A Survey on IoT: Architectures, Elements, Applications, QoS, Platforms and Security Concepts

Gonçalo Marques, Nuno Garcia and Nuno Pombo

Abstract The recent development of communication devices and wireless network technologies continues to advance the new era of the Internet and the telecommunications. The vision for the Internet of Things (IoT) states that various "things", which include not only communication devices but also every other physical object on the planet, are going to be connected and will be controlled across the Internet. The concept of the IoT has attracted significantly attention from many investigators in recent years. The incessant scientific improvements make possible to construct smart devices with huge potentials for sensing and connecting, allowing several enhancements based on the IoT paradigm. This chapter presents a review on research on IoT and analyses several IoT projects focused on IoT architectures, elements, Quality of Service (QoS) and currently open issues. The main objective of this chapter is to allow the reader to have an overview on the most important concepts and fundamental knowledge in IoT.

Keywords AAL · Smart homes · Sensors · IoT · Mobile computing · Design challenges · Social and ethical challenges · System architectures · Security · QoS

1 Introduction

The basic idea of the Internet of Things (IoT) is the pervasive presence of a variety of objects with interaction and cooperation capabilities among them to reach a common objective [1].

G. Marques · N. Garcia (✉) · N. Pombo
Faculty of Engineering, Computer Science Department,
Universidade da Beira Interior, Covilhã, Portugal
e-mail: ngarcia@di.ubi.pt

G. Marques · N. Garcia · N. Pombo
Assisted Living Computing and Telecommunications Laboratory (ALLab),
Instituto de Telecomunicações, Covilhã, Portugal

N. Garcia
Universidade Lusófona de Humanidades e Tecnologias, Lisbon, Portugal

C.X. Mavromoustakis et al. (eds.), *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, Studies in Big Data 22,
DOI 10.1007/978-3-319-45145-9_5

Is expected that the IoT will have a great impact on several aspects of everyday-life and this concept will be used in many applications such as domotics, assisted living, e-health and is also an ideal emerging technology to provide new evolving data and computational resources for create revolutionary software applications (also known as "apps") [2]. Systems based on the IoT interact via wireless technologies such as RFID (Radio-Frequency Identification), NFC (Near Field Communication), ZigBee, WSN (Wireless sensor network), DSL (Digital Subscriber Line), WLAN (wireless local area network), WiMax (Worldwide Interoperability for Microwave Access), UMTS (Universal Mobile Telecommunications System), GPRS (General Packet Radio Service), or LTE (Long-Term Evolution).

Moreover, IoT presents several challenges to be solved such as security and privacy, participatory sensing, big data, and architectural issues apart of the known WSN challenges, including energy efficiency, protocols, and Quality of Service (QoS) [2]. In the one hand, technological standardization of the IoT is now starting to be missed, so collaboration among IEEE (Institute of Electrical and Electronics Engineers), ISO (International Organization for Standardization), ETSI (European Telecommunications Standards Institute), IETF (Internet Engineering Task Force), ITU (International Telecommunication Union) and other related organizations is very important and urgent [3]. In the order hand, some authors define that premature standardization could risk stifling innovation [4]. Industry applications, monitoring and water control, smart homes' architecture, estimation of natural disaster, medical applications, agriculture application, intelligent transport system design, design of smart cities, smart metering and monitoring, smart security are examples of interesting applications of IoT [5].

This document is organized as follows. This paragraph concludes the introduction in Sect. 1. In Sect. 2, IoT visions and architecture are introduced. The essential elements of IoT are the subject of discussion in Sect. 3 and IoT applications, smart homes and health projects are addressed in Sect. 4. Section 5 gives an overview about IoT platforms and their open issues. In Sect. 6 important aspects about quality of service issues in IoT are introduced and Sect. 7 focuses on security and privacy concepts. Conclusions and future research topics are presented in Sect. 8

2 IoT Visions and Architecture

The paradigm of the IoT is referred to as the result of the merging of different views: things oriented vision, Internet oriented vision, and semantic oriented vision [6]. Under the same article, the IoT semantic oriented vision means a global network of interconnected objects that have a unique address based on standard communication protocols. The things oriented vision focuses on intelligent autonomous devices that use technologies such as NFC and RFID objects, applied to our daily lives. The Internet oriented vision focuses on the idea of keeping the devices connected to the network, having a single address and using standard

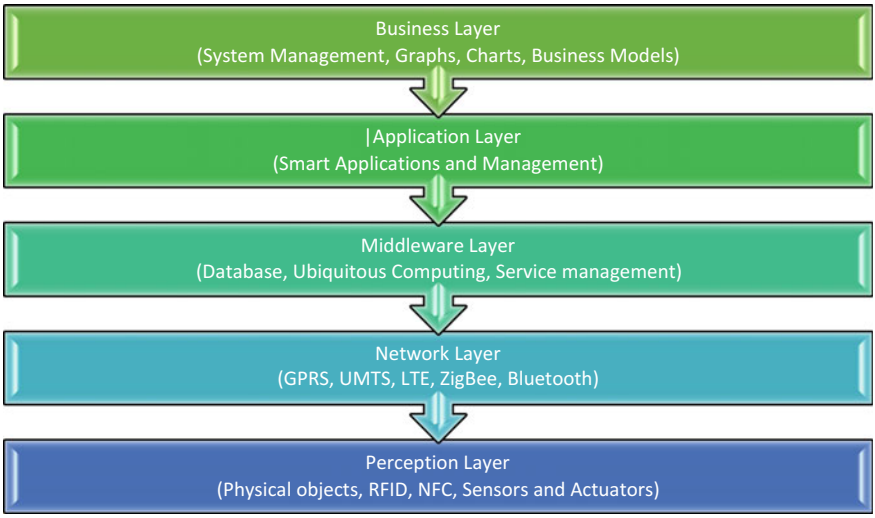

Fig. 1 IoT architecture layers adapted from [7]

protocols. Semantic oriented vision focuses on storage, searching and organizing information generated by IoT, seeking to create data and environment architectures modelling solutions to handle efficiently with the produced information.

