low Power and Lossy Networks). Because of that, there have been created protocols utilized to connect to things as well as to end-user applications. The most used application layer protocols are CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), MQTT-SN (MQTT For Sensor Networks), AMQP (Advanced Message Queuing Protocol), XMPP (Extensible Messaging and Presence Protocol), DDS (Data Distribution Service)- Some basic information about these protocols are presented in Table II. There are some other projects that define other protocols and groups of protocols to be used in IoT solutions such as Mihini/M3DA, LLAP (Lightweight Local Automation Protocol), LWM2M (Lightweight M2M). Also, some IoT applications may use other protocols such as HTTP, SSH, etc. *Service Discovery Protocols* such as *DNS-SD (DNS based service discovery), SSDP (*Simple Service Discovery Protocol*)*, SLP (Service Location Protocol), UDDI (Universal Description, Discovery, and Integration), *mDNS (Multicast DNS), Lightweight Directory Access Protocol (LDAP),* APIPA (*Automatic Private IP Addressing), Physical Web, HyperCat, UPnP (Universal Plug and Play)* are used to enable seamless and efficient discovery functions. These protocols can be grouped by function: discovery (DNS-SD, SLP, UDDI), naming (mDNS, LDAP) and addressing (APIPA) protocols.

Beside *TCP (Transmission Control Protocol)* [43] and *UDP (User Datagram Protocol)* [44] at transport layer, there are some other transport protocols used in experimental phases such as *QUIC (Quick UDP Internet Connections)* [195] and *NanoIP (Nano Internet Protocol)* [196]. QUIC is designed by Google to support a set of multiplexed connections between two endpoints over UDP. This protocol was designed to provide security protection equivalent to TLS/SSL, flow control equivalent to HTTP/2, and to reduce connection and transport latency as well as avoiding congestion by using mechanism of congestion control equivalent to TCP. NanoIP is a concept based on two transport techniques: nanoUDP for an unreliable and simple transport and nanoTCP which provides retransmissions and flow control. This project provides an alternative networking stack for control, automation and sensor networks without the overhead of TCP/IP.

Table II. Comparison between the IoT application protocols

Application protocol	Standard	RESTful Support	Transport protocol	Security	QoS support
CoAP [36]	IETF RFC 7252	Yes	UDP	DTLS	Yes
MQTT [37]	OASIS Standard	No	TCP	TLS/SSL	Yes
MQTT-SN	IBM Zurich Research website	No	TCP	TLS/SSL	Yes
XMPP [38], [39]	IETF RFC 6120, 6121	No	TCP	TLS/SSL	No
AMQP [40]	ISO and IEC	No	TCP	TLS/SSL	Yes
DDS [41]	OMG (Object Management Group)	No	UDP	DTLS	Yes
HTTP	IETF (RFC 2068, RFC 2616, RFC 7230), W3C	Yes	TCP	SSL	No
WebSocket [42]	IETF Internet Draft	Yes	TCP	TLS/SSL	No

IPv6 (Internet Protocol version 6) [45] is one of the key enablers for IoT [46] because IPv4 have gotten exhausted. It is a protocol for packet-switched networks that provides end-to-end datagram transmission across multiple IP networks. *RPL (Routing Protocol for Low Power and Lossy Networks)* [47] is mostly used routing protocol for IoT-based applications. It was created by IETF working group ROLL with the aim to support minimal routing requirements with simple and complex traffic models while enabling robust topology over lossy links with updating the routing information.

The most of IoT services rely on wireless technologies because of availability and mobility requirements. In Fig. 4. we present the most common wireless communication technologies used for IoT. Network technologies can be grouped into ANs (Access Networks) and CNs (Core Networks). Access networks such as Wi-Fi, WiMAX, GERAN, UTRAN, eUTRAN, satellite communication, etc. provide connectivity between IoT objects and CNs. Core networks such as 3GPP CNs, ETSI TISPAN CN, etc. provide as interconnection with other networks as well as roaming. There are various efforts to adapt to LLNs environment and to support lightweight traffic (low overhead) requirements. *6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks*) was created by the 6LoWPAN IETF WG [51]-[54] as a convergence layer to adapt link layer to IPv6 packets over IEEE 802.15.4 networks. It integrates IPv6 based infrastructure and WSNs to support low bandwidth, header compression, fragmentation, limited packet size (max. packet size to be transmitted on PHY layer is 127 bytes), multi-hop delivery and various address lengths described in [35]. It does not provide any routing capabilities and this task is provided by upper layers (e.g. RPL).

Some of the key enabling technologies for IoT are *RFID (Radio Frequency Identification) and NFC (Near Field Communication)* [48]-[50]. RFID is short range communication technology that uses an electromagnetic field to automatically identify and track tags attached to objects. RFID systems must not interfere with other systems such as radio emergency services or broadcasters of television signals, etc. Integrating sensor technologies and RFID enable a lot of new possibilities in IoT paradigm while enabling sensing, computing and connectivity capabilities in passive systems. The benefit of RFID technology has extended with tracking capabilities and making data accessible through the Internet. NFC is based on the ISO/IEC 18092:2004 standard and this technology is created on the RFID to enable a short-range communication. Each NFC tag has a unique identifier UID (Unique Identification). When it has Internet connectivity there is a possibility of data exchange with online services to extend its benefits. L. Atzori et al. [16] have presented some basic comparison between RFID, WSN, and RFID sensor networks.

IEEE 802.15.4 (Low-Rate Wireless Personal Area Networks - LR-WPANs) [55] was developed as a sub-layer for MAC (Medium Access Control) and PHY (Physical Layer). It is utilized for IoT due to reliable communication, low-power consumption, low data rate, low cost, high message throughput, security, encryption, authentication, and support for a large number of nodes [5]. This standard is the basis for several specifications such as ZigBee, ISA100.11a, MiWi, WirelessHART. The most popular specification based on this standard is *ZigBee* (IEEE 802.15.4-2006) that operates in the 2.4 GHz frequency range with 250 kbps and 1024 as the maximum number of nodes. It is a low-power, low-cost wireless technology (standard) that is deployed in many WSNs but its single channel nature makes it unreliable [6]. Also, it is not energy efficient while it requires router nodes to always be active [35]. This technology can be used with 6LoWPAN and traditional Internet protocols that empower its capabilities. However, it does not support QoS and this is very challenging issue. For example, interesting research area is the ZigBee evaluation to support QoS by exploiting a mix of IP multicasting, queuing management and traffic analytics techniques [56].

IEEE 802.15.1 (Bluetooth) operates in the 2.4 GHz worldwide available ISM (Industrial, Scientific and Medical) band and is one of the key enabling technologies for short-range IoT applications. Bluetooth SIG (Special Interest Group) proposed BLE (Bluetooth Low-Energy) in the Bluetooth 4.0 specification and Bluetooth 5 [57] as the latest version of the Bluetooth core specification to enable collecting and aggregating data from devices (sensors) which generate data at a very low rate. It is designed for short range (up to 50 meters) which is suitable for control and monitoring applications. BLE is also known as Bluetooth Smart protocol for short-range communication with low power consumption. Previous studies such as [58]-[62] have presented some of BLE functionalities with the conclusion of being a good option for some IoT case studies. IETF 6LoWPAN WG developed specification that enables transmission IPv6 packets over BLE [63] that empowered the IoT capabilities of this technology. New version Bluetooth 5 focuses on improvement of speed, range, security, energy efficiency, location-based functionalities, interoperability and coexistence with other technologies. It brings some major advances to the technology to make it a key enabler of IoT. Also, there are some other efforts to improve Bluetooth 5 such as Eddystone protocol [197]. It is released by Google in 2015 to define a BLE message format for proximity beacon messages.

IEEE 802.11 is set of MAC and PHY specifications for WLAN (Wireless Local Area Network) mostly known as Wi-Fi (Wireless Fidelity). The main issue of this technology is large energy consumption compared to Bluetooth and Zigbee [6]. Some improvements are required to overcome this limitation as well as to improve mobility, roaming, and QoS performances. There are some improvements such as IEEE 802.11ah (*Low-Power Wi-Fi*) [198] supports a wide range of IoT applications while being able to provide more energy efficiency, QoS, scalability (a large number of devices) and cost-effective solutions [64], [65].

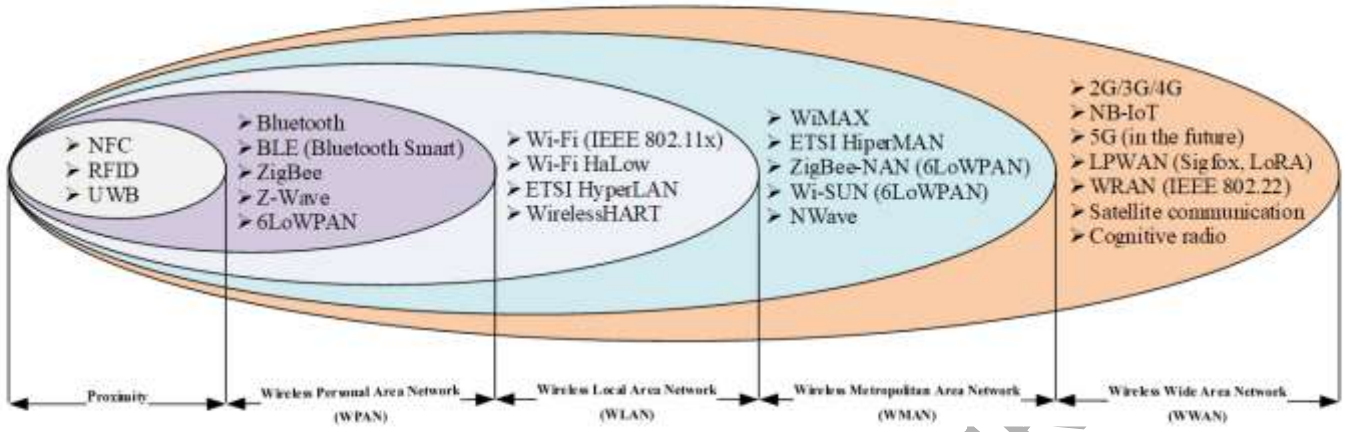


Fig. 4. Wireless communication technologies for Internet of Things

There are technologies that are primarily designed for IoT/M2M applications that need a wide area coverage, long battery lifetime, low bandwidth, low-cost devices. These technologies are known as *LPWAN (Low Power Wide Area Network)* [66] such as: Weightless [199], NB-IoT (Narrow-Band IoT) [200], LoRa WAN (Low Power Wide Area Network) [203], Sigfox [204], RPMA (Random Phase Multiple Access) [205], Wi-Fi HaLow [206], etc. In many cases, they operate in an unlicensed spectrum which is one of the main reasons leading to downsides such as scalability issues for a large-scale of devices due to spectrum congestion. Also, many IoT applications rely on data transfer over *cellular technologies* such as 2G (GSM, D-AMPS, PDC), 2.5G (GPRS), 2.75G (EDGE), 3G (UMTS/WCDMA, HSPA, HSUPA, EvDO), 4G (i.e. LTE, LTE-A), 5G. M2M (*Machine-to-Machine*) connectivity is referred within the cellular context or MTC (*Machine-type Communication*) within 3GPP (3rd Generation Partnership Project). 3G and 4 G technologies such as 3GPP LTE are enabling technologies that offer wide area coverage, QoS support, mobility and roaming support, scalability, billing, high level of security, the simplicity of management as well as connectivity of sensors through a standardized API [6]. LTE-A (Long Term Evolution – Advanced) and Mobile WiMAX Release 2 (*Wireless MAN - Advanced* or *IEEE 802.16m*) enabling higher speeds, more scalability, and low costs. In order to respond to the emerging IoT market needs and to avoid technology fragmentation, 3GPP has made major efforts in Release-13 and Release-14. For this purpose, 3GPP specified technologies such as eMTC (enhanced Machine-Type Communication), NB-IoT, and EC-GSM-IoT. The eMTC brings some LTE enhancements for MTC such as a new Power Save Mode (PSM). Release 14 brings new eMTC feature enhancements such as support for positioning and multicast, mobility for inter-frequency measurements, and higher data rates [202]. It brings enhancements such as lower costs, reduced data rate/bandwidth, and some other protocol optimizations. Also, Release-14 delivers new enhancements for the NB-IoT technology such as support for multicast, power consumption and latency reduction, mobility and service continuity enhancements, etc. EC-GSM-IoT delivered EGPRS enhancements, which in combination with PSM makes GSM/EDGE systems IoT ready. This technology brings improvements such as extended coverage, support for massive number of devices: at least 50.000 per cell, improved security compared to GSM/EDGE, etc. Summary for eMTC, NB-IoT, and EC-GSM-IoT has been delivered in the report on progress on 3GPP IoT [201]. All these technologies meet some of the requirements for IoT with but some other challenges occur. For example, QoS and network congestion are very challenging issues due to a huge number of deployed nodes (devices) [67].

A global perspective of 5G (5th generation mobile networks or 5th generation wireless systems) considers capabilities from ITU-R M.2083-0 and relates them to following use cases: mobile broadband, massive-machine communication, and mission-critical communication that should provide the possibility of full deployment of IoT solutions. 3GPP Releases 15 and 16 focuses to deliver the first set of 5G standards as well as the maturing of the LTE-Advanced Pro specifications. First functional specifications are expected in second half of 2018 which will include a performance evaluation against mMTC (massive Machine Type Communications) requirements, specifications for eMBB (enhanced Mobile Broadband) and URLLC (Ultra-Reliable and Low Latency Communications), etc. A detailed survey of the 5G cellular network architecture and some key emerging technologies such as interference management, spectrum sharing with cognitive radio, cloud computing, SDN, etc. has been presented in paper [4]. Some authors consider that there is a significant overlap among IoT and 5G. 5G design efforts are in place to support large-scale deployment of devices to enable global IoT as well as lower energy consumption with lower costs. An overview of unique characteristics and some comparisons of these technologies are compared in paper [191].

According to previous considerations, 3GPP has been working to support M2M application but still there are numerous challenges to overcome such as issues related to the energy efficiency, battery lifetime, network coverage, user identification, security, QoS, complexity, variety of IoT applications, etc. There are numerous open issues in 5G network design that need to be surveyed including advantages and shortcomings of backhaul solutions [69]. Enabling D2D (Device-to-Device) communication (exchange data without the involvement of base station or with its partial aid) is one of the turning points in a cellular system [68]. Also, very interesting research areas related to deploying

3GPP technologies for IoT are Fog computing, context-aware services, QoS management, etc.

3.4 Object domain

Object domain presents endpoint layer that includes physical things (real world entities) and virtual things (virtual entities). These objects have various capabilities such as sensing, actuation, identifying, data storage and processing, connecting with other objects, integration into communication networks, etc. IoT objects include embedded software (operating system, onboard application, etc.) and hardware (electrical and mechanical components with embedded sensors, processors, connectivity antennas, etc.).

