Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 111 (2017) 770 – 779

Energy Procedia

8th International Conference on Sustainability in Energy and Buildings, SEB-16, 11-13 September 2016, Turin, ITALY

A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications

Iman Khajenasiri[a,]*, Abouzar Estebsari[b], Marian Verhelst[a], Georges Gielen[a]

[a]*Dept. of Electrical Engineering, ESAT, MICAS, KU Leuven, Kasteelpark Arenberg 10, B-3001 Heverlee (Leuven), Belgium.*
[b]*Department of Energy, Politecnico di Torino, Corso Duca degli Abruzzi, 24, Torino 10129, Italy*

Abstract

A smart city exploits sustainable information and communication technologies to improve the quality and the performance of urban services for citizens and government, while reducing resources consumption. Intelligent energy control in buildings is an important aspect in this. The Internet of Things can provide a solution. It aims to connect numerous heterogeneous devices through the internet, for which it needs a flexible layered architecture where the things, the people and the cloud services are combined to facilitate an application task. Such flexible IoT hierarchical architecture model will be introduced in this paper with an overview of each key component for intelligent energy control in buildings for smart cities.

Peer-review under responsibility of KES International.

Keywords: Internet of Things; smart city; cloud services; smart biulding; IoT applications, energy control; IoT design challenges.

1. Introduction

In the new configuration for the Internet of Things (IoT), a revision on the traditional concept of the internet is essential. In the traditional version, the internet is an infrastructure which provides the terminals for end users, while within the Internet of Things it provides the interconnection of smart objects within a ubiquitous computing environment [1]. The internet infrastructure will play a vital role as the global platform to enable the communication capability of physical objects. The novelty will be enabled by embedding electronics into objects, making them smart while being integrated into the worldwide physical infrastructure.

* Corresponding author. Tel.: +32 16325696.
E-mail address: iman.khajenasiri@esat.kuleuven.be

Peer-review under responsibility of KES International.
doi:10.1016/j.egypro.2017.03.239

The term Internet of Things refers to this internet-based architecture which facilitates the exchange of services, information and data between billions of objects, mostly smart. It was first introduced by Kevin Ashton in 1998 and has obtained a lot of attention in the industry and academia [2]. In some texts, it is addressed as the Internet of Everything (IoE) to emphasize the ubiquitous usage of the internet-enabled objects. IoT provides the connection between all these objects to facilitate and make people's lives more comfortable and efficient in all situations. Within this approach different aspects of both hardware and software solutions work together to realize the Internet-of-Things paradigm.

The IoT should be capable of connecting billions or trillions of heterogeneous devices through the internet, so there is a critical need for a flexible layered architecture. The IoT domain encloses a wide range of standardized or unstandardized technologies, software platforms and diverse applications. Therefore, a single reference architecture cannot be used as a layout for all possible concrete implementations. Though a reference model can be considered for IoT, most likely several reference architectures will coexist [3]. Here, we define the architecture as a framework in which the things, the people and the cloud services are combined to facilitate application tasks. Therefore, the reference model for the IoT can schematically be depicted as in Fig. 1.

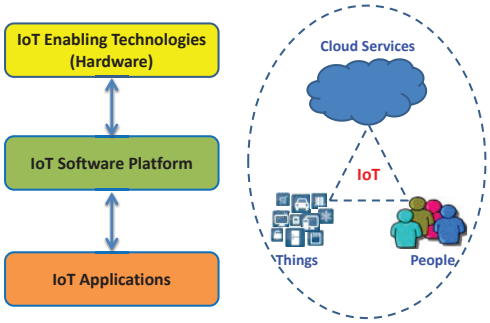

Fig. 1. The IoT architecture model.

An overview of each part of the IoT hierarchical architecture will be investigated in the following sections. The IoT applications in smart cities will be presented in Section 2. In Sections 3 and 4 IoT software and hardware infrastructures will be described with focus on intelligent energy control in buildings. In section 5, some IoT challenges are briefly discussed. This will help the reader to understand the IoT beyond the conventional layered networks where the user at the application layer is connected to the hardware. The implementation of an IoT system will offer the ability for smart objects to be identifiable, to communicate and to interact either among themselves, with building networks of interconnected objects, or with end users or other entities in the network. Developing technologies and solutions for enabling such an IoT vision is the main challenge ahead for IoT design engineers [1].