The architecture of the IoT can be divided into five layers such as: Objects Layer or Perception Layer, Object Abstract layer or Network Layer, Service Management Layer or Middleware Layer, and Application Layer and Business layer (Fig. 1). On the one hand, the Perception Layer refers to physical sensors and actuators that IoT systems absorb [7]. On the other hand, the Network Layer transfers data produced by the Perception Layer to the Middleware Layer through secure channels using technologies such as RFID, ZigBee, WPAN, WSN, DSL, UMTS, GPRS, WiFi, WiMax, LAN, WAN, 3G and LTE. Furthermore, the Middleware Layer pairs a service with its requester based on addresses and names in order to maintain independence from the hardware. On the contrary, the Application Layer provides the services requested by customers providing the system output information to the user that requests that information.

Finally, the Business Layer manages the overall IoT system activities and services to build a business model, graphs, flowcharts, etc. based on the received data from the Application layer.

3 Elements of the Internet of Things

This section will revisit the elements of IoT such as identification, sensing, communication, computation, services and semantic (Fig. 2).

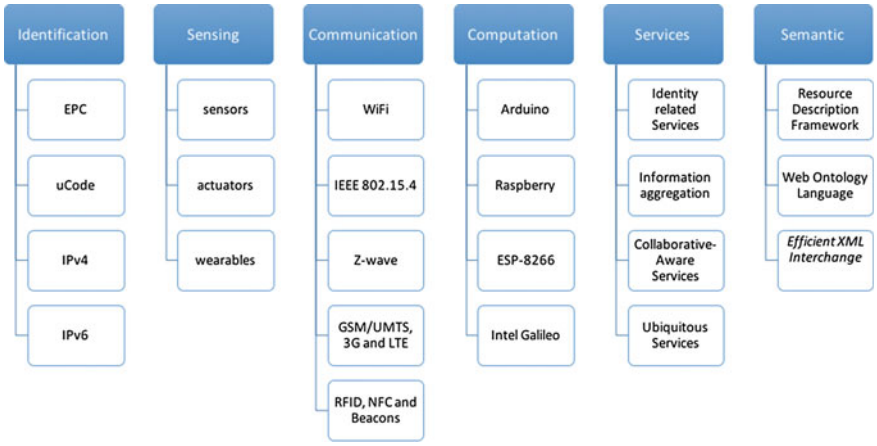

Fig. 2 IoT elements

The identification is essential for the development of the IoT and is important to ensure correct identification of objects in order to match services with their demand. Actually many identification methods exist such as electronic product codes (EPC) and ubiquitous code (uCode). Object identification refers to its name or designation and addressing refers to its IP address for communication on the network. Addressing methods include today's IPv4, IPv6 and 6LoWPAN that provides compression on IPv6 headers [8]. With the large address space provided by IPv6, all the addressing needs of the IoT are thought to be taken care of.

In IoT, sensing refers to acquire data from the environment and send it to a database, remote, local or in a cloud, and as example of IoT sensors one can find smart sensors, actuators or wearable sensors.

Moreover, the communication is an integral part of all IoT devices. Limited by the nature of the "things" themselves, as for example, battery life or limited range of data transmission, protocols such as WiFi, ZigBee, GSM, GPRS, UMTS, 3G, LTE and 5G [9], among others, are common. The IEEE 802.15.4e standard was released by IEEE in 2012 to enhance and add functionality to the previous 802.15.4 standard, as to address the emerging needs of embedded industrial applications [10]. There are also other communications technologies used for proximity communications like RFID [11], NFC [12] and Beacons (Bluetooth Low Energy) [13]. An memoryless-based collision window tree plus (CwT+) protocol for simplified computation in anti-collision radio frequency identification (RFID) is proposed by [14], the authors concluded the outperformance of the CwT+ compared with earlier protocols. A low-cost flexible NFC tags to allow everyday objects to communicate to smartphones and computers and thus participate in the IoT is proposed by [15], according to the authors the most important NFC regulatory standards are met, even with relaxed 5 micron design rules, using optimized design topologies. Bluetooth 4.2 offers features that makes Bluetooth Low Energy an appropriate protocol for

low-power communication technologies in the IoT and are applied in 6LoWPAN networks [16].

In addition, IoT are deployed using several hardware platforms applications such as Arduino [17], Intel Galileo [18], Raspberry Pi [19] or ESP8266 [20]. Cloud computing platforms are also an important computational part of the IoT paradigm because they provide facilities for storing and/or processing data in real time.

The different IoT services can be categorized as Identity related services, Information aggregation services, Collaborative-Aware services, and Ubiquitous services [21]. Identity-related services are focused on the identification of objects, whereas Aggregation services collet and summarize sensory data, and send them to the backend application. Furthermore, Collaborative-Aware services are used to turn the obtained data into a decision in order to react accordingly, while Ubiquitous services aim to provide Collaborative-Aware services anytime to anyone anywhere.