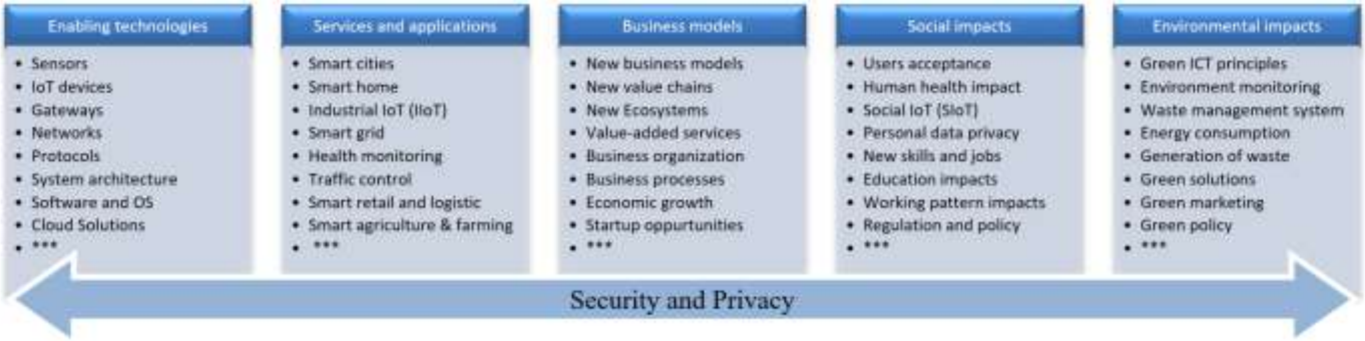


Fig. 5. Various aspects related to IoT

Sensors are objects that detect and measure some events or changes in its environment such as temperature, air pressure, acceleration, light, movement, etc. They perform various actions to provide an output for future processing. Various sensors are embedded in many objects (e.g. smartphones) to enable value-added services based on IoT. All devices should be identified by unique ID and connected with other objects and/or with IoT middleware. There are many identification methods including EPC (Electronic Product Code), uCode (Ubiquitous codes), QR (Quick Response) or matrix barcodes, etc. RFID identification has the similar function as Bar Code but is more advanced because it doesn't require the reader to be physically placed in front of it to have optical vision. RFID can be used as an actuator to trigger different events and even has modification abilities which Barcodes clearly do not have [70]. RFID tags (active or passive) have a unique identifier and the most commonly used is EPC. Active tags have a battery attached to the object and have continuously transmitted signals while passive tags emit signals only when it is triggered. As the unique identifier can be used the uID (Unique/Universal/Ubiquitous Identifier) architecture. Another technology with similar identification management is NFC.

Connectivity components enable wireless or wired connections by using different communication technologies which allow an exchange of information between different objects. SN (Sensor Networks) is a collection of sensors which communicates between each other or/and transmits data to some other infrastructure (e.g. Fog or/and Cloud). SN consists of the sensors, actuators, firmware and a thin layer of software framework. All these capabilities enable objects to be aware of their environment and to exchange data which is one of the goals of IoT. The most of IoT products use WSN (Wireless Sensor Networks) solutions which are mostly based on the IEEE 802.15.4 standard. This standard defines the MAC and PHY layers for low power as well as low bit rate communications in WPAN (Wireless Personal Area Network). IoT devices may contain gateways that collect data from sensors and send it over the Internet to other infrastructure (e.g. Cloud). They may be connected to other objects or networks via multiple gateways that can also act as a proxy between devices and networks. It is not strongly standardized how IoT devices are connected to the Internet apart from networking protocols [2]. IoT hardware platforms can facilitate communication, data flow as well as device, data and application management.

IoT constrained devices such as sensors have many challenges due to the requirements for identity management, processing, memory, connectivity, and energy capabilities. Many IoT projects were failed because of these issues [71]. Also, sensors have limited processing abilities and because of that they usually do not process data and instead they forward data to another infrastructure (data storage) across the network. Another major research field is to enhance sensors in sense of energy efficiency. Sometimes it is not possible to replace the sensor batteries due to dynamic environments; therefore, the design of low power sensors and sensors that not need any change of battery due the lifetime is a very attractive topic for future research.

4. IoT key issues and challenges

IoT based systems are usually complex due to a tremendous impact on all aspects of human lives as well as its various technologies deployed to enable autonomous data exchange between embedded devices. Development of IoT has an impact on various aspects of human lives (e.g. security, safety, health, mobility, energy efficiency, environmental sustainability, etc.). Therefore, IoT related issues and challenges need to be considered from various aspects such as enabling technologies, services and applications, business models, social and environmental impacts (Fig. 5). Analysis of recent contributions and research papers show that the most of the open issues arise due to an increasing number of connected devices which causes increased traffic demands with new traffic models. Other issues are related to the integration of various technologies, heterogeneous environment (e.g. various devices, data types, and network technologies), increased data storage and processing demands, privacy and security risks, etc. Therefore, in our focus are issues considered from technology-based perspective. We performed a classification of previous research and present a literature pool to bring order in the literature by classifying existing works according to different research areas (Table III).

We consider that full potential of IoT can be achieved only by deploying the corresponding architectures and enabling technologies. Because of that, there is a need for continuous improvement considering all aspects mentioned before. Therefore, it is very important to identify major issues and challenges related to the IoT development. This paper provides the insight into current research trends and provide some future research directions. The literature used in this paper is grouped according to research areas to facilitate future research.

Table III. Research and literature pool addressing IoT open issues and challenges

Research area	Research topics and literature pool	IoT enabling technologies	Literature Sources
Standardization	- IoT definition, vision and framework [1], [2] [5] [15]-[25], [28] - Architecture standardization [6]-[8], [19], [23], [24], [27], [32]-[35], [73]-[81] - Standardization of technology stack [5], [10], [23], [72], [73], [143], [172] - Standardization of Protocol Stack [35]-[44], [50]-[55], [57], [63], [66]	**IoT open issues and challenges listed in this table are related to enabling and emerging technologies** Application domain (*Architectures, APIs, Operating systems, Software, Applications*) Middleware domain (*Data storage infrastructure, Data processing mechanisms, Fog and Cloud computing*) Network domain (*Adoption mechanisms, Network interfaces, Communication technologies, Network protocols*) Object domain (*Mechanical & Electrical parts, Embedded objects, Hardware platforms*)	**Primary sources** (*Journal articles, Conference proceedings, Dissertations and Theses, Research projects, Standards*) **Secondary sources** (*Review articles, White papers, Books, Company reports, Technical reports*) **Tertiary sources** (*Practice guidelines, Dictionaries, Handbooks*)
System architecture	- Conceptual models [7], [8], [17]-[19], [23], [24], [26], [27], [32], [34], [75]-[81], [190], [207] - Hardware architectures [4], [7], [21], [34], [56], [82]-[87], [96], [97], [130], [178], [184], [188] - Cloud centric architectures [17], [30], [91], [114], [143], [193], [207]-[210] - Application frameworks [23], [30], [92], [114] - Process architectures [6], [8], [101], [102], [193], [210] - RESTful architecture [84], [93], [95], [190] - SOA architecture [24], [30], [98]-[100], [113]		
Interoperability and integration	- General interoperability issues [6], [38], [49], [71], [73], [103], [104] - Gateways support [10], [56], [88], [106]-[108], [126], [163], [178] - IoT platforms and architectures [6], [7], [24], [27], [29], [31], [74], [113], [180], [192] - Technical interoperability issues [5], [89], [90], [93], [111], [112], [190] - Semantic interoperability [23], [24], [114]-[118], [190]		
Availability and reliability	- Availability of IoT applications [6], [56], [179] - Seamless connectivity [3], [6], [11], [12], [19], [68], [130], [178], , [191] - Mobility and routing issues [6], [46], [56], [120]-[123], [126]-[128], [181] - Reliability of applications and services [5], [6], [35], [56], [127], [128], [179] - Reliability of infrastructure (network) [6], [46], [69], [121]-[123], [179], [191]		
Data storage and processing	- Computing and data analysis [1], [18], [31], [109], [124]-[128], [185], [193] - Data visualization [5], [17], [32], [185]		
Scalability	- Massive scaling issues [6], [7], [15], [18], [46], [67], [74], [107], [152], [181], [182], [185] - Discovery Service for the IoT *[5]*, [7], [14], *[161], [162]*		
Management and self-configuration	- Devices management [110], [137], [140]-[142] - Network management [4], [6], [11]-[12] [15], [56], [110], [131], [134]-[136], [138], [151] - Applications and data management [5], [131]-[133] - Trust management [113], [140], [182], [190]		
Performances and QoS	- Traffic loads and traffic models [9], [10], [17], [33], [148], [193], [209] - Application layer protocols [5], [32], [107], [153], [155]-[160], [189], [190] - Transport layer protocols [5], [160], [183], [195], [196] - Network layer protocols [5], [46], [56], [121]-[123], [194] - Link layer protocols evaluation [3], [5], [16], [58]-[62], [154], [197]-[206] - QoS and QoE evaluation [5], [67], [145]-[147], [149]-[152], [208]-[213]		
Identification and unique identity	- Identification technique and addressing schemes [17], [70], [140], [161] - IoT and IPv6 integration [15], [45]-[47], [51]-[53], [63], [120], [123], [162] - Services discovery protocols *[5], [161], [162]*		
Power and energy consumption	- Low-Power communications [17], [35], [55], [64], [65] - Low-power chipsets and terminals [2], [163]		
Security and privacy	- Security issues [5], [6], [18], [46], [56], [127], [128], [144], *[161]*, [167]-[175], [190], [192] - Privacy issues [46], [56], [161], [167], [169], [170], [182], [190]		
Environmental issues	- Green IoT technologies [13], [17], [176], [177]		

4.1. Standardization

Diversities in technologies and standards are identified as one of the major challenges in the development of IoT applications [5] [72]. Standardization of IoT architecture and communication technologies is considered as a backbone for the IoT development in the future [5], [35]. These facts imply that open standards are one of the key factors for the successful deployment of IoT. This type of standards is an important facilitator for innovation because of their availability to the public. They are being developed, approved, and maintained by a collaborative consensus-based decision-making process to provide better interoperability for systems using different technologies. Also, by using open standards there is less chance of being limited to a specific vendor or technology which is very important factor for IoT development.

The main standardization bodies such as ITU, ETSI, IETF, IEEE, W3C, OneM2M, OASIS, NIST, etc. are involved in the effort to make a framework for IoT standards. The scopes of standardization activities are various in order to provide open standards and architectures, seamless connectivity, interoperability, etc. But despite enormous efforts from standardization bodies and alliances, there is still no reference standard for IoT platform [10]. There is a problem to integrate various standards and contributions to be consistent and coherent. ETSI White Paper No.3 [73] highlighted several problems and typical consequences of non-coherent contributions such as incompleteness, inadequate interfaces (reference points), poor handling of options, lack of clarity and poor maintenance. All these open issues and challenges need to be considered in future to enable seamless connectivity as well as the integration and interoperability among various IoT enabling technologies.

Table IV. Examples of IoT conceptual models

Author	Description
ITU-T Rec. Y.2060 [19]	Reference model based on four layers: Device layer, Network layer, Service and Application support, Application layer.
ETSI TS 102 690 [75]	A functional architecture framework and high-level architecture for M2M where logical entities comprise this architecture.
ETSI TS 102 689 [76]	M2M high level system overview.
IEEE P2413 [77]	Three-tier IoT architecture.
CCSA [23]	General IoT architecture with functional platforms: Sensing and Gateway, Resource and Administration, Open Application.
GISFI IoT WG [78]	IoT Reference Architecture consist 5 layers: Sensor / Devices, Gateway, Core Network, Service Platform, Applications.
H2020 UNIFY-IoT [27]	IoT platforms with in-depth analysis as well as components across the IoT architectural layers.
IoT-A [34]	Reference models and architectures from different perspectives
A. H. Alhamedi [79]	Internet of things communication reference model
O. Vermesan, P. Friess [80]	The initial IoT6 architecture design approach.
Kaiwartya et al [81]	Five layered architecture for IoV (Internet of Vehicles) with description of functionalities for each layer.
Zoran B. Babovic [32]	A generic architecture of IoT web applications.
M. Kim, et al. [8]	Advanced conceptual architecture for organizing IoT-based pervasive communities and societies.
A. Rizzardi, et al. [190]	IoT cross-domain modular architecture communicating by means of RESTful services

4.2. Architecture

IoT systems should be framed within open IoT architecture and set of standards to enable integration of various technologies and to support full interoperability. IoT architecture needs to provide interoperability and to support full mobility to ensure service continuity (without interruption). Accordingly, one of the main challenges for IoT systems is to use an open, integrated and standardized architecture with separated application logic and hardware infrastructure. The corresponding architectures need to support heterogeneous nature of things, networks, data and applications to support full interoperability. Key design requirements for IoT architecture are scalability, interoperability, openness, and modularity in a heterogeneous environment. IoT architecture should enable multi-systems integration, cross-domain interactions, simple and scalable management functionalities, data analytics and user-friendly applications as well as the possibility to include the intelligence and automation across the IoT system. It may be treated as a system or paradigm which may consist physical objects (e.g. sensors, actuators), virtual objects (e.g. fog/cloud services, communication layers and protocols) or a hybrid of these two perspectives [74]. According to this perspective, IoT architecture can be classified into four groups: general/system-level, hardware/network, software and process [24].

General architecture considers a conceptual model to meet IoT requirements. There are numerous proposed IoT reference models but still, there is no general architecture which provides full interoperability. The existing approaches and efforts to solve this issue are based on layered frameworks and architectures [7]. In Table IV there is an overview of some existing general architectures and conceptual models.

Hardware/Network architectures have to enable interoperability among various networks and communication technologies to provide full connectivity between IoT objects. IoT devices can be grouped into two groups based on TCP/IP protocol suite support. In order to solve this heterogeneity related issue, there have been proposed several approaches such as APIs, gateway solutions, SDN-based solutions, NFV (Network Functions Virtualization), CCN (Content-Centric Networking), etc. Also, there are some other proposals such as a wearable IoT architecture with the ability to offer traceability of streamed data from source and the devices engaged with [188]. Other challenges are related to various technologies deployed in different networks including communication interfaces and access controls. All these issues must be considered in hardware and network architectures. Reference model and architecture based on IoT communication stack is presented in EU (European Union) project IoT-A [34]. This model is a good option for various cases but for some application domains other architectures should be investigated such as cloud centric architecture for cost efficiency services [17]. Examples of hardware/network-based architectures which support IoT paradigm are: EPCglobal based on RFID and EPC technologies [82], [83], Sensor and WSN based architecture [84], [85], peer-to-peer [86] and autonomic [87]. Despite the enormous efforts of standardization bodies and alliances, industries, academic and others there are still numerous open issues related to these architectures. For example, many recent researches focus on the questions such as "which computing paradigm (MCC, MEC, cloudlet, fog and cloud computing) to deploy in specific use case" or "when and where to deploy a specific computing system to facilitate the communication between IoT devices and application" [193].

Software architectures should provide a common set of services to enable processing (aggregation, computation, etc.) large amounts of data for service composition. IoT software architecture and framework need to be used to overcome the complexity of systems and to provide an environment for IoT services composition. IoT software platform should be created as OAP (Open Application Platform) to enable modular design as well as providing an open APIs (Application Programming Interface) to sensors and other devices. For example, JMS (Java Message Service) is a Java Message Oriented Middleware (MOM) API for sending messages between two or more clients. Also, there must be an integrated development environment such as Java and HTML5. Current IoT applications are mostly domain-specific with fragmented architectures that cannot integrate the data from different sources [23]. In order to enable integration of various services with other infrastructure (e.g. Fog and/or Cloud) it can be used APIs [5], gateways [56], [88], virtualization [89], SDN (Software Defined Networking) [90], cloud centric architecture [17], [91], etc. There are several approaches to provide application framework and another set of services for IoT such as SOA, RESTful, architectures based on fog and cloud computing, web application framework based on Google Toolkit [92], etc. These architectures cover Operating systems, IoT middleware, APIs, Data management, Big data, etc. Examples of Operating Systems (OS) for IoT support are Contiki, Riot OS, Android, TinyOS, LiteOS, etc. Future researches need to focus on improvements of RTOS (Real-Time Operating Systems), APIs and other components within IoT architectures to adapt these systems to IoT.