2. IoT Applications in Smart Cities

The IoT potentialities offer many possible applications. Some of these applications are shown in Fig. 2. Only some of them are currently completely deployed and in the future, there will be more intelligent applications for smarter cities, enterprises and factories. Smart city applications are developed not only to improve the management of urban flows but also to allow a real time response to challenges. Especially in this century, many emerging technological, economical and environmental changes have generated interest in smart cities. These changes include climate change [5], economic restructuring [6], ageing populations, and pressures on public finances [1]. A smart city can be considered as the general application category in which other domains such a smart home, smart grid, smart automotive and traffic management are included.

A smart home can be considered as a subcategory of smart cities. In this subcategory a residence' appliances, lighting, heating and air conditioning systems, video and audio streaming devices and security systems are capable of communicating with each other or through a central control unit in order to bring comfort, security and energy efficiency for home owners.

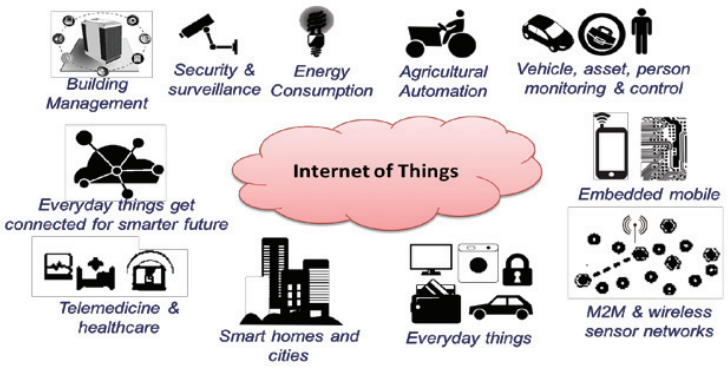

Fig. 2 Internet of Things application domains.

The research works on smart cities has attracted a lot of attentions in the last decade [7]. From market's point of view, the smart home is expanding rapidly and is expected to reach more than 100 billion dollars by 2022. In this application personal and family security is a key adoption motivation for the major consumers. In [8] a survey shows that 90% of people agree that security is one the most important reasons to purchase for a smart home system. The next motivation is costs saving as the exciting reason for the consumers to use smart home. In [9] it has been predicted that a typical family home may contain more than 500 smart devices by 2022, while currently for the most consumers, smart home is not an essential demand.

In European countries, since EU Parliament published a directive in 2002 to use the methodologies for increasing the energy efficiency in buildings [10], a lot of international research projects have established to use energy management system to reduce buildings' energy consumption. Some of these projects are: SEEMPubS (Smart Energy Efficient Middleware for Public Spaces) [11], DIMMER (District Information Modeling and Management for Energy Reduction) [12], AIM (A novel architecture for modeling, virtualizing and managing the energy consumption of household appliances) [13], IntUBE (Intelligent Use of Buildings' Energy Information) [14] and DEHEMS (Digital Environment Home Energy Management System) [15]. Among them SEEMPubS is one of the EU founded projects in which the main attention has given to development of an energy system for public and historical buildings.

Europe's historic buildings have visitors from all around the world every day. However, providing energy-efficient buildings without significant construction works can be a struggle. In SEEMPUBS project we were involved in developing an ICT-based energy management control system cope with avoiding possible damages caused by important building interventions due to energy management hardware installation [11], [16]. In this project a new computer-based system controls lighting, heaters, air conditioners and other environmental units in large buildings. The SEEMPUBS technology provides a central control system at software level which is connected wirelessly to energy structures placed in different parts of a building or even a number of buildings. Beyond the hardware, the most significant results have been on elaboration of an energy-efficient model for existing buildings and public spaces. This model can be applied to many different historic buildings to avoid construction work, disruption and possible damage, even with deploying new emerging technologies. As a user application, the Heating, Ventilation and Air Conditioning (HVAC) control applications include products, systems and services that target control strategies to save energy [17]. HVAC systems use IoT software and hardware infrastructures to achieve their objectives. An explanation of the applied energy control solution into an IoT home energy management system will be presented in reviewing of each of IoT's components in the following sections.