Semantic in the IoT is considered as the ability to extract knowledge from machines to provide the required services by discovering and using resources and modelling information. Thus, Semantic Web technologies examples are the Resource Description Framework (RDF) [22] and the Web Ontology Language (OWL) [23].

4 Applications

IoT turn into reality several important applications like smart homes, ambient assisted living and health domains, which are detailed in the next sections.

4.1 Smart Homes

Smart homes have been researched for decades, being the first Smart Rooms project implemented by the MIT Media Lab [24]. Nowadays, smart homes may be classified into three different categories: The first category aims to detect and to recognize the actions of its residents in order to determine their health condition. The second category, aims at storing and retrieving of multi-media captured within the smart home, in different levels from photos to experiences. The third category is focused on the surveillance, where the data captured in the environment are processed to obtain information that may help to raise alarms, in order to protect the home and the residents. There is also a type of smart homes that have the objective to reduce the energy consumption by monitoring and controlling electric devices [25].

Recent advances in information technology allowed lower prices of smart homes but provide them intelligence environments to make complex decisions remains a challenge. Thus, is expected an increasingly amount of interconnections among sensors for collect data in real time.

Three broad views about smart homes are introduced by [26]: a functional view; an instrumental view; and a socio-technical view. The functional view sees smart homes as a way of better managing the demands of daily living through technology. The instrumental view emphasises smart homes' potential for managing and reducing energy demand in households as part of a wider transition to a low-carbon future. The socio-technical view sees the smart home as the next wave of development in the ongoing electrification and digitalisation of everyday life.

A really interesting smart home application is introduced by [27], called Vital-Radio, which consists in a wireless sensing technology that monitors breathing and heart rate without body contact. This method demonstrates through a user study that it can track users' breathing and heart rates with a median accuracy of 99 %. In Europe, smart home projects include iDorm [28], Gloucester Smart Home [29], and CareLab [30], which is distinguished by its importance for the development of state of the art and due to innovative features.

Several challenges are related to IoT and AAL such as security, privacy, and legal. IoT devices are typically wireless and exposed to public range, the ownership of data collected from IoT devices must be clearly established. In fact, IoT devices should use encryption methods and be equipped with privacy policies.

In order to try to resolve privacy issues, the ambient sensing system AmbLEDs project, proposes the use of LEDs instead of other types of more invasive sensors such as cameras and microphones. In fact, this type of applications reveal the importance of using simple and intuitive interfaces for the interaction with people in the ambient assisted living [31].

Humans will often be the integral parts of the IoT system and therefore IoT will affect every aspect of human lives. In addition, due to the large scale of devices arise continuing problems of privacy and security so as consequence cooperation between the research communities is essential [32].

An really interesting example of IoT combined with ALL is proposed by [33] where an integrated platform for monitoring and controlling of a household that uses ZigBee Wireless network is reported which is distinguished by the use of open-source technologies.

The SPHERE Project [34] aims to build a generic platform that fuses complementary sensor data to generate rich datasets that support the detection and management of various health conditions. This project uses three sensing technologies: environment, video, and wearable sensing.

Furthermore, a cloud-based IoT platform for AAL proposed by [35], aims to manage the integration and behaviour-aware orchestration of devices as services stored and accessed on the cloud.

Well-known technologies like RFID, is still used to match IoT and ALL, allowing the creation of intelligent systems that can detect user-object interactions using for example supervised machine learning algorithms. In line with this, the project described in [36] where the authours present weighted Information Gain (wIG), an empirical method for reliably detecting unassisted, deviceless, and real time—user-object interaction using RFID.

In addition. the Home Health Hub Internet of Things (H3IoT) consists in an architectural framework for monitoring health of elderly people at his home. This framework presents several advantages such as: mobility, affordable price, usability, simple layered design, and delay tolerant [37].

4.2 Health Projects Based on IoT

IoT is a suitable approach to build health care systems, based on the technology advancements that allows to define new advanced methods for the treatment of many diseases e.g. by monitoring of chronic diseases to help doctors to determine the best treatments as proposed by [38].

A solution for diabetes therapy based on the IoT is proposed by [39]. This solution supports a patient's profile management architecture based on the personal RFID cards. A global connectivity among the patient's personal device, based on 6LoWPAN, the nurses/physicians' desktop application to manage personal health records, the glycaemic index information system, and the patient's web portal is provided.

On the last few years, the IoT has been proposed on several projects for remote health care aiming at to improve acquisition and processing of data [40]. Despite the potential of the IoT paradigm and technologies for health systems, there are still room for improvement on different topics. The direction and impact of the IoT economy is not yet clear, there are barriers to the immediate and ubiquitous adoption of IoT products and services, and these solutions may sound feasible for implementation, the timing may be too early [41].

In addition, IoT technologies provide many benefits to the healthcare domain in activities such as tracking of objects, patients and staff, identification and authentication of people, automatic data collection and sensing [6]. Thus, IoT gives a considerable solution as a platform to ubiquitous healthcare using wearable sensors to upload the data to servers and smartphones for communication along with Bluetooth for interfacing sensors measuring physiological parameters [2].

Health-care applications should incorporate several mechanisms that should be used to provide privacy of personal and/or sensitive information has harnessed the adoption of IoT Technologies. The interconnection of many IoT systems and sensors could trigger an intervention by the medical staff upon detection of conditions that otherwise unattended could lead to health and wellbeing deterioration, thus realizing preventive care [42].