CORE (IETF Constrained RESTful Environments) working group has defined the subset of the RESTful specification [93] with CoAP to meet requirements of IoT applications such as interoperability with HTTP (HyperText Transfer Protocol), low overhead, multicast. RESTful principles are investigated in researches such as [84], [94], [95]. Used content type is XML (eXtensible Markup Language) or JSON (JavaScript Object Notation) which depends on HTTP server. This architecture can be applied in smartphone applications as it only requires an HTTP library but straightforward implementation of RESTful architecture is not possible due to requirements of LLNs as described in [35]. ETSI SmartM2M and oneM2M are projects based on RESTful design with their aim to resolve various fragmentation issues and to enable interoperability but there are still some open issues such as scalability and mobility as well as integrating RESTful based services into business process. Although these issues are highly scalable and distributed RESTful compliant architecture is considered as one of the best solutions today because some features such as authentication, caching and others can be utilized as well as all cloud platforms having the support for it.

SOA architecture is recognized as a good solution for the IoT middleware but we need to emphasize that sometimes (in some cases) application layer is not considered as a part of the IoT middleware. A design of SOA for IoT is a big challenge while it needs to handle many devices connected to the system which phrases scalability issues [74] and the difficulty in extending SOA [30]. Examples of implementation of SOA approach are CORBA, Jini, UPnP, OPC-UA, etc. Some specific IoT case studies use SOA architecture in different ways. For example, middleware layer can have a purpose to develop and handle an infrastructure for data processing and transmitting data to a gateway or actuating node while other functionalities from SOA can be distributed on other layers and components. Some surveys of IoT middleware have been done in [96], [97] while overviews of SOA architecture are given in numerous researches such as [98]-[100].

Process architecture should incorporate business processes into IoT paradigm [101], [102]. IoT enables new business opportunities and brings possibilities for new business models and value chains. The major challenge is to structure workflows to support IoT environment. Conventional conceptual frameworks need to be extended in order to enable process-aware IoT [8]. There are some novel architectural paradigms for the future IoT which are based on allocation of resources and processes between data sources and other infrastructure such as edge computing. This is very interesting research area with many open issues such as the question "which functions to allocate to the things, edge and cloud and how to enable interaction between these architectural levels."

4.3. Interoperability and integration

Interoperability is the ability of multiple devices and systems to interoperate regardless of deployed hardware and software. A variety of standards and technologies used for IoT development as well as various solutions from different vendors leads to massive heterogeneity which causes interoperability issues. IoT interoperability issue is considered across all layers. To overcome this issue, it need to be used a layered framework with standardized architecture**.** According to this approach, ETSI White Paper No. 3 [73] presents four interoperability levels technical, syntactical, semantic, and organizational.

Technical interoperability is usually associated with communication infrastructure and protocols. IoT systems need to provide interoperability over heterogeneous devices, networks and a variety of communication protocols such as IPv6, IPv4, 6LoWPAN/RPL, CoAP/CoRE, ZigBee, GSM/GPRS, Wi-Fi, Bluetooth, RFID, etc. The existing Internet architecture doesn't support full connectivity of the heterogeneous devices and this is still a challenging task that causes complex integration issues [6], [103]. Significant challenge is the integration of different subsystems regardless of their native communication protocols. This should enable the co-existing of used protocols and seamless communication even beyond IP because some technologies deployed in IoT systems are not based on IP. Therefore, in order to enable the ubiquitous connectivity, it must be developed HetNet (Heterogeneous Networking) paradigm that supports different MAC/PHY. An abstraction layer is necessary to abstract heterogeneity [31]. Also, there is a requirement for mechanisms for management and coordination as referred to [6], [12], [104]. IEEE 1905.1 standard [105] was designed for interoperability support and provides a common interface (abstraction layer to hide diversity of MAC) widely deployed in home networking technologies. It provides interoperability as well as secure connections, facilities network management, path selection, auto configuration, extends network coverage, and supports end-to-end QoS. Solutions for interoperability problems are usually based on APIs [5], implementation of gateways [56], [88], integrating smart resource-constrained objects into the Internet using virtual networks [89], the approach based on SDN [90], etc.

Gateways provide several solutions such as protocol conversion or centralizing remote connectivity depending on purpose and layer where they are implemented. Interoperable gateways at object layer support multiple interfaces to enable devices to be connected through a different kind of ANs (Access Networks) while their implementation at the network layer enables connectivity between various network technologies including ANs and CNs. According to a study [106] avoiding gateways as architectural elements at object layer can support full connectivity and peer-to-peer networking solutions while gateway roles can be addressed in smart objects such as smartphones. This solution enables devices to be directly connected to any other device or point on the Internet which is a true IoT vision. Also, this can solve the potential problem of implementing gateways such as slowing down a full end-to-end connectivity but the challenge is to enhance devices capabilities such as computing, storage, communication interfaces, low power consumption, etc. The solution for this problem can be smartphone-based mobile gateways as presented in [10], [107], [108] while everyday smartphones capabilities are improved [109]. There are several challenges related to this solution such as development of mobile gateway software architecture which supports full interoperability, limited storage and computation capabilities, efficiency in battery consumption especially when concurrent communication interfaces are deployed.

API based solutions for interoperability can be used for the automatic conversion between various application protocols. According to used protocols, IoT devices can be grouped into two groups based on support for TCP/IP protocol suite. IoT applications that use CoAP, MQTT, MQTT-SN, AMQP, REST and some other support TCP/IP but also there are applications without this support and because of that interoperability issue occurs. Al-Fuqaha et al. [5] emphasize the need for new protocols for communication compatibility in a heterogeneous environment. APIs can be implemented in different software and cloud platforms. Some operating systems like Contiki, Riot OS, Android, TinyOS, LiteOS, etc. enable modular design and provide open APIs which are necessary for application interoperability. There are several interesting research topics related to APIs interoperability such as to provide a trustworthy interoperability by using a proxy framework for API interoperability in the IoT.

IoT platforms improve interoperability in a heterogeneous environment and provide functionalities such as connectivity of various objects using communication technologies, device management, data processing, data visualization, etc. According to their functionalities, IoT platforms can be grouped as hardware platforms, software platforms, and cloud platforms. These platforms can include various solutions such as different network interfaces, gateways, APIs, etc. *IoT hardware platforms* enable devices connectivity as well as data processing outside the data center. They provide gateways to enable connectivity of devices with various network technologies. IoT hardware platforms provide technical interoperability by enabling development of IoT products which deploy various devices and networks. Examples of hardware platforms are Arduino, Raspberry Pi, Gadgeteer, BeagleBoard, pcDuino, etc. However, there is still the challenge to develop a platform able to interact with all technologies deployed in IoT. Another major issue is to enable interconnection between various platforms to empower their capabilities. Other issues are related to power supply, energy efficiency, security, seamless connectivity, mobility of platforms, etc. *IoT software platforms* enable IoT objects to integrate (sensors/actuators) with network technologies by using various communication protocols. These platforms integrate development environment (HTML5, Java, etc.) and provide APIs to enable developers to communicate with IoT devices over various network technologies. *Cloud platforms* enable to develop IoT solutions based on three models of cloud service: Software as a Service (SaaS), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). Some analysis of the most used and leading IoT platforms on today's market have been done in H2020 – UNIFY-IoT Project [27]. Key issues for all IoT platforms are related to supporting technologies such as processors and semiconductors, sensors, communication hardware and protocols, operating systems, developer tools, analytic tools, etc. Another key issue for these platforms is related to security (authentication, authorization, access control, intrusion detection, recovery mechanisms, etc.).

There are some other solutions for technical interoperability issues at different layers which provide dynamic, flexible and automated management and reconfiguration of the network [6]. The aim is to simplify network design and management by resolving some technical interoperability issues. In paper [110], authors proposed a cognitive management framework for IoT to solve heterogeneity problems among devices and associated services. Another interesting solution is a hub-based approach that provides scalable and reliable communication and improve some interoperability issues [111], [112]. Also, software architectures such as SOA reduce the system integration problems and improve interoperability among heterogeneous IoT devices in physical networks [113]. It is done by providing a powerful framework which support connectivity and component integration in IoT systems. The primarily goal of this architecture is to enhance IoT application interoperability and extendibility at the service and application layers. However, despite the flexibility offered by this framework, there are some issues related to SOA architecture such as the lack of an intelligent and connection-aware framework to support interoperability.

Syntactical interoperability is associated with understanding content (information) and refers to data formats, syntaxes, and coding such as XML and HTML. IoT applications need to integrate the data from different sources [23]. The new software architecture must enable searching, aggregating and processing the data generated by heterogeneous devices [24]. For that purpose, it has to be used a standardized data formats, syntaxes, and coding. IoT middleware needs to include mechanisms such as APIs solution for support interoperability within the diverse applications, services, and data format.

Semantic interoperability enables interpretation of content (the meaning of information) to be shared by communicating parties [114]. The term "semantic" in the IoT refers to the possibility of extracting knowledge from raw data collected from sensors. This "knowledge" enables to provide useful services and reports based on analyzed data [115]. The evolution of "Semantic Technologies" enables some level of data interoperability as well as advanced decision-making. Semantic interoperability enables IoT objects to learn, think and understand social and physical worlds. A common high-level framework with adequate architecture as well as new techniques such as data mining are needed to enable extraction meta-information (convert raw data to knowledge). For example, semantic level interoperability architecture for pervasive computing and IoT is presented in [114]. Some of the semantic technologies for the IoT including JSON, W3C, OWL (Web Ontology Language), RDF (Resource Description Framework), EXI (Efficient XML Interchange), and WSDL (Web Services Description Language) have been presented in [116]. **A v**ariety of these technologies leads to heterogeneity at a semantic level which is significant research field. One of the possible solutions is to use the semantic model with XML and ontology [117], [118]. Also, there are some useful data standards such as IOTDB, SensorML, Semantic Sensor Net Ontology - W3C, Wolfram Language, RAML (RESTful API Modeling Language), SENML (Media Types for Sensor Markup Language), LsDL (Lemonbeat smart Device Language), etc. However, it is still open issue to design a semantic IoT framework and open data standards to support full interoperability.

Organizational interoperability is usually associated with the ability of data exchange even though using different information systems and infrastructure. There is wide area of research topics related to IoT interoperability issues such as: developing new APIs, enhancement existing gateways or creating new gateway, improving devices capabilities to enable seamless connectivity and interoperability, improvement of solutions based on integrating smart resource-constrained objects into the Internet using virtual networks, using concept based on SDN, etc. SDN is very interesting research area in recent years because it is considered as emerging networking technology which provide the ability to establish and manage virtualized resources as well as to provide some level of interoperability without deploying a new hardware. All solutions mentioned above require the corresponding architecture to enable full interoperability.

4.4. Availability and reliability

Availability of services is one of the key issues to be addressed to properly manage the dynamics of IoT systems. Availability means that IoT applications should be available anywhere and anytime for every authorized object. The objects that are going to be connected should be adaptive and intelligent to support seamless connectivity and desired availability.

Availability of network and its coverage area must enable the continuity of the services use regardless of mobility, dynamic change of network topology or currently used technologies. All this requires mechanisms for interoperability, handover, and recovery in case of some unattended operations. An appropriate monitoring system, protocols, and self-healing mechanisms need to be deployed to enable robustness of system [119]. Some communication technologies suffer from intermittent availability which can cause service interruption. For example, some IoT applications can rely only on satellite communication which fluctuating quality. Therefore, it must be enabled computing (data collecting, processing, control, etc.) which is independent of sending data over the Internet or other networks to the computing infrastructure. MCC, MEC, Cloudlet, and Fog computing are paradigms proposed to overcome some of these issues. However, there are some new challenges as described before in this paper.

Mobility is another major challenge in IoT systems where services are provided to mobile users. IoT devices may be moved and frequent topology changes can occur. The goal is to create a robust system in spite of these dynamic changes. Because of that, there is a requirement for efficient mobility management mechanisms [120]. MIPv6 (Mobile IPv6) is a protocol developed to support mobility in IPv6 networks. In addition, IPSec (Internet Protocol Security) is mandatory for MIPv6 in order to support trust between home agent and mobile device. Also, some deployments of IoT systems imply that devices need to know their locations and to be aware of its environment (location of neighbor devices). This is another major challenge for future research especially when developing some real-time applications that require a location-awareness.

Routing issues are very important for reliability due to scheduling and routing in the multi-hop mesh topologies. Routing processes need to support dynamic topology changes, multihop routing, scalability, context awareness security mechanisms, QoS, etc. Also, routing protocols need to be context-aware and energy-aware (green routing protocols). Some surveys for multicast routing in the IoT environment have been done in [121] where authors propose algorithms for the establishing a multicast routing tree. RSVP (Resource Reservation Protocol) and MPLS (Multi-Protocol Label Switching) solve several routing problems. Also, deploying RPL routing protocol provide some solutions for routing issues while connecting LLNs to the Internet [122]. This protocol enables topology adoption and provides efficient routing functionalities. However, it has some weaknesses and limits such as high overhead, high packet loss, and latency in mobile conditions [123]. Another challenge is to provide a trade-off between reliability and energy consumption. This is a reason to use UDP as a transport protocol while retransmission control mechanisms could be implemented at the application layer [35]. Therefore, it must be deployed efficient upper-layer protocols (transport and application) that provide end-to-end reliability. Another solution for these problems is to develop a new protocol extension such as a new mobility support layer (MoMoRo) for Low Power Wireless Sensor Networks [194].

The IEEE 802.15.4e enables high reliability while it deploys TSCH (Time Synchronized Channel Hopping) as its part [35]. It defines a simple scheme for shared cells to solve a problem of collision as well as synchronization (acknowledgment-based and frame-based). However, this issue is still open to further improvement.

4.5. Data storage, processing and visualization

With a huge increase of connected objects and data traffic volume, there is a requirement for new calibration and analytic techniques. IoT systems need a common analytic platform to support a big data which need to be delivered as a service to IoT applications. Various data mining methods such as AI (Artificial Intelligence), machine learning and others intelligent decision-making algorithms enable computational processes to discover patterns in large datasets. These techniques can be used to organize raw data as well as to extract usable information and knowledge from it but costs are a limitation.

To handle continuously increased amount of data it seems that only Cloud technology can effectively meet these requirements. There are several Cloud platforms that exist on the market (Table I) with different storage and computing capabilities, supporting application protocols, interoperability, gateway support, billing models, etc. However, there are some issues that need to be considered. Transferring big data from the edge devices (e.g. sensors, smartphones, etc.) to the cloud infrastructure brings the following issues: network performances (e.g. delays, bandwidth, congestion, reliability, availability, etc.), costs of moving data through the Internet (it is very expensive), cost of storing data on cloud servers, security of data transmission and storing, privacy issues, etc. In paper [5], authors identified several other challenges related to deploying Cloud computing for IoT such as synchronization and standardization between different cloud vendors, balancing between IoT requirements and cloud services environments, reliability in sense of security between devices and cloud platforms, management of cloud computing and IoT, etc. The interesting challenge is to develop a scalable and high performances hybrid cloud platform. Also, there is a need for new algorithms for raw data filtering, selection, abstraction, and aggregation. Surveys on state of the art for Cloud computing and IoT integration has been done in [1], [31], [124], [129].