Another subcategory application for IoT in a smart city is where the automotive industry offers smart cars. From headlights to engine all systems in between request a range of innovative technologies in modern cars [18]. IoT will provide web-connected vehicles to implement telemetry, predictive maintenance, car-to-car and car-to-user connections. It is mostly desired to replace wire with wireless communications in a smart car while maintaining a safe and comfortable driving [19].

3. IoT Software Platform

The IoT hardware requires operating systems and communication protocols to interact with human (user) and other devices. There are middleware components that facilitate communication and exchange of information between devices. In IoT architectures, integration layers play an important role in combining and integrating information acquired from thousands of devices and presenting this information to users. In this section we review general software structure inside of an IoT system.

In design of an IoT software platform, scalability, the extensibility and interoperability between heterogeneous devices and their business models should be considered. In addition, IoT enabling technologies (hardware) may move geographically hence need to communicate with others in a real-time mode. This kind of operation necessitates decentralized and event-driven software architecture [20].

Service-oriented-architecture (SoA) ensures the scalability and interoperability of heterogeneous technologies in one platform. In a generic SoA four layers are defined [21],[22]: 1) sensing layer uses integrated hardware to sense things' statuses; 2) network layer which connects the things together and collects the data from hardware infrastructure, 3) service layer creates and manages services requested by users or applications; 4) interface layer enables the interaction methods with applications or users.

In a SoA for an IoT middleware, the software between objects (things which are equipped with sensors) and applications should provide object abstraction, service managements and service composition through a secure network. SoA-based architecture for an IoT middleware is shown in Fig. 3.

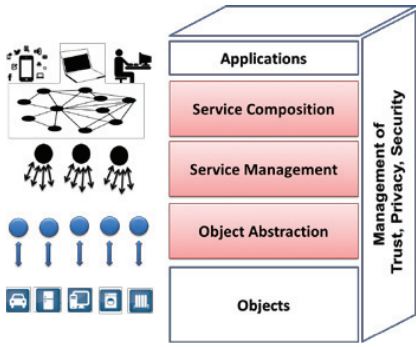

Fig. 3 Service-oriented-architecture for a middleware in IoT based on [22]

As an example of *Applications* in a SoA oriented approach, in SEEMPubS project, we implemented a HVAC system in which cooling and heating systems are controlled based on the presence of a user in buildings. In this control strategy a software application which is connected to a database uses the occupancy information, the residual space temperature, the outdoor temperature and the equipment capacity to keep the building temperature in a comfort zone during day and night. This control strategy will be available only using an IoT system in which users from different level of authorizations can control the room temperature at anytime and form anywhere. Nevertheless, an automatic control strategy is also applied to provide energy savings using the information collected by smart devices in order to switch on/off home appliances. A description about these smart devices technologies will be given in Section 4 while more details are presented by Atzori et al. [23]. The practical developed form of a self-adaptive HVAC system as a part of SEEMPubS intelligent ICT-based service system for monitoring and controlling the environmental conditions in a real existing building has been applied successfully. In this control strategy a preset schedule allows turning off the heating when the room is unoccupied, unless a presence is detected. However, the user can always override the system by changing the set-point temperature of the fan coils with an individual switcher. We have explained this control strategy in more detail in [17] and [24]. For an experimental case study, an average energy saving of 71% has been achieved during the test period of three days in summer. For the annual period and for the overall case test buildings, simulation results have been also presented: for these cases, the energy savings can reach up to 40% for lighting, 35% for heating and 30% for cooling. Fig 4 presents the percentage savings for heating, cooling and lighting obtained with the new control strategies with respect to

traditional (manual) controls (savings for test rooms with respect to reference rooms) in sample buildings. The results for a complete year have been determined by simulations.

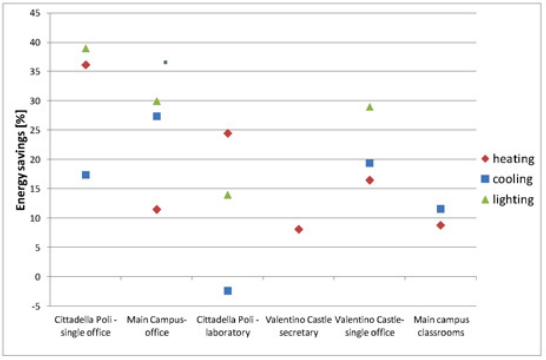

Fig. 4 Energy saving (in %) obtained for cooling, heating and lighting of the developed energy control strategy as a user-application in an IoT smart-home.