In fact, security vulnerabilities exist in a Machine-to-machine (M2M)/IoT communication, aiming at to ensure the proper access to the right entities at the right time, and supported by a secure architecture. Other big challenge is that M2M/IoT devices may not have enough capabilities to execute encryption methods on the device [43]. This challenge must be solved if a secure health systems based on IoT is provided.

The Health-IoT (in-home health care service based on the IoT technologies) has promising prospects. A business-technology co- design methodology is proposed for cross-boundary integration of in-home health care devices and services based in IoT [44].

An IoT based sensing architecture facilitates improving energy efficiency by permit dynamic utilization of sensors and the use of IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) has been proposed to connect energy constrained WPAN devices to the Internet [45, 46].

The IoT paradigm specifies a way to monitor, store and utilize health and wellbeing related data on a 24/7 basis [47] and also provide services to be ubiquitous and customized for personal needs [42, 48].

An proof of concept implementation of an IoT-based remote health monitoring system includes an demo of a Smart e-Health Gateway called UT-GATE is proposed by [49]. UT-GATE provides local services for health monitoring applications such as local repository, compression, signal processing, data standardization, WebSocket server, protocol translation and tunnelling, firewall, and data mining and notification.

5 IoT Platforms

A IoT platform can be defined as the middleware infrastructure that supports the interactions between devices and users. These platforms can be divided in general into Cloud-based platforms (Fig. 3) and Local platforms (Fig. 4).

The most important characteristics of an IoT platform are the support to heterogeneous devices, the data privacy and security, data fusion and sharing, the support to APIs and to the IoT ecosystem. In line with this, this section will briefly summarize a number of platforms for the Internet of Things. It is intended to

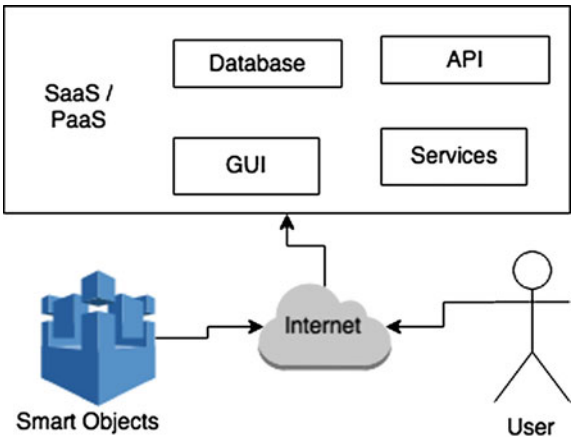

Fig. 3 Cloud platform

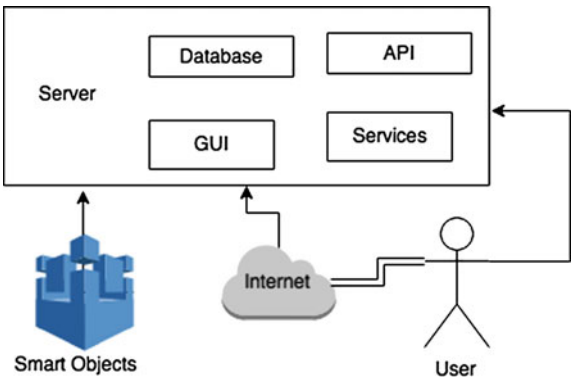

Fig. 4 Local platform

highlight the most important platforms, so those who have more advantages and which are distinguished by its importance for the development of state of the art and due to innovative features.

1. **OpenIoT**: supports heterogeneous devices have a decentralized architecture, is open-source (LGPLv3), have user-based privileges and service discovery [50].
2. **The thing system**: have a centralized architecture, provides service discovery, is open-source (M.I.T. License), does not provide storage functionalities and are designed to only provide access remotely to home's smart devices [51].
3. **Xively**: is a proprietary cloud-based platform that provides open-source API's and supports RESTful API [52].
4. **ARM mbed**: is a proprietary platform with centralized/Cloud-based architecture designed for embedded devices that supports security functionalities such as Transport Layer Security (TLS), it supports CoAP and RESTful API for create M2M networks [53].
5. **H.A.T.—Hub of All Things**: is an open-source platform that have a decentralized architecture that aim to create economic and business opportunities using generated data by IoT home's systems and supports RESTful API [54].
6. **Ericsson IoT Framework**: is a PaaS that includes a REST API, data storage functionalities and OpenId access control. It is a open-source (Apache license 2.0) platform with a centralized architecture [55].
7. **Calvin-Base**: is an open-source platform with a centralized architecture that supports REST API and is main goal is to be extremely extendable and for that it have a large amount of plugins applications to ensure interoperability [56].
8. **OpenRemote**: is an open-source platform with a centralized architecture that supports REST API and have local store system. This platform supports home and domotics environments [57].
9. **ThingWorx**: is a proprietary cloud-based architecture M2M platform (PaaS) that supports REST API and service discovery [58].

10. **Sense Tecnic WoTkit**: is a proprietary cloud-based architecture platform supports REST API and service discovery and have secured access [59].

As referred by [60] the success of the platforms and frameworks is based on different topics, as follows:

1. Enable devices, applications and systems to securely expose API's for 3rd party systems and to facilitate API management;
2. Enable systems to have protocol interoperability with other 3rd party API's and ensure they are extendable for new protocols;
3. Enabling constrained devices to participate into application networks. That is size, bandwidth, power supply(battery) and processing power constraints;
4. Governance—Enabling management and governance of heterogeneous networks of devices and applications.