Cloud computing is not always necessary such as in the cases when local infrastructure resources are sufficient for data storage and processing. Processing raw data at locally deployed nodes can reduce the amount of data needed to be transferred through the Internet. This reduces data congestion, latency, costs, and improves some other performances. New computing paradigms such as MCC, MEC, Cloudlet, and Fog computing deploy rule-based system applied to a local infrastructure in order to provide an extension of Cloud computing. These systems improve some IoT performances such as QoS, reliability, mobility, security, and privacy. For example, fog computing enables to deploy smart devices like smartphones and home gateways for preprocessing data and context-aware computing. However, these platforms are not tailor-made in all use cases due to lack of capabilities for complex analysis and storing huge amount of data. These functionalities are complemented with Cloud computing. Therefore, only some basic computation processes can be done at edge layer. In order to overcome resource limitations of local infrastructure, data need to be forwarded to a Cloud. This issue is related to the question when and where to deploy some computing system. Also, integration of IoT and edge computing systems have to face with static and dynamic IoT devices in order to provide mobility support. This leads to services migration challenge and computational issue due to low power requirements. Another important issue related to mobility is collaboration and synchronization between edge nodes. A mechanism for aggregating data could be implemented at the gateway to manage data flows but this solution implies deployment of adequate software. Therefore, integration of IoT and edge computing doesn't solve issues such as mobility, complex analysis, security and privacy of data on edge devices [127], [128]. Also, interesting research topic is context-aware computing that was identified as one of the key factors for IoT development [31], [125].

There are a few current and forthcoming problems and some specific challenges related to data visualization such as to provide tools for the interaction of the user with the IoT environment, visualization of the raw data in a meaningful way and according to the end-user needs [17], etc. IoT applications require connectivity to infrastructure (e.g. cloud and network) and they must support user-friendly interfaces to enable secure and remote control over various devices. Eliminating the need for physical controls in the object itself by using new digital user interfaces is less costly and has more customizes capabilities. IoT applications can be autonomous or controlled by humans (directly, passively or hybrid). This is very interesting research area due to several challenges such as understanding different types of human-in-the-loops controls, how to implement feedback control, etc. Visualization of data gathered from sensors includes charts, animations, maps, tracking location on maps, etc. GUI (Graphic User Interface) provides visualization of performed measurements and enables to perform different control actions. Also, there are some threats while extracting information from raw data such as the oversimplification of data or overreliance on visuals. These issues imply requirements for methods of data visualization which enable reducing or illustrating data in simplified ways. However, this simplification of big data could lead to unfounded conclusions. Web technologies such as HTML 5 provide solutions for some of these issues. It specifies canvas elements for dynamic rendering of the 2D graphic while WebGL (Web Graphics Library) is JavaScript API running on HTML 5 canvas element for advanced 2D and 3D graphics application development [32]. Emerging technologies such as touchscreen technologies, 3D screens, and others can provide an efficient way to navigate the data as well as to extract useful information from raw data. Although the evolution of visualization technologies from CRT to Plasma, LCD, LED and beyond this is still open research area. For example, a very interesting and emerging research topic is the representation of sensors in the 3D landscape.

4.6. Scalability

Scalability is the ability to add new devices and services to IoT system without degradation of existing service performances. A key challenge related to scalability is to support a large number of various devices with memory, processing, bandwidth and other resource constraints [107]. Scalable mechanisms must be deployed for efficient discovery of devices but also to enable their interoperability. To enable scalability as well as interoperability there must be used a layered framework and architecture [7]. Design of IoT architectures that support scalability is a big challenge when it comes to the future development of IoT systems. These architectures need to handle numerous devices connected to the system which phrases scalability issues [74]. One of the possible solutions is to use highly scalable cloud-based platforms with the possibility to store a huge amount of collected data. The Therefore, a Cloud of Things [124], [129] can be used as a global architecture that scales up cloud computing. Another solution are edge computing systems that extends Cloud services to edge devices. This technology provides storage, computing, and some networking services between devices and Cloud infrastructure. The problem is that edge computing systems cannot provide functionalities such as complex analysis, data access to a large number of users and storing historical data which are complemented with Cloud computing [31]. Another challenge is to enable context-aware computing with scalability support. This problem emphasizes issues of object performances including storage and processing capabilities including the power consumption. A major scalability related problem is to provide a seamless connectivity to make it easy when adding new components and objects to IoT system as well as to support topology change. To solve these problems in the context of distribution scalability, mobility and security there is a CCN vision of the next generation of network architecture [130]. It enables automatic and application-neutral caching in memory wherever it is located in the network. This paradigm is still in its nascent stage and it is a very attractive research topic.

4.7. Management and self-configuration

Managing IoT applications and devices is a very critical factor for successful IoT deployments [131]. Management functionalities such as monitoring, control, and configuration are a big challenge due to IoT complexity, heterogeneity, a huge number of deployed devices and traffic demands. IoT software must be able to identify various smart objects and interact with them to provide efficient management and self-configuration functionalities. Self-configuration means IoT system has capabilities of the dynamical adoption of changes in its environment. For example, if devices could switch off when there is no activity it will provide more efficiency in energy consumption.

Data management mechanisms need to provide various functionalities such as raw data aggregation, data analytics, data recovery, and security. They need to enable a different kind of reports that include: descriptive (e.g. products' condition), diagnostic (e.g. causes of failure), predictive (e.g. expected events), etc. IoT data management framework presented in [132] includes applications (analysis) layer, query layer, federation layer, a source layer, communication layer, things layer. Also, these mechanisms need to be adaptive, scalable, and trustworthy [113]. This implies the usage of new approaches to data aggregation and complex computations to provide efficient and real-time decision-making [133]. Another challenge is to provide automatic decisions and self-configuring operations in complex, integrated and open IoT systems. Objects need to gain some knowledge from collected data and according to that performing some context-aware actions. A very interesting research topic is to automatically allocate tasks between layers of system architecture. For example, it is challenging task to determine which functions should be allocated to Fog nodes rather than Cloud infrastructure.

Network management functionalities need to provide efficiency in network topology management, devices synchronization as well as traffic and congestion control management. A new network's design needs to deploy efficient management mechanisms to manage the large-scale of connected devices, an enormous amount of data (traffic loads) and various services with different QoS requirements. Monitoring network infrastructure enables detection of any changes and events that effect on network resource usage and security. There is a need for dynamic resource management solution with a resource allocation scheme which will be effective under the uncertainty nature of IoT environment. Various protocols have been developed to monitor and control network elements such as devices, gateways, terminal servers, etc. LNMP (LoWPAN Network Management Protocol) and SNMP (Simple Network Management Protocol) are existing management protocols for IPv6 based networks [15] that perform some network management functions. Also, TSMP (Time Synchronized Mesh Protocol) is a communication protocol that enables synchronization of devices (motes) in self-organizing wireless networks. There have been proposed various novel concepts and technologies for the efficient management of networks. For example, M. A. Rajan et al. [131] proposed a novel heterogeneous and self-optimizing SN management with a flexible auto-configuration of WSNs. RANaaS (Radio Access Network as a Service) is a concept that has been developed to manage network resources and to enable flexible management [134]. SDN is an enabling technology for 5G systems [135] that has been developed to provide dynamic, flexible and automated management and reconfiguration of a network [6] as well as simplifying network design and management [136]. It enables a cost-effectively scaling necessary for IoT services. SDN and NFV (Network Function Virtualization) enable a new way of network management by providing a virtualization of some network functions to be managed through software (e.g. servers as computing platforms). Also, these paradigms provide functionalities to manage heterogeneous devices with various deployments and use-cases [137]. Although these paradigms bring new efficient network management functions there are still some open issues [138]. For example, fragmentation of APIs and controller functions in SDN is a very challenging problem which causes standardization issue. Also, it is a challenge to determine how often QoS signaling data should be sent from network to a controller component.

Devices management mechanisms need to provide monitoring and remote-control functionalities including remote devices' activation or deactivation, firmware update, etc. Some device management functionalities can be included in SBC (Single Board Computer) but for remote control, there must be deployed other mechanisms including devices and services management protocols. Managing devices and enabling seamless integration in various networks are challenges due to a deployment of various hardware and software while providing operations such as addressing and optimization at the architectural and protocol levels [139]. One of the major issues in IoT systems is the identity management of devices as well as ensuring trusted environment [140]. The OMA (Open Mobile Alliance) and its Device Management Working Group specify some protocols and mechanisms for devices and services management in resource-constrained environments such as LWM2M (The Light-weight M2M) [141]. There are some other light protocols for devices management including NETCONF Light protocol [142]. The challenge of device management is especially pronounced because of the heterogeneity among devices and associated services. There are several efforts to solve this problem such as cognitive management framework solution [110] and hardware platforms which enable integration of objects and networks with a few management functionalities. Some other open issues are related to the development of lightweight and secure IoT device management framework which provide functionalities such as location awareness, mobility, low power consumption, support for various mobile OS, etc.

4.8. Network performances and QoS

The ability to handle numerous connected devices with various services and processes depends on IoT system performances. Major issues are related to traffic loads and various traffic models [9] which have a dramatic impact on a networks' performance and QoS (Quality of Service). Some significant issues related to QoS include bandwidth, throughput, latency, etc. Also, the connected devices' growth and increased data rates in wireless networks have caused radio spectrum usage to be a critical issue [143]. Some countries might have a problem to find an additional spectrum as a spectral efficiency of radio networks is reaching its physical limits. All these facts influence on performances of IoT systems which are considered as extremely significant in most applications [144].

QoS in IoT system depends on deployed technologies, protocols, traffic demands, etc. Several studies have been done for the evaluation of IoT service performances but this is still an open issue [145]. QoE (Quality of Experience) is related to user's perception and need to be considered in some application scenarios but not in all cases. In IoT applications where QoE is not of interest than QoS – based approach could be used [146]. The most of the previous researches considered QoS parameters for IoT services while only a few studies considered QoE [147]. Due to the different traffic loads and characteristics of multiple traffic types, it is necessary to develop new models for forecasting traffic load. For example, it is needed a novel traffic model for a new-generation of SN [186]. Human-based communications (H2H and H2M) and traffic models are difficult to apply directly to IoT. Laya A. et al. [148] have presented some differs between M2M (IoT) and human-based traffic characteristics. In order to simplify traffic management, there is a need for data (traffic) aggregation science a huge diversity of traffic types and sources. Some impact of data aggregation in IoT (M2M) on QoS parameters such as delay and throughput has been surveyed in [149]. A challenge that occurs due to new traffic requirements is a need for new QoS specifications. There is a requirement for a new controlled and optimal approach for different traffic types and applications [17] as well as efficient congestion control, dynamic scheduling, resource allocation algorithms, buffering mechanisms, etc. QoS-aware scheduling mechanisms are required to support various traffic characteristics and QoS specifications [150]. Another challenge is related to QoS management while IoT devices operate under bandwidth, battery, and processing constraints [151]. Also, QoS-based service selection is the key to large-scale service-oriented IoT [152]. This is one of the major issues in the future development of IoT services due to the increasing number of services with various QoS requirements.

IoT performances depend on all components and communication protocols deployed in a system. One of the major challenges is to select the corresponding protocols for a specific use case (according to various traffic requirements) while there is no evaluation that includes all protocols and scenarios [153]. The existing surveys are mostly focused on the comparative analysis of various protocols with an aim of evaluating their performances in specific IoT scenarios. Z. Sheng et al. [154] have done a survey on protocols and technologies according to standards, challenges, and opportunities. CoAP, MQTT, XMPP, AMQP, REST and DDS protocols have been addressed as a common application layer protocols used in IoT systems [5], [153], [155]. In [32] were analyzed MQTT, AMQP, XMPP, and DDS by measuring latency and throughput rate by running on three different web platforms: HTML 5, Adobe Flash and Microsoft Silverlight. The survey [32] concluded that HTML 5 is a much more mature platform for real-time IoT applications although Adobe Flash has the best performances while Microsoft Silverlight has the poorest performances. CoAP and HTTP response time and energy consumption were analyzed by Walter C. et al. [156]. The performance evaluation of MQTT and CoAP in different use cases have been done in [107], [157]. Some performances comparisons between AMQP and RESTful have been presented by Joel L.F. et al. [158]. Some characteristics of WebSocket and HTTP while delivering real-time messages have been described in [159]. The most of the application layer protocol use some of existing transport protocols which cause several open issues such as fairness problem [189]. TCP protocol was not originally developed for wireless networks and it exhibits serious network performance degradation in these networks [160]. UDP is a lightweight protocol and is better for real-time applications but it is not reliable. Also, routing protocols need to be adopted for effective communication in IoT systems to ensure reliability and to reduce delay. Some of existing routing algorithms used in IoT systems are: RPL (Routing Protocol for Low Power and Lossy Networks), AOMDV-IoT (Ad-hoc on Demand Multipath Distance Vector), EARA (Energy Aware Ant Routing Algorithm), PAIR (Pruned Adaptive IoT Routing), SMRP (Secure Multihop Routing Protocol), REL (Routing protocol based on Energy and Link Quality), etc. IoT routing protocols can be evaluated by using many parameters such as multihop routing support, energy aware, context-aware, security support, dynamic topology support, heterogeneity support, link quality, reliability, latency, data redundancy, load balancing, scalability, routing information maintaining, etc. Routing protocols affect reliability and other performances of IoT systems as we described before. Therefore, optimizations of routing techniques, energy efficient routing protocols and developing more intelligent routing algorithms (context-aware algorithms) are very interesting research areas.

QoS performances such as latency, jitter, packet loss, and reliability have to be considered at all layers of network architecture. The corresponding option for system-level architecture and optimization of resources allocation leads to QoS improvement. Many IoT applications rely on the Cloud infrastructure to handle a huge amount of data that need to be stored and processed. However, transferring big data from the edge devices (e.g. sensors, smartphones, etc.) to the cloud infrastructure brings the following network issues: network performances (e.g. delays, bandwidth, congestion, reliability), costs of moving data through the Internet, etc. These are very challenging issues especially for latency-sensitive applications because many IoT applications require very low end-to-end latency (e.g. within a few milliseconds) and jitter. Also, Cloud computing is not sufficient to handle mobility support, geo-distribution, and real-time location-awareness. The concept of edge computing is proposed to overcome some of these challenges and limitations. It is a novel system-level architecture that distributes some resources, processes, and services to data centers which are closer to the edge of the network. For example, fog computing can provide small and deterministic latency for IoT applications which is crucial for some real-time systems. It provides better QoS in terms of better response time, jitter and throughput. Edge computing technologies enable QoS awareness by providing dynamically adaption to the available resources. However, edge computing is not tailor-made in all use cases due to computational limitations. To overcome the computational limitation, it is proposed IFCIoT (Integrated Fog Cloud IoT) architecture. Integration of IoT and Fog/Cloud computing causes some new open issues such as the metric of computation (e.g. resource and functions allocation) and development of dynamic resource allocation algorithms.