4. IoT Hardware Enabling Technologies

In an IoT system, a hardware is in charge of object identification, sensing desired parameters on objects (things), communicating information inside the IoT and primary processing and computation in the information [25]. For object identification, different addressing methods are used based on internet protocols (IPs) such as IPv4, IPv6, and 6LoWPAN [26], [27]. For the identification it should be notified that object's identification and address are different. While an object can be identified locally, for example inside a 6LoWPAN network, the object within the global network uses public IPs as the address. Identification methods aim to make a clear identity for any object inside the network. Sensing refers to actuators and sensors which convert the measured information, such as temperature in smart home or heart rate in e-health, to electrical signals. Electrical signals then can be understood by electronics circuits for further processing and transmission through a communication link to a data base. In the field of sensor and actuators design many works have been presented in design and implementation of precise, invasive/noninvasive and miniaturized sensors [22].

Communication link technologies should provide the infrastructure for the connection of smart devices (sensor nodes). The IoT sensor nodes should work normally under severe designs specifications including low-power consumption, and operation in noisy environment. Currently, there are different communication protocols which can be used for IoT applications, such as WiFi, IEEE 802.15.4, Bluetooth, Z-Wave, LTE-advanced, ZigBee, IrDA, etc. Different technologies work at frequency bands between a few MHz to tens of GHz. The frequency bands are determined by local and international official regulators. General design specifications for each technology are optimized for a certain application. For example, a fitness bracelet needs only a low energy and short distance communication range, so Bluetooth technology as a short-range and low-data rate standard is used to connect the fitness bracelet to smart phone. Another example is networks connections inside/outside of a car. In this case, a high performance technology such as mobile 4G is required to operate in a car moving at high speed. For smart home, a combination of ZigBee, Wi-Fi and promising solutions like UWB can be seen. All of these applications need specific hardware design and software apps to embed a variety of wireless protocols into "things".

The very first pioneer implemented technology for object identification as the primary usage of IoT is realized using radio frequency identification (RFID) technology [28]. In EPC-GEN2 RFID technology, a machine-to-machine (M2M) communication is implemented between a tag and a reader in which the RFID reader sends a query signal to the tag and receives reflected signal from the tag (typically a passive tag), which in turn is passed to the database. The database is connected to a processing center and identifies objects based on the reflected signals. RFID tags can be equipped with battery so called, active tag, or implemented based on passive circuits, called passive tag, or a combination of both called semi-active/passive. In general, the active RFID tags should consume very low power in order to enable supplying from a scavenger which converts an environmental energy type e.g. RF signal to

DC power. Another very important feature in designing RFID tags is the implementation cost. For most of the identification applications in IoT, for example for object identification in a warehouse, the tag should be very chip and easy to plugin. Luckily, using CMOS technology has enabled implementation of low-cost RFID tags, however the price is much higher compared to identification techniques based on barcode. A RFID system can work in different frequency bands. For Low-Frequency (LF) it works at 125 – 134.2 kHz, for High-Frequency (HF) band it works at 13.56 MHz. For Ultra-High-Frequency (UHF) bands, where the EPC-GEN2 protocol is defined, it works at 850 – 960MHz.

Near Field Communication (NFC) protocol which works at 13.56 MHz frequency band is based on RFID technology which supports up to 424 kbps. The range for NFC communication is around 10cm. This technology is based on ISO 180000-3 air interface protocol and only provides a point-to-point network. This technology is growing for the next generation of payment systems [29]. This contactless communication protocol has been developed for very short distance applications and has already integrated in many smartphones in the market.

Ultra-Wideband (UWB) communication technology is another IoT enabling technology which is introduced for short range applications especially when an accurate positioning is required. This is a unique feature for UWB signals thanks to short-pulses of UWB signals in the time domain. It also consumes very low power because of pulsed based nature of the transmitted signals. The UWB technology can be a useful technology in the IoT applications where low-power and high position accuracy are demanded [30], [23].