There are challenges and problems that cross all these IoT platforms including the following: standardization, power and energy efficiency, Big Data, security and privacy, intelligence, integration methodology, pricing, network communications, storage and scalability and flexibility as showed in Fig. 5.

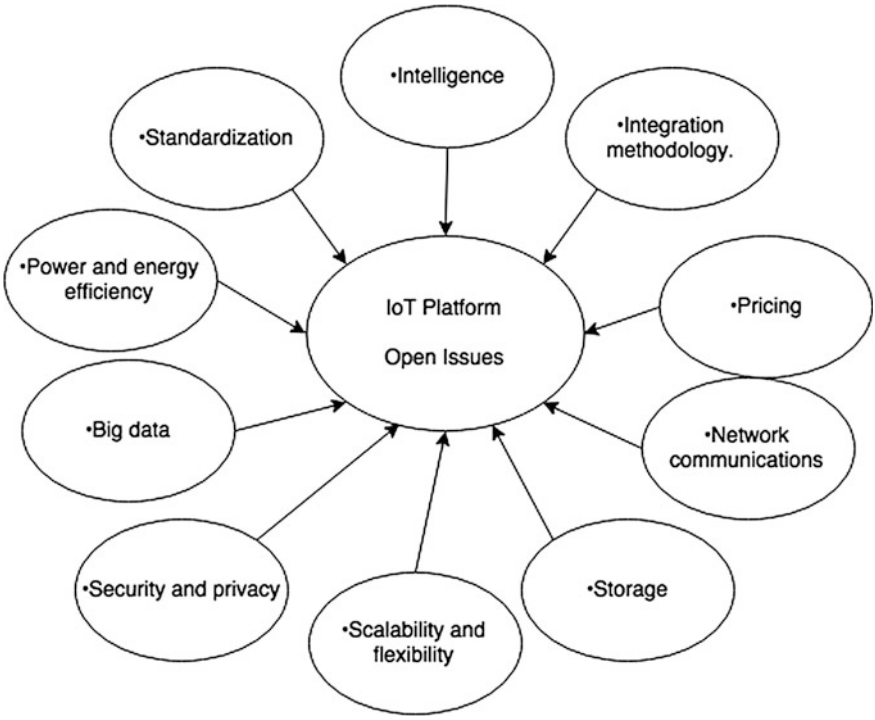

Fig. 5 Cloud platforms open issues

6 QoS in IoT

IoT presents several QoS (Quality of Service) issues such as availability, reliability, mobility, performance, scalability and interoperability, most of this issues are identified by [5–7, 42].

On the one hand, the availability of the IoT systems refers to provide anywhere and anytime services to customers. The IoT must try to be compatible with all devices and follow the protocols such as IPv6, and 6LoWPAN. On the other hand, the reliability refers to provide a high success rate for the IoT service delivery, and implemented in software and hardware throughout all the IoT layers. In addition, the mobility refers to connecting users with their desired services continuously while on the move, interruption for mobile devices can occur when these devices transfer from one gateway to another. An architecture based on IoT to support mobility and security in medical environments is proposed by [61].

Moreover, the performance of IoT services is a big challenge because it depends on the performance of many components of the IoT systems that needs to continuously develop and improve the performance of its services to meet the requirements.

Furthermore, the scalability of the IoT refers to the ability to add new devices, services and functions without affecting the quality of service. In the presence of diverse hardware platforms and communications protocols adding new operations and supporting new devices are challenging tasks. In addition, is not easy to assure the interoperability on these large-scale applications composed by a large number of heterogeneous things that belong to different platforms [62].

7 Security and Privacy

Security is the most significant challenge for IoT applications, and its architecture should fit the lifecycle of IoT, and its potentials. Thus, IoT systems must take into account the effect of packet fragmentation on security, with particular focus on possible DoS attacks [63].

Manufacturing IoT must not only address technical problems, but also consider planning, infrastructure, management, and security problems [64]. At the network layer, the IoT systems must use encryption and enhance the capacity against DoS attack.

In 2008 the ISO/IEC 29192 standards were created in order to provide light-weight cryptography for constrained devices, including block and stream ciphers and asymmetric mechanisms. Lightweight cryptography contributes to the security of smart objects networks because of its efficiency and smaller footprint [65].

The attacks on IoT systems can be categorized as physical attacks, side channel attacks, cryptanalysis attacks, software attacks and network attacks [66]. Physical attacks refer to attack the physical hardware and are harder to perform. Side channel

attacks makes use of information to recover the key the device is using. Cryptanalysis attacks are focused on the cipher text with the objective to break the encryption. Software attacks exploit vulnerabilities in the systems through its own communication interface. Networks communications are vulnerable to networks security attacks due to the broadcast nature of the transmission medium.

In fact, IoT systems that use wireless technologies may experience several security issues like attacks on secrecy and authentication, silent attacks on service integrity and attacks at network availability. Network availability attacks can be catalogued as DoS (Denial of Service) attacks an occur at physical, link, network, transport and application layers (Fig. 6) [67].