4.9. Modeling and simulation

Major challenges in developing IoT services are due to its complexity and heterogeneity in all parts of system architecture. Heterogeneous nature of applications, devices, interfaces, radio technologies, etc. leads to the IoT system modeling issue. There is no standard methodology available for modeling such real-world complex IoT-based systems [214]. Therefore, IoT system modeling for finding eligible deployments is a very challenging issue [208]. Some contributions in theoretical modeling of IoT based on edge computing was presented in [209]-[211]. However, there is lack of mathematical formulation for systems based on the integration of IoT, computing systems, and other parts of IoT system architecture. This formulation could help to design IoT system with the most appropriate technologies according to specific requirements. IoT devices are usually resource-constrained in sense of identifying, sensing, networking, computation and other capabilities. Therefore, one of the key issues is a QoS-aware deployment of IoT through the corresponding computational offloading system. Because of that, the future of IoT depends on decentralizing networks. There are different edge computing models which help to offload IoT devices and Cloud infrastructure. The most of IoT applications rely on the support of some computing systems which are the part of IoT system architecture. Even though cloud computing supports the development of IoT applications this model is facing many challenges such as network delays, cost of transferring raw data through the Internet, etc. Therefore, some IoT applications require a new computing model to support the ubiquitous deployment of sensors and other devices. These systems are part of paradigms known as Fog computing, MCC, MCC, and Cloudlet. They are based on an allocation of resources between data sources and cloud infrastructure. However, there is a challenge of determining which functions should be allocated to edge nodes rather than Cloud [128]. The allocation of tasks between layers of system architecture needs to be enabled dynamically based on the system resource state [207]. Using an appropriate model of integration of IoT and computing systems can reduce the amount of data that need to be transmitted to the cloud infrastructure over the Internet. This improves QoS performances as well as reduces resource consumption and costs.

Simulation tools such as Opnet, NS-3, Cloudsim, and others can be used for understanding and modeling the IoT system. However, the complexity and heterogeneity of IoT scenarios complicate these processes [211]. This imposes the use of sophisticated, hybrid and multi-level modeling and simulation techniques [212]. An overview of some other modeling and simulation challenges have been presented in paper [213]. For example, one of the major issues in existing simulation tools is lack of integrated options to simulate network and cloud infrastructure to obtain overall performance of IoT system. Also, there is a problem of simulating various protocols, security attacks, computing and other IoT processes in order to obtain different results such as network performances, energy consumption, etc. Another important issue is enabling simulation of IoT scenarios which include a large number of heterogeneous devices with various traffic loads and types. This implies that the problem of simulating IoT scenarios is not only related to software tools but also hardware performances have to provide enormous resources such as CPU, RAM, etc. According to previous considerations, a new enhancement of simulation tools should improve the ability to simulate small, medium, and large-scale IoT scenarios. Simulation and modeling tools need to support a dynamic nature of IoT, real-time requirements and increasing processing requirements. These scenarios include deployment of heterogeneous technologies. To address these shortcomings there is a need for the continuous enhancement of simulation and modeling tools.

4.10. Unique Identification

Each IoT object needs to have a unique identifier such as IP address or URI (*Uniform Resource Identifier)* and this is considered as one of the most critical factors for IoT success [17]. Appropriate identity management with unique identifiers and efficient key distribution schemes are issues highlighted in [140], [161]. If each object has a unique identifier and connection to the Internet than objects can be monitored, controlled and managed throughout the entire lifecycle. In that context, it must be differentiated objects ID and its network address (IPv4 or IPv6). Also, some objects need to have multiple identifiers while sensors, actuators, and other parts are attached to them. The most critical features related to addressing schemes such as uniqueness, reliability, persistence and scalability are described in paper [17].

There are many identification methods and technologies for IoT objects such as EPC (Electronic Product Code), uCode (Ubiquitous codes), QR (Quick Response) or matrix barcodes, etc. EPCglobal is an organization which efforts are in the field of standardization and integration EPC with RFID technology. Registration, unique identification and discovery in a context-aware way of IoT devices are issues that require future researches.

IPv4 have got exhausted and it is challenge to provide a unique network address to all objects. The solution for this problem is IPv6 that uses 128-bit addresses which provide a huge amount of addresses. IPv6 is considered as one of the key enablers for IoT. Integration of IPv6 and its related protocols into constrained capabilities of WSN is identified as one of its major challenges [15].

Because of scalability issues, a manual and static management of system resources is not an appropriate solution. To solve this problem, it can be used some of service discovery protocols such as DNS-SD, SSDP, SLP, mDNS, APIPA, etc. These protocols can be grouped by their function as we described before. However, there is a challenge to adapt these protocols for IoT services [162] because of requirement for autonomous registration. Discovery functionality need be dynamically adapted with the inclusion of new IoT devices in the network. Therefore, IoT architecture should enable to devices to join or leave IoT platform without affect to all IoT system and this is another open issue for network architecture which need to support IoT services.

4.11. Power and energy consumption

Power and energy storage technologies need to meet various IoT requirements such as providing energy sources for small embedded devices. Supplying reliable power to the sensors and devices as well as developing low-power chipsets is highlighted as a very challenging problem [2]. Wireless power technologies can transmit power at some distance and this is promising solution but we are being still in the early phase of development of these technologies. Another significant challenge is to integrate large computation with small embedded devices that have low power consumption particularly in the case of image and video processing-based applications. Lanzisera et al. [163] highlighted the challenge of producing low-cost terminal with low active power. One of the major issues is improving device's capabilities (e.g. computation and networking) while reducing both costs of devices and power consumption. Also, a low power communication stack is identified as one of the core requirements related to power and energy efficiency [35].

Existing communication protocols such as HTTP and TCP are not optimized for IoT as not considered to be deployed in low-power systems. Energy efficient MAC protocol and appropriate routing protocol are identified as critical factors for the system to be efficient [17]. Standardization bodies such as ITU-T, IETF, ISO, IEEE, etc. have defined a several protocols and interfaces on the low communication stack layer but the actual deployments of such features are still not satisfactory. One of the proposed solutions is IEEE 802.15.4 [55] and its improvements such as IEEE 802.15.4e. This standard defines PHY and MAC layers for the low-power but it is still ill-suited for low-power multi-hop networks as explained in [35]. This is another open issue where future effort should improve the capability of IEEE 802.15.4 low-power radio technology. Another research area includes optimization of routing techniques to reduce energy requirements and optimize energy consumption. For example, elimination of data redundancy will reduce energy requirements for data routing. There are some new technologies such as networking paradigm known as IoNT (Internet of Nano-Things) that can decrease the power consumption but it is still in nascent phase of development.

4.12. Security and privacy

Security and privacy issues are identified as key challenges in deployment of IoT solutions [31] because there are numerous examples of threats, vulnerabilities and risks [164]. Several security models and threats taxonomy models for the IoT systems have been proposed [165], [166]. According to Hewlett Packard Enterprise Research study [167], most of the devices privacy concerns raised due to: insufficient authentication and authorization, lack of transport encryption, insecure web interface, insecure software and firmware, etc. In Fig. 6. we present the most common IoT security and privacy related issues.

To provide confidence in IoT systems security and privacy need to be considered from various aspects including legal, social and cultural point of view [168]. Security functionalities need to be embedded at every level of IoT architecture and efficient trust management [169], [170] must be deployed. This is the reason why IoT security architecture is still evolving [171] [192] as well as various mechanisms being developed to improve security and privacy. Security mechanisms should provide authentication, access control, data integrity and privacy, encryption and other capabilities while enabling automatic data processing based on the policies and rules configured by users. These mechanisms must operate in real-time and they need to be cost effective and scalable to minimize the complexity and maximize usability. One key issue is lacking a solution for IoT IITP (Identity Theft Prevention) [171] consequently authorization scheme for IoT which needs to be context-aware. For example, IoT objects should be aware of location in order to provide robust security. Also, security issues are more emphasized in a heterogeneous environment and because of the standardization perspective of data exchange [172]. The most of security issues are related to communication threats such as: Malicious Code Injection, Sniffing Attack, Spear-Phishing Attack, DoS (Denial-of-Service Attack), Sybil Attack, Proxy Attack, Sleep Deprivation attack, etc. Because of these attacks various mechanisms must be deployed such as: authorization, authentication, encryption, anti-virus protection, etc. Although these mechanisms improve security level in IoT systems there are many issues that still need to be considered. For example, *proxy attack* or *man-in-the-middle attack* can occur regardless that the transmitted signal is encrypted or not.

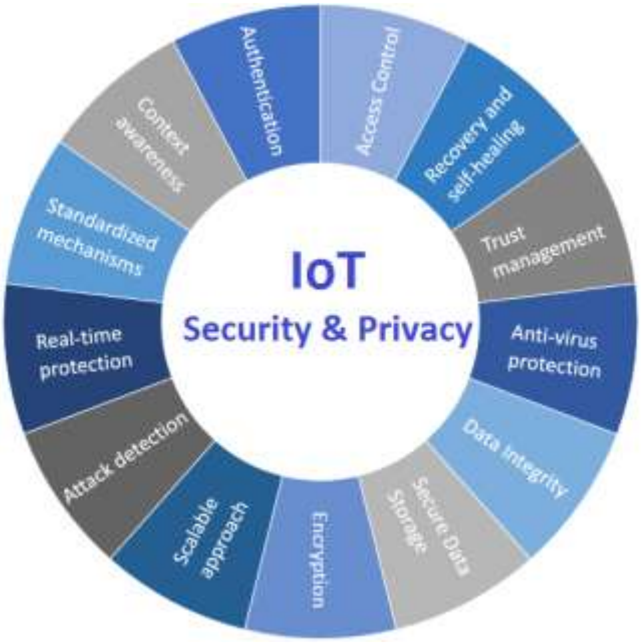


Fig. 6. IoT security and privacy issues

IoT systems require reliable and secure communication protocols at all protocol stack layers. There are three main solutions to provide security at application layer. The best solution to provide superior security properties is to develop a custom application layer security protocol but design of such protocol is very complex. Some standards and protocols such as OTrP (Open Trust Protocol) [173] are used by applications to install, update, and delete applications as well as to manage security configuration. Another solution for enhancement of security is to use IPSec (Internet Protocol Security) but it is not suitable for all IoT applications and it is much easier to run the protocol over TLS (Transport Layer Security) [174] which provide a transparent connection-oriented channel. Some IoT application protocols use other specific methods to enhance security but the most of security solutions rely on cryptography protocols such as SSL (Secure Sockets Layer) and DTLS (Datagram Transport Layer Security). These protocols are implemented between the application layer and the transport layer of TCP/IP protocol stack. TLS must run over a reliable transport channel (typically TCP) but some IoT applications prefer to use UDP. Thus, a datagram-compatible variant of TLS is required. DTLS [175] is a protocol based on TLS which provides equivalent security guarantees for datagram protocols. Security protocols use various mechanisms and standards such as X.509 which is used to manage digital certificates and public-key encryption in TLS. CoAP use DTLS while a compressed version of DTLS is used in Lightweight Secure CoAP for the IoT. XMPP and AMQP for security purpose use TLS and SASL (Simple Authentication and Security Layer). MQTT application protocol is mostly based on leveraging TLS/SSL [5] but there are some other solutions such as OASIS MQTT that uses Cyber security framework or a new secure MQTT mechanism named AUPS (AUthenticated Publish&Subscribe) [190].

Security risk emphasizes more when IoT system uses wireless communications technologies as well because of the system openness, physical accessibility to some components such as sensors, etc. There should be deployed mechanisms for malicious activities' detection and mechanisms for recovery (self-healing). IPSec provide end-to-end security at the network layer and it can be used with various transport protocols. Link layer security is limited to provide secure communication between devices [171] while effective algorithm for encryption must be used. Encryption is one of the key elements of ensuring information security but is a very challenging issue to encrypt large volumes of real-time that data needs to be transferred. Encryption algorithm needs to be efficient in power consumption. It is a very challenging task to implement complex schemes for improving security in the environment where IoT components should deploy a low energy. Very interesting research area includes interoperable lightweight protocols and encryption algorithms for better security in IoT environment.

Beside various mechanisms, it is needed appropriate policies to protect privacy and make sure all users feel comfortable using IoT solutions. Privacy policies need to allow some dynamic changes due to changes in the IoT environment. One of the key challenges is due to an openness of and interoperability of system with others while each system has its own privacy policies. Each object in an IoT system should be able to check the other’s privacy policies for compatibility before sharing data [161]. The privacy policies for infrastructure and applications must be specified by users (human entities – data owners or physical entities - things). Also, one of crucial factors is a management policy to guarantee a good level of security [190].

4.13 Environmental issues

Internet of Things has both positive and negative impacts on the environment. Every day there is more and more devices that are being deployed thus “environmental friendliness” is a topic that should be given more attention in future research. Environmental sustainability is one of the greatest concern due to increasing energy demands and electronic waste. Examples of interesting research topics are: reduce energy consumption, use renewable sources of energy, reduce a size of devices to decrease the amount of no degradable materials, various effects on human health, etc. The Internet consumes up to 5% of the total energy [17] with more and more demands and this is another issue to be considered in the future development of IoT-based systems. New green ICT enabling technologies with general green ICT principles must be deployed in the development of IoT systems [13], [176], [177]. However, IoT is providing some new ways to solve many environmental problems. One of the most common use of IoT technologies is to provide an innovative way to address these issues. IoT provide a great potential for developing new solutions for environmental sustainability such as IoT monitoring systems [187]. This is research field unprecedented opportunities for future development.

5. Future research

The main scope of this paper is to provide a comprehensive overview of IoT open issues and challenges. In this Section, we provide some insights into specific emerging issues and ideas to be tackled by the future research. Analysis of recent contributions and research papers show that the most of challenges arise due to increased traffic demands with various traffic types, greater variance in data formats, variety of IoT devices, heterogeneous networks, etc. All these indicators have a dramatic impact on IoT system performances. There are specific application demands in sense of computing and communication capabilities, QoS, mobility, reliability, privacy and security, etc. To meet these requirements, IoT applications rely on other systems such as Cloud computing. There are some other systems based on Cloud technologies such as fog computing, cloudlets, MEC, MCC, that can be considered as a part of IoT system architecture. The most of current IoT applications and services are cloud-based where smart devices exchange data with Cloud infrastructure to provide services. This model is facing many challenges such as technical limitations (e.g. network delays, throughput, reliability), economic considerations (e.g. cost of transferring data to the Cloud), and some other challenges originated from social and administrative aspects. Therefore, a new computing paradigm is needed to support emerging IoT applications. During the last year's there have been proposed several architectures and computing paradigms which deploy infrastructure closer to the source of data such as fog computing, cloudlets, MEC, MCC, etc. The distinction between these paradigms lies in the "infrastructure distance" from the IoT objects, type of infrastructure where functions are allocated, etc. Cloud computing capabilities outclass the storage and computing capabilities of the infrastructure at the edge of the network. It can be used for long-term operations such as data storage and pattern analysis. However, the integration of IoT and Cloud computing is not efficient for all IoT applications due to inherent problems such as unacceptable delay, lack of mobility support, location-awareness, security and privacy issues, etc. Deploying edge computing systems helps to overcome some issues. For example, they help to reduce costs of data transferring as well as to improve system performances such as QoS. However, there are some bottlenecks for each model of integration and using the corresponding architecture of integrating IoT and computing systems can alleviate some of the major limitations of IoT systems. The key questions are “which model of integration to choose and which functions to allocate to the IoT devices, edge, and cloud systems”, “how to enable interaction between these subsystems”, and “which technologies to deploy for the development of the IoT system”? These questions put in light IoT system modeling issue.