WiFi is another communication technology that is widely in use for data exchange between WiFi-enabled devices in home and office environments. WiFi provides longer range and higher data rate compared to protocols such as Bluetooth and ZigBee at the expense of higher energy consumption. The WiFi equipped sensor nodes should be charged very frequent (every day or every other days depending on the data usage). So, for many low-power and autonomous applications are not suitable.

Bluetooth is a communication technology that presents moderate data rates for short range applications which optimized for low power consumption [31]. Recently, Bluetooth and Bluetooth low energy are two types of this protocol which provide IP connectivity in order to support IoT [32].

IEEE 802.15.4 standard is characterized to investigate low data rate devices with a several months to several years' battery life with low complexity implementation [33]. It operates in an unlicensed band for sensor nodes. Sixteen channels in the 2.4GHz ISM band, ten channels in the 915MHz and one channel in the 868MHz band are allocated to this standard. IEEE 802.15.4 defines general physical layer and medium access control layer requirements for standard compliant devices. This standard is the basis for ISA100, ZigBee and WirelessHART. Each of them extends further by developing the upper layers which are not specified in the standard. The main application target for this standard is for low-rate wireless personal area networks (WPAN) with low power consumption. Many IEEE 802.15.4 sensor nodes mainly based on ZigBee, sub-protocol for IoT applications have been developed and introduced in the market [34].

Mobile communication protocols such as GPRS, 3G and 4G are introduced originally for high-speed data communications between mobile phones. However, this data networks can be considered as one of the enabling technologies for IoT application where a high data rate is demanded. The latest commercialized version of mobile networks is LTE-advanced in which a peak download rate of 1Gbit/s is expected. In spite of the high power consumption of LTE-advanced technology, it is in use in mobile devices especially for online high-definition (HD) video streaming [35].

Cellular systems industry is expecting an increase by a factor of 1000 in network capacity over the next decade to meet higher demanding traffic. In addition, different IoT devices each working based on different technology will be connected and managed by a user smartphone device. Hence, the mobile industry is working to develop fifth generation of mobile services to manage big data transfer between mobile phones and cloud services at the same time to maintain the latency as low as possible. However, many IoT application domains, such as M2M application, should be low cost, cheap with low-data rate which is a very different requirement compared to smartphone user interests.

Besides the enabling communication protocols for IoT which differ in terms of communication range, data rate, latency and power consumption, the IoT hardware should also enable a level of local computation and processing on the sensed data before the transmission. These computations are performed in the processing units e.g. microprocessors, microcontroller, FPGAs and system-on-chips (SOCs). Different hardware platforms are developed

to be used in IoT applications such as WiSense, Arduino, Mulle, Intel Galileo and ARM. The interaction between processing unit, communication protocols and cloud platforms are then implemented using software operating systems such as LiteOS and TinyOS [36], [37].

As it was discussed in Section 3, a presence-based control strategy is applied in our work to obtain a better energy saving using promising attributes of IoT. The information analysed at user level come from smart devices as the hardware of an IoT system. In addition, smartphones can be used to monitor, control, and manage the energy control systems remotely from anywhere and anytime. After the authentication and authorization, the occupants are allowed to modify and change their energy saving policies by interacting with the smart devices' information. In our developed framework, we used different smart devices to monitor buildings temperature, appliances energy consumption and user presence. The utilized smart devices use different technologies which discussed here including ZigBee, Bluetooth, WiFi and UWB. Thanks to applying an integration layer in the software platform, the interoperability of these heterogeneous devices achieved successfully.

In summary, there are plenty of enabling technologies and standards introduced for IoT applications. Their specifications are optimized based on the available application requirements and are updated frequently to satisfy promising application needs.

5. IoT Design Challenges

As stated in Section 1, IoT architecture can be considered as a three-layers system consist of IoT enabling technologies, IoT software and IoT applications and services. The main vision for an IoT system is to fulfill a reliable, secure and user-friendly interconnection of different layers to finally provide a certain quality of service for maximum number of users. However, individual layers can be designed independently, but their interconnections cause some issues and challenges such as interoperability of heterogeneous systems, security and privacy issues, etc. In this section, we address a brief review of some key challenges in IoT discussed in the recent literature and works.