Although a lot of research has been done in order to increase the security in the IoT, open problems remain in a number of areas, such as cryptographic mechanisms, network protocols, data and identity management, user privacy, self-management, and trusted architectures [68]. Several proposals for security arrangements for IoT can be found in [69–74]. An overview of low-complexity physical-layer security schemes that are suitable for the IoT is proposed by [69]. A novel system architecture, called the Unit and Ubiquitous IoT (U2IoT) is proposed by [70] to face security issues. On the contrary, a two way authentication security scheme for the IoT based on existing Internet standards, especially the Datagram Transport Layer Security (DTLS) protocol is proposed by [71]. The possibility of reducing the over- head of DTLS by means of 6LoWPAN header compression is proposed by [72]. A new security solution for integrating WSNs into the Internet as part of the IoT is presented by [73]. Authors of [74] demonstrates the feasibility of using the Generic Bootstrapping Architecture (GBA) defined by the 3rd Generation Partnership Project (3GPP) to perform secure authentication of resource-constrained for IoT devices.

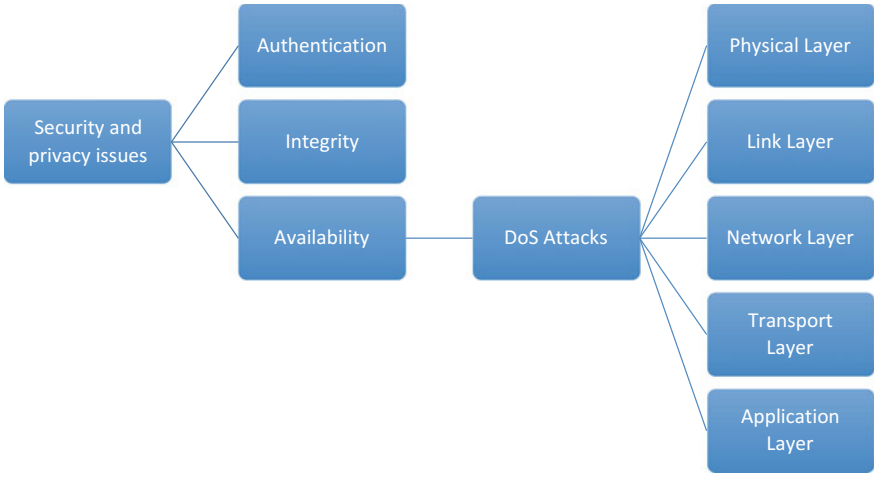

Fig. 6 Hierarchical diagram of security issues in IoT systems that incorporate wireless technologies adapted from [68]

8 Conclusions

The IoT is a paradigm that aims to improve the quality of human live. There are several visions of the IoT such as things oriented vision, Internet oriented and semantic oriented vision. The IoT can be divided into 5 layers such as Objects Layer or Perception Layer, Object Abstract layer or Network Layer, Service Management Layer or Middleware Layer, Application Layer and Business layer.

The main elements of the IoT are identification, sensing, communication, computation, services and semantic and exist several examples of fascinating applications like prediction of natural disaster, industry applications, design of smart homes, health applications, agriculture applications, intelligent transport system design, design of smart cities, smart security, smart metering and monitoring.

The IoT systems and ALL will continue side-by-side mutually contributing scientific advances in assisted living allowing also lower the cost of assisted living systems.

The IoT platforms must support heterogeneous devices, data fusion and sharing, data privacy and security, API's for interoperability and standardization. There are several open issues related with the IoT, such as standardization, security and privacy, power and energy efficiency, intelligence, integration methodology, big data, pricing, storage, network communications, scalability and flexibility. The IoT continues to present several QoS issues such as availability, reliability, mobility, performance, scalability and interoperability.

This paper presented an overview of the IoT concepts such as architecture, vision, elements, main applications focus on smart homes and heath systems, platforms, QoS and security issues, which should provide a good transversal sense of IoT technologies.

Despite the numerous technologic enhancements, some issues in the design of IoT systems continue to exist, namely corresponding to privacy, confidentiality, security, and interoperability of such systems.

Acknowledgements The authors would like to acknowledge the contribution of the COST Action IC1303—Architectures, Algorithms and Platforms for Enhanced Living Environments (AAPELE). Contributing to this research, the Authors affiliated with the *Instituto de Telecomunicações* also acknowledge the funding for the research by means of the program FCT project UID/EEA/50008/2013. (*Este trabalho foi suportado pelo projecto FCT UID/EEA/50008/2013*).

References

1. Giusto, D. (ed.): The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications. Springer, New York (2010)
2. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
3. Tan, L., Wang, N.: Future internet: the Internet of Things, pp. V5–376–V5–380 (2010)