In order to select the corresponding model of IoT and computing systems integration, there is a need for a modeling methodology. However, there is a lack of mathematical formulation and evaluation methods which include multiple metrics. Contribution in this emerging research field could help in finding eligible deployments for any part of IoT system architecture. Therefore, it is required to propose a comprehensive IoT model which include all possible architectures, technologies, and integration possibilities. Also, there is a requirement for a quantitative method of evaluating IoT system performances. This method could be used for selecting the corresponding integration model and technologies as well as for creating performance-based profiles of IoT applications. There are many possible metrics for quantitative analysis which can be used for creating IoT application profiles including power consumption, computation metrics including CPU metrics, RAM usage, network-related metrics including network latency, throughput, packet loss, etc. Most of the previous studies are based on analysis of individual metric observed on the specific use case. There is lack of approaches which integrate more than one metric in order to allow more comprehensive evaluation of IoT systems. This is another challenge that needs to be addressed for future research. Therefore, the evaluation method should include multiple metrics to enable a resource optimization as well as finding eligible and QoS-aware deployment of various architectures, interaction models, and technologies. It could be based on an algorithm which will enable to optimize the load distribution between IoT subsystems. By using this kind of evaluation, it could be possible to propose a classification scheme for IoT application according to their performance profile (e.g. QoS requirements). Also, this evaluation method could enable evaluation of different application designs and resource management policies. Also, this method could be used for QoS and QoE evaluation as well as for IoT system modeling. Adequate mathematical formulation of IoT system and evaluation methods can break through the future development.

6. Conclusion

IoT needs to enable a seamless connectivity anytime, anywhere by anyone and anything to provide intelligent services including identifying, sensing, networking, processing and visualization capabilities. This concept brought many new possibilities for large-scale services and products development which caused a massive wave of innovations and new business opportunities. Various visions and approaches, as well as the lack of coordination between standards and technologies, lead to the fragmentation of IoT industries which cause a set of new challenges to be tackled by future research. IoT-based solutions have become more advanced and sophisticated while there is no a comprehensive framework with integrated all standards and technologies. This open several issues which arise due to an increasing number of connected devices, integration of various technologies, increased traffic demands with new traffic models, raw data storage and processing demands, privacy and security risks, etc. This paper clarified different IoT visions and definitions on the basis of referenced literature. Also, the paper provides insights into the IoT enabling technologies by presenting the functional domains with key utility factors. Besides existing solutions, there are many emerging technologies which empowers IoT systems with numerous of new capabilities and functionalities. This paper summarized the current state-of-the-art of IoT enabling and emerging technologies in order to provide a comprehensive list of open issues with some details. Furthermore, this is used to provide some future research directions. We performed the classification of previous research and present a literature pool to bring order in the literature by classifying existing works according to different research areas. Therefore, this paper is mostly focused on issues related to the IoT enabling and emerging technologies.

New IoT applications and emerging technologies bring new challenges that require attention from the research community. We have summarized and discussed these issues and outlined the main challenges by envisioning perspectives for the most attractive future research topics and developments. One of the most attractive future research topics is related to the integration of IoT with emerging technologies such as hybrid cloud platforms, MCC, MEC, fog, and cloudlet, nano technologies, etc. These solutions can breakthrough future development of IoT with a new architecture known as Cloud of Things or even beyond in a paradigm known as IoNT (Internet of Nano-Things). Combining these technologies by enabling cross-domain integration with existing web technologies in a concept called WoT (Web of Things) provides an even wider spectrum of new capabilities and functionalities. However, despite the enormous research efforts many open issues and challenges remain. We highlight these issues such as IoT system modeling and requirement for a quantitative method of evaluating system performances. A brief overview of interesting research topics, a classification of open issues according to proposed functional domains and insights into specific emerging issues and ideas facilitate the future research. Therefore, this paper is valuable to the research community as it can be used as a starting point for future research.

References

[1] D. Singh, G. Tripathi, A. J. Jara, “A Survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services,“ *In Proc. IEEE World Forum on Internet of Things 2014*, At Seoul, 2014, pp. 287–292.

[2] M. H. Miraz, M. Ali, “A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet of Nano Things (IoNT),” *In Proc. Internet Technologies and Applications (ITA)*, 2015, pp. 219 – 224.

[3] M. Condoluci, G. Araniti, T. Mahmoodi; M. Dohler, “Enabling the IoT Machine Age With 5G: Machine-Type Multicast Services for Innovative Real-Time Applications, “*IEEE Access*, vol. 4, pp. 5555 – 5569, May 2016.

[4] A. Gupta, R. K. Jha, “A Survey of 5G Network: Architecture and Emerging Technologies,“ *IEEE Access*, vol. 3, pp. 1206 – 1232, Jul. 2015.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,“ *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347 – 2376, Jun. 2015.

[6] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, L. Ladid, “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models,“ *IEEE Journal on Selected Areas in Communications*,vol. 34, no. 3, pp. 510 – 527, Feb. 2016.

[7] C. Sarkar, Akshay Uttama Nambi S. N, R. V. Prasad, A. Rahim, R. Neisse, G. Baldini, "DIAT: A Scalable Distributed Architecture for IoT," *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 230 – 239, Dec. 2014.

[8] M. Kim, H. Ahn, K. P. Kim, “Process-Aware Internet of Things: A Conceptual Extension of the Internet of Things Framework and Architecture,“ *KSII Transaction on Internet and Information systems*, vol. 10, no. 8, Aug. 2016.

[9] E. Soltanmohammadi, K. Ghavami, M. Naraghi-Pour, “A Survey of Traffic Issues in Machine-to-Machine Communications Over LTE,“ *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 865 – 884, Feb. 2016.

[10] G. Aloi, G. Caliciuri, G. Fortino, R. Gravina, P .Pace, W. Russo, C. Savaglio, “Enabling IoT interoperability through opportunistic smarthpone based mobile gateways,“ *Journal of Network and Computer Applications*, pp. 74-84, vol. 81, Mar. 2016.

[11] B. Soret; K. I. Pedersen; N. T. K. Jorgensen; V. Fernández-López, “Interference coordination for dense wireless networks,“ *IEEE Communications Magazine*, vol. 53, no. 1, pp. 102 – 109, Jan. 2015.

[12] J. G. Andrews, “Seven ways that HetNets are a cellular paradigm shift,“ *IEEE Communications Magazine*, vol. 51, no. 3, pp. 136 – 144, Mar. 2013.

[13] C. Zhu; V. C. M. Leung; L. Shu; E. C.-H. Ngai, “Green Internet of Things for Smart World,“ *IEEE Access*, vol 3, pp. 2151 – 2162, Nov. 2015.

[14] F. Paganelli, D. Parlanti, “A DHT-Based Discovery Service for the Internet of Things,” *Journal of Computer Networks and Communications*, vol. 2012, Sep. 2012.

[15] N. Benamar; A. Jara; L. Ladid; D. E. Ouadghiri, “Challenges of the Internet of Things: IPv6 and Network Management,“ *In Proc. Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2014, pp. 328 - 333

[16] L. Atzori, A. Iera, G. Morabito, “The Internet of Things: A Survey,“ *Computer networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[17] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,“ *Future Generation Computer Systems*, pp. 1645–1660, Feb. 2013.

[18] J. A. Stankovic, “Research directions for the internet of things,“ *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, Mar. 2014.

[19] *Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks, Next Generation Networks – Frameworks and functional architecture models: Overview of the Internet of things*, ITU-T Recommendation Y.2060 Series Y, 2012.

[20] *Internet of Things (IoT)*, ISO/IEC JTC 1 Information Technology, Preliminary Report, 2014.

[21] *Architectural Considerations in Smart Object Networking*, IETF RFC 7452, Mar. 2015.

[22] *Internet of Things in 2020, A Roadmap for the Future*, INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in Co-operation with the RFID Working Group of the ETP EPOSS Version 1.1, 27 May 2008.

[23] S. Chen; H. Xu; D. Liu; B. Hu; H. Wang, “A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective,“ *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 349 – 359, Jul. 2014.

[24] A. Whitmore, A. Agarwal, L. D. Xu, ”The Internet of Things — A survey of topics and trends," *Inf Syst Front*, pp. 261-274, Mar. 2014.

[25] Oxford Dictionaries, Jan. 2017. [Online]. Available: http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things

[26] S. Sebastian, P. P. Ray, “Development of IoT invasive architecture for complying with health of home,” *in Proc International Conference on Computing and Communication Systems (I3CS '15)*, Shillong, India, Apr. 2015, pp. 79–83.

[27] H2020 – UNIFY-IoT Project, “Supporting Internet of Things Activities on Innovation Ecosystems,” Report on IoT platform activities, Oct. 2016. [Online]. Available: http://www.unify-iot.eu/wp-content/uploads/2016/10/D03_01_WP02_H2020_UNIFY-IoT_Final.pdf

[28] A. Gluhak; S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, “A survey on facilities for experimental internet of things research,“ *IEEE Communications Magazine*, vol. 49, no. 11, pp. 58 – 67, Nov. 2011.

[29] K. Gama, R. Wanderley, D. Maranhao, V. C. Garcia, “A Web-based platform for scavenger hunt games using the Internet of Things,“ *In Proc 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015, pp. 597 - 598

[30] H-C. Hsieh, K-D. Chang, L-F- Wang, J-L. Chen, H-C. Chao, “ScriptIoT: A Script Framework for and Internet-of-Things Applications,“ *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 628 - 636, Sep. 2015.

[31] Z. B. Babovic, J. Protic, V. Milutinovic, “Web Performance Evaluation for Internet of Things Applications,“ *IEEE Access*, vol. 4, pp. 6974 - 6992, Oct. 2016.

[32] M. Díaz, C. Martín, B. Rubio, “State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing,“ *Journal of Network and Computer Applications*, vol. 67, no. C, pp. 99-117, May 2016.

[33] *MT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, ITU-R Recommendation M.2083-0, Sep. 2015.

[34] IoT-A (Internet-of-Things Architecture), “Initial Architectural Reference Model for IoT,” Project Deliverable D1.2, Jun. 2011.

[35] 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," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp.1389 – 1406, Dec. 2012.

[36] Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol (CoAP),“ *IETF RFC 7252*, Jun. 2014, [Online]. Available: https://tools.ietf.org/html/rfc7252

[37] *MQTT (Message Queue Telemetry Transport), OASIS Standard*, Oct. 2014. [Online]. Available: http://mqtt.org/2014/11/mqtt-v3-1-1-now-an-oasis-standard

[38] P. Saint-Andre, “Extensible messaging and Presence Protocol (XMPP): Core,” *IETF RFC 6120*, Mar. 2011. [Online], Available: https://tools.ietf.org/html/rfc6120

[39] P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence,” Mar. 2011. [Online], Available https://tools.ietf.org/html/rfc6121

[40] *Advanced Message Queuing Protocol (AMQP), OASIS Standard*, Oct. 2012. [Online]. Available: https://www.amqp.org/

[41] *Data distribution services specification*, Object Manage. Group (OMG), Needham, MA, USA, Apr 2015. [Online]. Available: http://www.omg.org/spec/DDS/1.2/

[42] I. Fette, A. Melnikov, “The WebSocket Protocol,“ *IETF RFC 6455*, Dec. 2011. [Online]. Available: https://tools.ietf.org/html/rfc6455

[43] J. Postel, "Transmission Control Protocol," *IETF RFC 793*, Sep. 1981. [Online]. Available: https://tools.ietf.org/html/rfc793

[44] J. Postel, "User Datagram Protocol,” *IETF RFC 768*, Aug. 1980. [Online]. Available: https://www.ietf.org/rfc/rfc768.txt

[45] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” *IETF RFC 2460*, Dec. 1998. [Online]. Available: https://tools.ietf.org/html/rfc2460

[46] A. J. Jara, L. Ladid, A. Skarmeta, “The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities,“ *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 4, no. 3, pp. 97-118 , Sep. 2013.

[47] T. Winter *et al*., “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks“, IETF RFC 6550, Mar. 2012. [Online]. Available: https://tools.ietf.org/html/rfc6550

[48] L Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, L. Tarricone, “An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515 - 526, Mar. 2015.

[49] L. Chunli, L. Donghui, “Application and development of RFID technique," *In Proc. 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, pp. 900–903.

[50] Y. Choi, Y. Choi, D. Kim; J Park, “Scheme to guarantee IP continuity for NFC-based IoT networking,", *In Proc. 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 695 – 698.

[51] - N. Kushalnagar, G. Montenegro, and C. Schumacher, “IPv6 over LowPower Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals,” *IETF RFC 4919*, Aug. 2007. [Online]. Available: https://tools.ietf.org/html/rfc4919

[52] Montenegro et al., “Transmission of IPv6 Packets over IEEE 802.15.4 Networks," *IETF RFC 4944*, Sep. 2007, [Online]. Available: https://tools.ietf.org/html/rfc4944

[53] J. Hui, P. Thubert, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," *IETF RFC 6282*, Sep. 2011. [Online]. Available: https://tools.ietf.org/html/rfc6282

[54] B. Campbell, H. Tschofenig, “An IETF URN Sub-Namespace for OAuth," *IETF RFC 6755*, Sep. 2007. [Online]. Available: https://tools.ietf.org/html/rfc6755

[55] *802. 15. 4 IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard - WG802.15, 2011.

[56] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, M. Mohammadi, “Toward better horizontal integration among IoT services," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 72 – 79, Sep. 2015.

[57] *Bluetooth Core Specification*, Bluetooth Special Interest Group (SIG), 2016. [Online]. Available: https://www.bluetooth.com/specifications/bluetooth-core-specification

[58] S. Raza, P. Misra, Z. He, T. Voigt, “Bluetooth smart: An enabling technology for the Internet of Things,“ *In Proc. IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct. 2015, pp. 155 – 162.

[59] J. DeCuir, “Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies,“ *IEEE Consumer Electronics Magazine*, vol. 3, no. 1, pp. 12 - 18, Jan. 2014.

[60] R. Frank, W. Bronzi, G. Castignani, T. Engel, “Bluetooth Low Energy: An alternative technology for VANET applications,“ *In Proc. 11th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, 2014, pp. 104 – 107.

[61] E. Mackensen, M. Lai, T. M. Wendt, “Bluetooth Low Energy (BLE) based wireless sensors,“ *In Proc. Sensors, 2012 IEEE*, Oct. 2012, pp. 1 - 4

[62] M. O. Al Kalaa, W. Balid, N. Bitar, H. H. Refai, "Evaluating Bluetooth Low Energy in realistic wireless environments," *In Proc. IEEE Wireless Communications and Networking Conference*, Apr. 2016, pp. 1 - 6.

[63] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby and C. Gomez, “IPv6 over bluetooth(r) low energy,“ IETF 6Lo Working Group, Aug. 2015. [Online]. Available: https://tools.ietf.org/html/draft-ietf-6lo-btle-17

[64] T. Adame, A. Bel, B. Bellalta, J. Barcelo, M. Oliver, “IEEE 802.11AH: the WiFi approach for M2M communications,“ *IEEE Wireless Communications*, vol. 21, no. 6, pp. 144 – 152, Jan. 2014.

[65] E. Khorov, A. Krotov, A. Lyakhov, “Modelling machine type communication in IEEE 802.11ah networks,“ *In Proc. IEEE International Conference on Communication Workshop (ICCW)*, Jun. 2015, pp. 1149 - 1154

[66] U. Raza, P. Kulkarni, M. Sooriyabandara, “Low Power Wide Area Networks: An Overview,“ *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1 - 1, Jan. 2017.

[67] M. Hasan, E. Hossain, D. Niyato, “Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches,“ *IEEE Communications Magazine*, vol. 51, no. 6, pp. 86 – 93, Jun. 2013.

[68] M. N. Tehrani, M. Uysal, H. Yanikomeroglu, “Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions,“ *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86 - 92, May 2014.

[69] M. Jaber, M. A. Imran, R. Tafazolli, A. Tukmanov, “5G Backhaul Challenges and Emerging Research Directions: A Survey,“ *IEEE Access*,vol. 4, pp. 1743 - 1766, Apr. 2016.