4. Blackstock, M., Lea, R.: IoT interoperability: a hub-based approach, pp. 79–84 (2014)
5. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the Internet of Things architecture, possible applications and key challenges, pp. 257–260 (2012)
6. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
7. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutorial **17**(4), 2347–2376 (2015)
8. Jara, A.J., Zamora, M.A., Skarmeta, A.: Glowbal IP: an adaptive and transparent IPv6 integration in the Internet of Things. Mob. Inf. Syst. **8**(3) (2012)
9. Jermyn, J., Jover, R.P., Murynets, I., Istomin, M., Stolfo, S.: Scalability of machine to machine systems and the Internet of Things on LTE mobile networks. In: 2015 IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–9 (2015)
10. De Guglielmo, D., Anastasi, G., Seghetti, A.: From IEEE 802.15.4 to IEEE 802.15.4e: a step towards the Internet of Things. In: Gaglio, S., Lo Re, G. (eds.) Advances onto the Internet of Things, vol. 260, pp. 135–152. Springer (2014)
11. Falk, R., Kohlmayer, F., Köpf, A.: Device and method for providing RFID identification data for an authentication server. Google Patents (2015)
12. Curran, K., Millar, A., Mc Garvey, C.: Near field communication. Int. J. Electr. Comput. Eng. **2**(3), 371 (2012)
13. Gomez, C., Oller, J., Paradells, J.: Overview and evaluation of bluetooth low energy: an emerging low-power wireless technology. Sensors **12**(12), 11734–11753 (2012)
14. Garcia Zuazola, I.J., Bengtsson, L., Perallos, A., Landaluce, H.: Simplified computation in memoryless anti-collision RFID identification protocols. Electron. Lett. **50**(17), 1250–1252 (2014)
15. Myny, K., Cobb, B., van der Steen, J.-L., Tripathi, A.K., Genoe, J., Gelinck, G., Heremans, P.: 16.3 Flexible thin-film NFC tags powered by commercial USB reader device at 13.56 MHz, 1–3 (2015)
16. Raza, S., Misra, P., He, Z., Voigt, T.: Bluetooth smart: an enabling technology for the Internet of Things, pp. 155–162 (2015)
17. Doukas, C.: Building Internet of Things with the Arduino. CreateSpace Independent Publishing Platform (2012)
18. Ramon, M.C.: Intel Galileo and Intel Galileo Gen 2. Springer (2014)
19. Upton, E., Halfacree, G.: Raspberry Pi User Guide. Wiley (2014)
20. Raspaile, P., Keswani, V.: Integrating wireless sensor network with open source cloud for application of smart home
21. Gigli, M., Koo, S.: Internet of Things: services and applications categorization. Adv. Internet Things **01**(02), 27–31 (2011)
22. Vertan, C., Merkmale, R.-F.: Resource Description Framework (rdf) (2004)
23. McGuinness, D.L., Van Harmelen, F.: OWL web ontology language overview. W3C Recomm. **10**(10), 2004 (2004)
24. Moukas, A., Zacharia, G., Guttman, R., Maes, P.: Agent-mediated electronic commerce: an mit media laboratory perspective. Int. J. Electron. Commer. **4**(3), 5–21 (2000)
25. De Silva, L.C., Morikawa, C., Petra, I.M.: State of the art of smart homes. Adv. Issues Artif. Intell. Pattern Recognit. Intell. Surveill. Syst. Smart Home Environ. **25**(7), 1313–1321 (2012)
26. Wilson, C., Hargreaves, T., Hauxwell-Baldwin, R.: Smart homes and their users: a systematic analysis and key challenges. Pers. Ubiquit. Comput. **19**(2), 463–476 (2015)
27. Adib, F., Mao, H., Kabelac, Z., Katabi, D., Miller, R.C.: Smart homes that monitor breathing and heart rate. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, pp. 837–846 (2015)
28. Pounds-Cornish, A., Holmes, A.: The iDorm—a practical deployment of grid technology. In: 2002. 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 470–470 (2002)

29. Orpwood, R., Gibbs, C., Adlam, T., Faulkner, R., Meegahawatte, D.: The gloucester smart house for people with dementia—user-interface aspects. In: Keates, S., Clarkson, J., Langdon, P., Robinson, P. (eds.) Designing a More Inclusive World, pp. 237–245. Springer, London (2004)
30. Henkemans, O.B., Caine, K.E., Rogers, W.A., Fisk, A.D.: Medical monitoring for independent living: user-centered design of smart home technologies for older adults, in Proc, pp. 18–20. Telemedicine and Health Information and Communication Technologies, Med-e-Tel Conf. eHealth (2007)
31. Cunha, M., Fuks, H.: AmbLEDs para ambientes de moradia assistidos em cidades inteligentes. In: Proceedings of the 13th Brazilian Symposium on Human Factors in Computing Systems, Foz do Igua and ccedil; u, Brazil, 2014, pp. 409–412
32. Stankovic, J.A.: research directions for the Internet of Things. Internet Things J. IEEE **1**(1), 3–9 (2014)
33. Suryadevara, N.K., Kelly, S., Mukhopadhyay, S.C.: Ambient assisted living environment towards internet of things using multifarious sensors integrated with XBee platform. In: Mukhopadhyay, S.C. (ed.) Internet of Things, vol. 9, pp. 217–231. Springer (2014)
34. Zhu, N., Diethe, T., Camplani, M., Tao, L., Burrows, A., Twomey, N., Kaleshi, D., Mirmehdi, M., Flach, P., Craddock, I.: Bridging e-health and the Internet of Things: the SPHERE project. Intell. Syst. IEEE **30**(4), 39–46 (2015)
35. Cubo, J., Nieto, A., Pimentel, E.: A cloud-based Internet of Things platform for ambient assisted living. Sensors **14**(8), 14070–14105 (2014)
36. Parada, R., Melia-Segui, J., Morenza-Cinos, M., Carreras, A., Pous, R.: Using RFID to detect interactions in ambient assisted living environments. Intell. Syst. IEEE **30**(4), 16–22 (2015)
37. Ray, P.P.: Home health hub Internet of Things (H3IoT): an architectural framework for monitoring health of elderly people. In: 2014 International Conference on Science Engineering and Management Research (ICSEMR), pp. 1–3 (2014)
38. Chui, M., Löffler, M., Roberts, R.: The Internet of Things. McKinsey Q. **2**(2010), 1–9 (2010)
39. Jara, A.J., Zamora, M.A., Skarmeta, A.F.: An Internet of Things—based personal device for diabetes therapy management in ambient assisted living (AAL). Pers. Ubiquit. Comput. **15**(4), 431–440 (2011)
40. Luo, J., Chen, Y., Tang, K., Luo, J.: Remote monitoring information system and its applications based on the Internet of Things. In: FBIE 2009. International Conference on Future BioMedical Information Engineering, 2009, pp. 482–485 (2009)
41. Swan, M.: Sensor mania! The Internet of Things, wearable computing, objective metrics, and the quantified self 2.0. J. Sens. Actuator Netw. **1**(3), 217–253 (2012)
42. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of Things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
43. Lake, D., Milito, R., Morrow, M., Vangheese, R.: Internet of Things: architectural framework for eHealth security. J. ICT **3**, 301–330 (2014)
44. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., Chen, Q.: Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. Enterp. Inf. Syst. **9**(1), 86–116 (2015)
45. Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Kantarci, B., Andreescu, S.: Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: opportunities and challenges, pp. 285–292 (2015)
46. Talukder, A.K., Garcia, N.M., Jayateertha, G.M.: Convergence Through All-IP Networks. CRC Press (2013)
47. Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., Schreier, G.: The Internet of Things for ambient assisted living, pp. 804–809 (2010)
48. Domingo, M.C.: Review: an overview of the Internet of Things for people with disabilities. J. Netw. Comput. Appl. **35**(2), 584–596 (2012)
49. Rahmani, A.-M., Thanigaivelan, N.K., Gia, T.N., Granados, J., Negash, B., Liljeberg, P., Tenhunen, H.: Smart e-Health gateway: bringing intelligence to Internet-of-Things based ubiquitous healthcare systems, pp. 826–834 (2015)

50. Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J.-P., Riahi, M., Aberer, K., Jayaraman, P.P., Zaslavsky, A., Žarko, I.P., Skorin-Kapov, L., Herzog, R.: OpenIoT: open source Internet-of-Things in the cloud. In: Podnar Žarko, I., Pripužić, K., Serrano, M. (eds.) Interoperability and Open-Source Solutions for the Internet of Things: International Workshop, FP7 OpenIoT Project, Held in Conjunction with SoftCOM 2014, Split, Croatia, September 18, 2014, Invited Papers, pp. 13–25. Springer, Cham (2015)
51. The thing system. http://thethingsystem.com/dev/The-Thing-Philosophy.html
52. Xively. https://xively.com
53. Toulson, R., Wilmshurst, T.: Fast and Effective Embedded Systems Design: Applying the Arm Mbed. Elsevier (2012)
54. Hub of all things. http://hubofallthings.com
55. Arias Fernández, J., Bahers, Q., Blázquez Rodrıguez, A., Blomberg, M., Carenvall, C., Ionescu, K., Kalra, S.S., Koutsoumpakis, G., Koutsoumpakis, G., Li, H.: IoT-framework (2014)
56. Calvin-base. https://github.com/EricssonResearch/calvin-base
57. OpenRemote. http://www.openremote.org/display/HOME/OpenRemote
58. ThingWorx. http://www.thingworx.com/platform/
59. Sense tecnic wotkit. http://sensetecnic.com
60. Derhamy, H., Eliasson, J., Delsing, J., Priller, P.: A survey of commercial frameworks for the Internet of Things, pp. 1–8 (2015)
61. Valera, A.J.J., Zamora, M.A., Skarmeta, A.F.G.: An architecture based on Internet of Things to support mobility and security in medical environments, pp. 1–5 (2010)
62. Liu, Y., Zhou, G.: Key technologies and applications of Internet of Things, pp. 197–200 (2012)
63. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K.: Security challenges in the IP-based Internet of Things. Wirel. Pers. Commun. **61**(3), 527–542 (2011)
64. Gan, G., Lu, Z., Jiang, J.: Internet of Things security analysis, pp. 1–4 (2011)
65. Katagi, M., Moriai, S.: Lightweight Cryptography for the Internet of Things, pp. 7–10. Sony Corp. (2008)
66. Babar, S., Stango, A., Prasad, N., Sen, J., Prasad, R.: Proposed embedded security framework for Internet of Things (IoT), pp. 1–5 (2011)
67. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of Internet of Things. CoRR **abs/1501.02211** (2015)
68. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer **44**(9), 51–58 (2011)
69. Mukherjee, A.: Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. Proc. IEEE **103**(10), 1747–1761 (2015)
70. Ning, H., Liu, H., Yang, L.T.: Cyberentity security in the Internet of Things. Computer **46**(4), 46–53 (2013)
71. Kothmayr, T., Schmitt, C., Hu, W., Brunig, M., Carle, G.: A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication, pp. 956–963 (2012)
72. Raza, S., Shafagh, H., Hewage, K., Hummen, R., Voigt, T.: Lithe: lightweight secure CoAP for the Internet of Things. Sens. J. IEEE **13**(10), 3711–3720 (2013)
73. Li, F., Xiong, P.: Practical secure communication for integrating wireless sensor networks into the Internet of Things. IEEE Sens. J. **13**(10), 3677–3684 (2013)
74. Sethi, M., Kortoci, P., Di Francesco, M., Aura, T.: Secure and low-power authentication for resource-constrained devices, pp. 30–36 (2015)