[70] U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal: „A Review on Internet of Things (IoT),“ *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1-7, Mar. 2015.

[71] N. Lin, W. Shi, “The research on Internet of things application architecture based on web,” *In Proc. Advanced Research and Technology in Industry Applications (WARTIA), IEEE Workshop*, Sep. 2014, pp. 184-187.

[72] Noboru Koshizuka; Ken Sakamura: "Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things," IEEE Pervasive Computing, 2010, Volume: 9, Issue: 4, Pages: 98 - 101

[73] H. van der Veer, A. Wiles, “Achieving Technical, Interoperability - the ETSI Approach,” *ETSI White Paper No. 3*, Apr. 2008. [Online]. Available: http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf

[74] P.P. Ray, “A survey on Internet of Things architectures,“ *Journal of King Saud University – Computer and Information Sciences*, pp.1319-1578, Oct. 2016.

[75] *Machine-to-Machine communications (M2M); Functional architecture*, ETSI TS 102 690, 2011.

[76] *Machine-to-Machine communications (M2M); M2M Service Requirements*, ETSI TS 102 689, 2013.

[77] *P2413 - Standard for an Architectural Framework for the Internet of Things (IoT),* BOG/CAG - Corporate Advisory Group, BOG - IEEE-SA Board of Governors, Active Project.

[78] *Technical Report on IoT Reference Architecture,* GISFI TR 06.001, 2012.

[79] A. H. Alhamedi, V. Snasel, H. M. Aldosari, A. Abraham, "Internet of things communication reference model," *In Proc. 6th International Conference on Computational Aspects of Social Networks*, Aug. 2014. pp. 61 – 66.

[80] O. Vermesan, P. Friess, “Scalable Integration Framework for Heterogeneous Smart Objects, Applications and Services”, in *Internet of Things – From Research and Innovation to Market Deployment,* River Publishers Series in Communications, Denmark, 2014, pp. 225-239.

[81] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C-T. Lin, X. Liu, “Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects,” *IEEE Access*, vol. 4, pp. 5356 - 5373, Sep. 2016.

[82] H. Hada, J. Mitsugi, “EPC based internet of things architecture,“ *In Proc. IEEE International Conference on RFID-Technologies and Applications*, Sep. 2011, pp. 527 – 532.

[83] M. Yun, B. Yuxin, “Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid,” *In Proc. International Conference on Advances in Energy Engineering*, 2010, pp. 69 – 72.

[84] A. P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, “Architecture and protocols for the Internet of Things: A case study,“ *In Proc. 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2010, pp. 678 – 683.

[85] S. Hong, D. Kim, M. Ha, S. Bae, S. J. Park, W. Jung, J. Kim, “SNAIL: an IP-based wireless sensor network approach to the internet of things,“ *IEEE Wireless Communications*, vol. 17, no. 6, pp. 34 – 42, Dec. 2010.

[86] F. Andreini, F. Crisciani, C. Cicconetti, R. Mambrini, “Context-aware location in the Internet of Things," *In Proc. 2010 IEEE Globecom Workshops*, 2010, pp. 300 – 304.

[87] G. Pujolle, “An Autonomic-oriented Architecture for the Internet of Things,” *In Proc. Modern Computing, 2006. IEEE JVA '06*, Oct. 2006.

[88] S. Guoqiang, C. Yanming, Z. Chao, Z. Yanxu, “Design and Implementation of a Smart IoT Gateway," *In Proc. IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2013, pp. 720 – 723.

[89] I. Ishaq, J. Hoebeke, I. Moerman, P. Demeester, “Internet of Things Virtual Networks: Bringing Network Virtualization to Resource-Constrained Devices,” *In Proc. IEEE International Conference on Green Computing and Communications*, 2012, pp. 293 – 300.

[90] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, N. Venkatasubramanian, “A Software Defined Networking architecture for the Internet-of-Things,” *In Proc. IEEE Network Operations and Management Symposium (NOMS)*, 2014, pp. 1 – 9.

[91] G. C. Fox, S. Kamburugamuve, R. D. Hartman, “Architecture and measured characteristics of a cloud based internet of things,“ *In Proc. International Conference on Collaboration Technologies and Systems (CTS)*, 2012, pp. 6 - 12

[92] A. P. Castellani, M. Dissegna, N. Bui, M. Zorzi, “WebIoT: A web application framework for the internet of things,“ *In Proc. IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2012, pp. 202 – 207.

[93] *Constrained RESTful Environments (Core)*, IETF Working Group, [Online]. Available: http://www.ietf.org/dyn/wg/charter/core-charter.html.

[94] B. Upadhyaya, Y. Zou, H. Xiao, J. Ng, A. Lau, “Migration of SOAP-based services to RESTful services,“ *In Proc. 13th IEEE International Symposium on Web Systems Evolution (WSE)*, 2011, pp. 105 – 114.

[95] D. Guinard, V. Trifa, E. Wilde, “A resource oriented architecture for the Web of Things,“ *In Proc. Internet of Things (IoT)*, Dec. 2010, pp. 1 – 8.

[96] A. H. H. Ngu; M. Gutierrez; V. Metsis; S. Nepal; M. Z. Sheng, “IoT Middleware: A Survey on Issues and Enabling technologies,“ *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1 - 1, Oct. 2016.

[97] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, S. Clarke, “Middleware for Internet of Things: A Survey,“ *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70 - 95, Feb. 2016.

[98] I. Grønbæk, „Architecture for the Internet of Things (IoT): API and Interconnect,” *In Proc. Second International Conference on Sensor Technologies and Applications (sensorcomm*), 2008, pp. 802 – 807.

[99] B. Cheng, D. Zhu, S. Zhao, J. Chen, "Situation-Aware IoT Service Coordination Using the Event-Driven SOA Paradigm", *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 349 – 361, Mar. 2016.

[100] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. M. Sá de Souza, V. Trifa, “SOA-Based Integration of the Internet of Things in Enterprise Services,” *In Proc. IEEE International Conference on Web Services*, 2009, pp. 968 – 975.

[101] Z. J. Muhsin, A. Al-Taee, M. A. Al-Taee, W. Al-Nuaimy, A. Al-Ataby, “Mobile workflow management system based on the Internet of Things,” *In Proc. 13th International Multi-Conference on Systems, Signals & Devices (SSD)*, 2016, pp. 436 – 441.

[102] F. Kawsar, G. Kortuem, B. Altakrouri, “Supporting interaction with the Internet of Things across objects, time and space,” *In Proc. Internet of Things (IoT)*, 2010, pp. 1 – 8.

[103] A. Bhavana, “Evaluating Perception, Characteristics and Research Directions for Internet of Things (IoT): An Investigational Survey,” *International Journal of Computer Applications*, vol. 121, no. 4, pp. 13-19, Jul. 2015.

[104] B. Soret; K. I. Pedersen; N. T. K. Jorgensen; V. Fernández-López, “Interference coordination for dense wireless networks,“ *IEEE Communications Magazine*, vol. 53, no. 1, pp. 102 - 109, Jan. 2015.

[105] *1905.1-2013 - IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies,* IEEE Standard, 2013.

[106] S. Aguzzi et al., “Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination,” *A study prepared for the European Commission – Final Report*, pp. 64-67, 2014.

[107] C. Pereira, A. Aguiar, “Towards Efficient Mobile M2M Communications: Survey and Open Challenges,” *Sensors*, vol, 14, no. 10, pp. 19582-19608, Oct. 2014,

[108] J. Santos, J. Rodrigues, B. M. Silva, J. Casal, K. Saleem, V. Denisov, “An IoT-based mobile gateway for intelligent personal assistants on mobile health environments,” *Journal of Network and Computer Applications*, vol. 71, pp. 194–204, Mar. 2016.

[109] G.Aloi, M. Di Felice, V. Loscri, P. Pace, G. Ruggeri, “Spontaneous smartphone networks as a user-centric solution for the future internet,” *IEEE Communications Magazine*, vol. 52, no. 12, pp. 26 – 33, Dec. 2014.

[110] P. Vlacheas, et al., “Enabling smart cities through a cognitive management framework for the internet of things,“ *IEEE Communications Magazine*, vol. 51, no. 6, pp. 102 - 111, Jun. 2013.

[111] M. Blackstock, R. Lea, “IoT interoperability: A hub-based approach,“ *In Proc. International Conference on the Internet of Things (IoT)*, 2014, pp. 79 – 84.

[112] L. E. Talavera, et al., “The Mobile Hub concept: Enabling applications for the Internet of Mobile Things,“ *In Proc. IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2015, pp. 123 – 128.

[113] I-R. Chen, J. Guo, F. Bao, “Trust Management for SOA-Based IoT and Its Application to Service Composition,“ *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482 - 495, Oct. 2016.

[114] J. Kiljander, et al., “Semantic Interoperability Architecture for Pervasive Computing and Internet of Things,“ *IEEE Access*, vol. 2, no. 856 - 873, Aug. 2014.

[115] P. Barnaghi, W. Wang, C. Henson, K. Taylor, “Semantics for the Internet of Things: Early progress and back to the future,” *International Journal on Semantic Web and Information Systems*, vol. 8, no. 1, pp. 1–21, Jan. 2012.

[116] M. Ganzha, M. Paprzycki, W. Pawlowski, P. Szmeja, K. Wasielewska, “Semantic Technologies for the IoT - An Inter-IoT Perspective,“ *In Proc. IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2016, pp. 271 – 276.

[117] Y. Huang, G. Li, “A Semantic Analysis for Internet of Things,” *In Proc. International Conference on Intelligent Computation Technology and Automation*, 2010, vol. 1, pp. 336 – 339.

[118] Z. Song, A. A. Cardenas, R. Masuoka, “Semantic middleware for the Internet of Things,” *In Proc. Internet of Things (IoT)*, 2010, Pages: 1 – 8.

[119] Y. Wu, J. Li, J. Stankovic, K. Whitehouse, S. Son, K. Kapitanova, “Run Time Assurance of Application-Level Requirements in Wireless Sensor Networks,” *In Proc. 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 2010, pp. 197-208.

[120] S-I. Choi, S-J. Koh, “Use of Proxy Mobile IPv6 for Mobility Management in CoAP-Based Internet-of-Things Networks,” *IEEE Communications Letters*, vol. 20, no. 11, pp. 2284 - 2287, Aug. 2016.

[121] J. Huang, Q. Duan, Y. Zhao, Z. Zheng, W. Wang, “Multicast Routing for Multimedia Communications in the Internet of Things,” *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1 - 1, Feb. 2017.

[122] J. Ko, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, P. Levis, “Connecting low-power and lossy networks to the internet,“ *IEEE Communications Magazine*, vol. 49, no. 4, pp. 96 – 101, Apr. 2011.

[123] T. Clausen; U. Herberg; M. Philipp, “A critical evaluation of the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL),” *In Proc. IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2011, pp. 365 – 372.

[124] S. Abdelwahab; B. Hamdaoui; M. Guizani; T. Znati, “Cloud of Things for Sensing-as-a-Service: Architecture, Algorithms, and Use Case,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1099 – 1112, Dec. 2016.

[125] C. Perera; A. Zaslavsky; P. Christen; D. Georgakopoulos, “Context Aware Computing for The Internet of Things: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414 - 454, First Quarter 2014.

[126] A. Mukherjee; H. S. Paul; S. Dey; A. Banerjee, “ANGELS for distributed analytics in IoT,” *In Proc. IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 565 – 570.

[127] H. Madsen, B. Burtschy, G. Albeanu, Fl. Popentiu-Vladicescu, “Reliability in the utility computing era: Towards reliable Fog computing,” *In Proc. 20th International Conference on Systems, Signals and Image Processing (IWSSIP)*, 2013, pp. 43 – 46.

[128] M. Chiang; T. Zhang, “Fog and IoT: An Overview of Research Opportunities,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854 - 864, Dec. 2016.

[129] M. Roopaei; P. Rad; K-K. R. Choo, "Cloud of Things in Smart Agriculture: Intelligent Irrigation Monitoring by Thermal Imaging," *IEEE Cloud Computing*, vol. 4, no. 1, Mar. 2017.

[130] M. Mosko, I. Solis, E. Uzun, C. Wood, “CCNx 1.0 Protocol Architecture,” *A Xerox Company, Computing Science Labaratory PARC*, Apr. 2017, [Online]. Available: http://www.ccnx.org/pubs/CCNxProtocolArchitecture.pdf

[131] M. A. Rajan, P. Balamuralidhar, K. P. Chethan, M. Swarnahpriyaah, “A Self-Reconfigurable Sensor Network Management System for Internet of Things Paradigm, “ *In Proc. International Conference on Devices and Communications (ICDeCom)*, 2011, pp. 1 – 5.

[132] M. Abu-Elkheir, M. Hayajneh, N.A. Ali, “Data Management for the Internet of Things: Design Primitives and Solution,” *Sensors*, vol. 13, pp. 15582-15612, Oct. 2013.

[133] C-W. Tsai; C-F. Lai; M-C. Chiang; L. T. Yang, “Data Mining for Internet of Things: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 77 - 97, First Quarter 2014.

[134] P. Rost, et al., “Cloud technologies for flexible 5G radio access networks“, IEEE Communications Magazine,” vol. 52, no. 5, pp. 68 – 76, Sep. 2014.

[135] H.H. Cho, C-F. Lai, T. K. Shih, H-C. Chao, “Integration of SDR and SDN for 5G,“ *IEEE Access*, vol. 2, pp. 1196 - 1204, Sep. 2014.

[136] M. A. S. Santos; B. A. A. Nunes; K. Obraczka; T. Turletti; B. T. de Oliveira; C. B. Margi, “Decentralizing SDN's control plane,“ *In Proc. 39th Annual IEEE Conference on Local Computer Networks*, 2014, pp. 402 – 405.

[137] N. Bizanis, F. A. Kuipers, “SDN and Virtualization Solutions for the Internet of Things: A Survey,” *IEEE Access*, vol. 4, pp. 5591 - 5606, Sep. 2016.

[138] K. Sood, S. Yu, Y. Xiang, “Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review,“ *IEEE Internet of Things Journal*, vol. 3, no. 4, Aug. 2016.

[139] D. Bandyopadhyay, J. Sen, “Internet of Things: Applications and Challenges in Technology and Standardization,“ *Wireless Pers. Commun.*, vol. 58, no. 1, pp 49–69, May 2011.

[140] M. Trnka, T. Cerny, “Identity Management of Devices in Internet of Things Environment,” *In Proc. 6th International Conference on IT Convergence and Security (ICITCS)*, 2016, pp. 1 – 4.

[141] *OMA LightweightM2M (LWM2M)*, OMA (Open Mobile Alliance) Specification, Feb. 2017. [Online]. Available: http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0-2

[142] V. Perelman, J. Schoenwaelder, M. Ersue, K. Watsen, “Network Configuration Protocol Light (NETCONF Light),” *IETF Network Working Group*, Jan. 2012, [Online]. Available: https://tools.ietf.org/html/draft-schoenw-netconf-light-01

[143] Q. Wu, G. Ding, Z. Du, Y. Sun, M. Jo, A. V. Vasilakos, “A Cloud-Based Architecture for the Internet of Spectrum Devices Over Future Wireless Networks,“ *IEEE Access*, vol. 4, pp. 2854 - 286, Jun. 2016.

[144] M. Elkhodr; S. Shahrestani; H. Cheung, “A Smart Home Application Based on the Internet of Things Management Platform,“ *In Proc. IEEE International Conference on Data Science and Data Intensive Systems*, 2015, pp. 491 – 496.

[145] T. Shah, A. Yavari, K. Mitra, S. Saguna, P. P. Jayaraman, F. Rabhi, R. Ranjan, “Remote health care cyber-physical system: quality of service (QoS) challenges and opportunities,“ *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 40 – 48, Jan. 2017.

[146] A. Floris, L. Atzori, “Quality of Experience in the Multimedia Internet of Things: Definition and practical use-cases,“ *In Proc. IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1747 – 1752.

[147] Q. Wu, G. Ding, Y. Xu, S. Feng, Z. Du, J. Wang, K. Long, “Cognitive Internet of Things: A New Paradigm Beyond Connection,“ *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 129 - 143, Apr. 2014.

[148] A. Laya; L. Alonso; J. Alonso-Zarate, “Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives,“ *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, First Quarter 2014.

[149] A. Lo, Y. W. Law, M. Jacobsson, “A cellular-centric service architecture for machine-to-machine (M2M) communications,“ *IEEE Wireless Communications*,vol. 20, no. 5, pp. 143 - 151, Oct. 2013.

[150] L. Li, S. Li, S. Zhao, “QoS-Aware Scheduling of Services-Oriented Internet of Things,“ *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1497 - 1505, May 2014.

[151] F. Samie, V. Tsoutsouras, S. Xydis, L. Bauer, D. Soudris, J. Henkel, “Distributed QoS management for Internet of Things under resource constraints,“ *In Proc. International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, 2016, pp. 1 – 10.

[152] C. Xiang, P. Yang, X. Wu, H. He, S. Xiao, “QoS-based service selection with lightweight description for large-scale service-oriented internet of things,“ *Tsinghua Science and Technology*,vol. 20, no. 4, pp. 336 - 347, Aug. 2015.

[153] M. B. Yassein, Mohammed Q. Shatnawi, D. Al-zoubi, “Application layer protocols for the Internet of Things: A survey,” In Proc. International Conference Engineering & MIS (ICEMIS), 2016, pp. 1-4.

[154] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann, K. K. Leung, “A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities,” *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.

[155] P. Masek, et al., “Implementation of true IoT vision: Survey on enabling protocols and hands-on experience,“ *International Journal of Distributed Sensor Networks*, vol. 12, no. 4, pp. 1-18, Apr. 2016.

[156] W. Colitti, K. Steenhaut, N. De Caro, B. Buta, V. Dobrota, “Evaluation of constrained application protocol for wireless sensor networks,” *In Proc. 18th IEEE Workshop LANMAN*, 2011, pp. 1–6.

[157] N. De Caro, W. Colitti, K. Steenhaut, G. Mangino, G. Reali, “Comparison of two lightweight protocols for smartphone-based sensing,” *In Proc. IEEE 20th SCVT*, 2013, pp. 1–6.

[158] J. L. Fernandes, I. C. Lopes, J. J. P. C. Rodrigues, S. Ullah, “Performance evaluation of RESTful web services and AMQP protocol,“ *In Proc. Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2013, pp. 810 – 815.

[159] V. Pimentel, B. G. Nickerson, “Communicating and Displaying Real-Time Data with WebSocket,“ *IEEE Internet Computing*, vol. 16, no. 4, pp. 45 - 53, May 2012.

[160] A. Čolaković, T. Čaršimamović, “The Corresponding Options of TCP Variants for Fairness Problem in AD HOC Networks,“ *International Journal of Soft Computing and Engineering*, vol. 5, no. 2, pp. 1-8, May 2015.

[161] R. Roman, P. Najera, J. Lopez, “Securing the Internet of Things,” *Computer*, vol. 44, no. 9, pp. 51 - 58, Sep. 2011.

[162] A. J. Jara; P. Martinez-Julia; A. Skarmeta, “Light-Weight Multicast DNS and DNS-SD (lmDNS-SD): IPv6-Based Resource and Service Discovery for the Web of Things,” *In Proc. Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2012, pp. 731 – 738.

[163] S. Lanzisera, A. R. Weber, A. Liao, D. Pajak, A. K. Meier, “Communicating Power Supplies: Bringing the Internet to the Ubiquitous Energy Gateways of Electronic Devices“, *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 153 - 160, Apr. 2014.

[164] J. Qi, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, “Security of the Internet of Things: perspectives and challenges,“ *Wireless Networks*, vol. 20, no. 8, pp. 2481-2501, Nov. 2014.

[165] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, “Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT),“ *In Proc. Communications in Computer and Information Science*, vol. 89, 2010, pp. 420-429.

[166] S. Kalra, S. K. Sood, “Secure authentication scheme for IoT and cloud servers,“ *Pervasive and Mobile Computing*, vol. 24, pp. 210-223, Dec. 2015.

[167] *Internet of Things research study*, Hewlett Packard Enterprise report, 2015, [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050#.WPoNH6KxWUk

[168] L. D. Xu; W. He; S. Li, “Internet of Things in Industries: A Survey,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233 - 2243, Nov. 2014.

[169] Z. Yan, P. Zhang, A. V. Vasilakos, “A survey on trust management for Internet of Things,“ *Journal of network and computer applications*, vol. 42, pp. 120-134, Jun. 2014.

[170] K. Kang, Z. Pang, L. D. Xu, L. Ma, C. Wang, “An Interactive Trust Model for Application Market of the Internet of Things,“ *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1516 - 1526, May. 2014.

[171] D. Singh, G. Tripath, A. Jara, “Secure layers based architecture for Internet of Things,“ *In Proc. IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 321 – 326.

[172] S. L. Keoh, S. S. Kumar, H. Tschofenig, “Securing the Internet of Things: A Standardization Perspective,“ *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265 – 275, Jun. 2014.

[173] M. Pei, N. Cook, M. Yoo, A. Atyeo, H. Tschofenig, “The Open Trust Protocol (OTrP),“ *IETF*, 2016. [Online]. Available: https://tools.ietf.org/html/draft-pei-opentrustprotocol-00

[174] T. Dierks, C. Allen, “The TLS Protocol Version 1.0", *IETF RFC 2246*, 1999. [Online]. Available: https://www.ietf.org/rfc/rfc2246.txt

[175] E. Rescorla, N. Modadugu, “Datagram Transport Layer Security,” *IETF RFC 4347*, [Online] Available: https://tools.ietf.org/html/rfc4347

[176] S. Vatari, A. Bakshi, T. Thakur, “Green house by using IOT and cloud computing,” *In Proc. IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2016, pp. 246 – 250.

[177] F. K. Shaikh, S.Zeadally, E. Exposito, “Enabling Technologies for Green Internet of Things,” *IEEE Systems Journal*, vol. PP, no. 99, pp. 1 – 12, Apr. 2015.

[178] S. K. Datta; C. Bonnet; N. Nikaein, “An IoT gateway centric architecture to provide novel M2M services, “ *In Proc. 2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 514 - 519

[179] D. Macedo, L. A. Guedes; I. Silva, “A dependability evaluation for Internet of Things incorporating redundancy aspects,” *In Proc. Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control*, 2014, pp. 417 – 422.

[180] J. Yun, I-Y. Ahn, N-M. Sung, J. Kim, “A device software platform for consumer electronics based on the internet of things,“ *IEEE Transactions on Consumer Electronics*, vol. 61, no. 4, pp. 564 - 571, Nov. 2015.

[181] H-L. Fu, P. Lin, H. Yue, G-M. Huang, C-P. Lee, “Group Mobility Management for Large-Scale Machine-to-Machine Mobile Networking,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 3, pp. 1296 - 1305, Mar. 2014.

[182] F. Bao, I-R. Chen, J Guo, “Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems,“ *In Proc. IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, 2013, pp. 1 – 7.

[183] M. Masirap, et al., “Evaluation of reliable UDP-based transport protocols for Internet of Things (IoT)", *In Proc. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2016, pp. 200 – 205.

[184] R. Fantacci, T. Pecorella, R. Viti, C. Carlini, “A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities,” *IEEE Wireless Communications*, vol. 21, no. 4, pp. 113 - 119, Aug. 2014.

[185] A. Taivalsaari, T. Mikkonen, “A Roadmap to the Programmable World: Software Challenges in the IoT Era,” *IEEE Software*, vol. 34, no. 1, pp. 72 - 80, Jan. 2017.

[186] F. Al-Turjman, A. Radwan, S. Mumtaz, J. Rodriguez, "Mobile traffic modelling for wireless multimedia sensor networks in IoT," *Computer Communications*, vol. 112, pp. 109 - 115, Nov. 2017.

[187] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1 - 31, Dec. 2014.

[188] R. K. Lomotey, J. Pry, S. Sriramoju, "Wearable IoT data stream traceability in a distributed health information system," *Pervasive and Mobile Computing*, vol. 40, p.p. 692-707, Sep. 2017.

[189] Y. Xu, V. Mahendran, W. Guo, S. Radhakrishnan, "Fairness in fog networks: Achieving fair throughput performance in MQTT-based IoTs," *In. Proc. Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual*, 2017, pp. 191-196.

[190] A. Rizzardi, S. Sicari, D. Miorandi, A. Coen-Porisini, “AUPS: an Open Source AUthenticated Publish/Subscribe system for the Internet of Things,” *Information Systems, Vol.* 62, pp. 29-41, Dec. 2016.

[191] M. Maier, M. Chowdhury, B.P. Rimal, D.P. Van, "The tactile internet: vision, recent progress, and open challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 138 – 145, May 2016.

[192] S. Sicaria, A. Rizzardia, D. Miorandib, C. Cappielloc, A. Coen-Porisinia, “A secure and quality-aware prototypical architecture for the Internet of Things,” *Information Systems*, vol. 58, pp. 43-55, Jun. 2016.

[193] D. Mazza, D. Tarchi, G. E. Corazza, "A Unified Urban Mobile Cloud Computing Offloading Mechanism for Smart Cities," *IEEE Communication Magazine*, vol. 55, no. 3, pp. 30-37, Mar. 2017.

[194] H. Lamaazi, N. Benamar, A. J.Jara, "RPL-based networks in static and mobile environment: A performance assessment analysis," *Journal of King Saud University - Computer and Information Sciences*, pp. 1-14, Apr. 2017.

[195] R. Hamilton, J. Iyengar, I. Swett, A. Wilk, "QUIC: A UDP-Based Secure and Reliable Transport for HTTP/2 draft-tsvwg-quic-protocol-02," Internet-Draft, Jan. 2016, [Online]. Available: https://tools.ietf.org/html/draft-tsvwg-quic-protocol-02

[196] Z. Shelby, M. Huttunen, M. Saarnivala, J. Riihijärvi, O. Raivio, P. Mähönen, "nanoIP," *Internet Draft*, Feb. 2005, [Online]. Available: https://tools.ietf.org/html/draft-shelby-nanoip-00

[197] *Eddystone format*, Apr. 2018, [Online]. Available: https://developer.estimote.com/eddystone/
[198] *IEEE Std 802.11ah-2016*, WG802.11 - Wireless LAN Working Group, 2016, [Online]. Available: https://standards.ieee.org/findstds/standard/802.11ah-2016.html
[199] *Weightless Specification*, Nov. 2017, [Online]. Available: http://www.weightless.org/about/weightless-specification
[200] *Standardization of NB-IOT*, Jun. 2016, [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete
[201] *Progress on 3GPP IoT*, Feb. 2016, [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1766-iot_progress
[202] *Release 14*, Feb. 2016, [Online]. Available: http://www.3gpp.org/release-14
[203] *LoRaWAN™ Specification*, Nov. 2015, https://lora-alliance.org/about-lorawan
[204] *Sigfox Technology Overview*, 2017, https://www.sigfox.com/en/sigfox-iot-technology-overview
[205] *Random Phase Multiple Access technology*, Ingenu Inc, 2016, https://www.ingenu.com/technology/rpma/
[206] *Wi-Fi HaLow*, Wi-Fi Alliance®, Jan. 2016, https://www.wi-fi.org/discover-wi-fi/wi-fi-halow
[207] A. Munir, P. Kansakar, S. U. Khan, "IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 74 - 82, Jun. 2017.
[208] A. Brogi, A: Forti, "QoS-aware Deployment of IoT Applications Through the Fog," *IEEE Internet of Things Journal*, May 2017, Vol. PP, No. 99, pp. 1-8.
[209] W. Li, I. Santos, F. C. Delicato, P. F. Pires, L. Pirmez, W. Wei, H. Song, A. Zomaya, S. Khan, „System modelling and performance evaluation of a three-tier Cloud of Things," *Future Generation Computer Systems*, vol. 70, pp. 104-125, May. 2017.
[210] S. Sarkar, S. Misra, „Theoretical modelling of fog computing: a green computing paradigm to support IoT applications," *IET Networks*, vol. 5. no. 2, pp. 1-7, Mar. 2016.
[211] G. Fortino, R. Gravina, W. Russo, C. Savaglio, „Modeling and Simulating Internet-of-Things Systems: A Hybrid Agent-Oriented Approach," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 68-76, Oct. 2017.
[212] G. D'Angelo, S. Ferretti, V. Ghini, "Modeling the Internet of Things: a simulation perspective," *In Proc. High Performance Computing & Simulation (HPCS)*, pp. 18-27, Sep. 2017.
[213] G. Kecskemeti, G. Casale, D.N. Jha, J. Lyon, R. Ranjan, "Modelling and Simulation Challenges in Internet of Things," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 62-69, Jan.-Feb. 2017.
[214] K. Batool, M. A. Niaz, "Modeling the internet of things: a hybrid modeling approach using complex networks and agent-based models," *Complex Adaptive Systems Modeling*, vol. 5, no.4, pp. 1-19, Mar. 2017.

Alem Čolaković received the B.Sc. and M.Sc. degree in Communication technologies from the Faculty of Traffic and Communications, University of Sarajevo, in 2009 and 2011, respectively. He is currently a Ph.D. candidate at the same department. Since February 2011, he working as a Teaching Assistant and System Engineer. He was involved in several international and national research projects including four IPA projects co-funded by the European Union. His research interests span communication technologies, Internet of Things, computer networks, ICT infrastructure, information systems, intelligent transport systems, technological mediation, etc. Mr. Čolaković is IEEE member as well as a member of Professional Association of Transportation and Communication Engineers in Bosnia and Herzegovina. He received several awards including the Golden Badge of the University of Sarajevo.

Mesud Hadžialić received the Dipl. Ing., M.S.E.E. and Ph.D. degrees from the Faculty of Electrical Engineering in Sarajevo, University of Sarajevo, in 1978, 1986 and 2001, respectively. From May 2015, he has been a Full Professor at the Department of Telecommunications, Faculty of Electrical Engineering University of Sarajevo. In the period from 2009 to now he has been performed duties Vice Dean for Science and Research and Head of the Department of Telecommunications. His research and teaching interests are in the general area of telecommunication techniques, theory and practice in the information networks, simulation methods and techniques in telecommunication channels and networks. He is an author (or coauthor) of: five textbooks of which three university textbooks; several papers in journals and over fifty papers at conferences. He was B&H project leader in projects: the project co-funded by the European Union (South East Europe Transnational Cooperation Programme): “Tackling the “Digital Divide” in SEE by using the capacity of DTT networks”, realized from 2012 to 2014; project „Extending the SON simulator with Carrier Aggregation techniques “, supported by CTVR/The Telecommunications Research Centre, O'Reilly Institute at Trinity College Dublin, Ireland, 2013. He led and participated in: five scientific projects in the field of telecommunications supported by Federal Ministry of Science of Federation of Bosnia and Herzegovina and more than ten local and international projects in the domain of network simulations.