Some examples of IoT challenges are discussed in literature such as: reliability, mobility, interoperability, scalability, availability, security, big data analytics, cloud computing, low-power and modular sensor nodes design [38], [39], [40], [41]. We briefly overview these challenges in the next few paragraphs.

Availability: The concept of availability refers to the capability of an IoT system to provide the demanding services for the customers anytime and anywhere [42] . This availability applies to both IoT hardware and software.

Reliability: Any IoT system should be reliable. It means that the system should be successful in delivering IoT service at different circumstances. This feature is more critical in the field of emergency response applications [43]. A reliable IoT system should utilize a failure resilient communication network. A reliable network distributes the information successfully throughout all the IoT layers. An unreliable network leads to long delays and data loss which finally ends to wrong decisions. Wrong decisions in an IoT system may lead to unpredictable scenarios such as confusion, disorderliness and irrecoverable damages. For example, a failure in an IoT e-health monitoring system may lead to patient death.

Interoperability: one of the biggest issues in deploying tens of heterogeneous smart devices with different platforms is interoperability. Different platforms both at the software and hardware layers should be integrated in an IoT system. Thus, IoT sensor nodes' manufacturers and IoT application developers should consider interoperability to ensure delivery of requested services for all users regardless of whether kind of hardware platform that they use. Modern smartphones support different communication protocols such as GSM, 3G, 4G, NFC, WiFi and Bluetooth to ensure the interoperability of the smartphone in different scenarios. From software point of view, the IoT programmers should develop applications which allow adding new functions with no issue for other applications and communication protocols. Thus, interoperability is a critical feature in design and build of IoT services to meet the user requirements [44]. One challenge in realizing interoperability is that different vendors interpret the same standard differently [45]. In order to solve this issue, some research works have been developed to provide semantic interoperability for IoT [46], [47]. In SEEMPubS project, we obtained interoperability of heterogeneous devices using an integration layer between sensor nodes and database. It translates the technology commands to a user understandable format. This layer resides at the lowest layer in the middleware platform [16].

Scalability: In an IoT system scalability addresses the system ability to be extended by new modules (including sensor nodes, devices, services and applications) for users without affecting the quality of available services. If a

system is not scalable, then it will not be able to handle future expansion when new technologies arrive, at both hardware and software layers. This leaves customers with unusable systems and devices that should either be replaced or be completed with a new design. Both approaches are expensive. In addition, a scalable IoT system should remain operational when one part of it (for example a number of sensor nodes in a home energy management system) remove. One approach in utilizing sensor nodes and technologies inside an IoT system is using ad-hoc networks which can be added to the system with minimum hardware and software configurations.

Performance management: deploying billions of internet-enabled devices cause many issues for service providers to manage the fault, performance and security of the devices. A management service should monitor M2M communications inside the IoT, manage the accessibility of different user-levels, manage the configurations of network devices, and provide services priority management [48], [49].

Security and privacy: in heterogeneous networks as used in an IoT system, it is difficult to guarantee a high level of privacy and security for users. One of the reasons for this issue is the lack of common standard for IoT security. Insides the global internet infrastructure, billions of objects distribute information including the keys and passwords that should be protected and encrypted with a high-level of security [25]. Based on survey of Xu et al. [50], the most important security requirements include authentication and data tracking, mutual trust, data and information integrity, and digital forgetting. In addition, the privacy is the most important feature which lets the users to trust a system. Pervasive usage of smart devices with private information about a user necessitates using appropriate content privacy techniques to protect clients' information against hackers, criminal activities, and terrorist attacks [51]. Despite many technologies introduced to achieve customers' data privacy [52], still IoT systems privacy and security needs to be upgraded frequently to enhance the information privacy techniques.

Big data analytics: the expansion of IoT system demands saving a huge amount of information in data bases. This data may be processed real-time which requires fast and power efficient techniques. Big data analysis is one the most challenging research fields in IoT [53]. Big data needs smart and efficient data bases. This big data comes from connected devices with different level of processing capabilities in which they store, process and retrieve the data. In smart-device data processing unit trades with the device power consumption. More processing may lead to higher power consumption comparing to the case that it transmits raw data to a central processing unit. However, optimization of the amount on-the-node data processing is highly dependent to the application specifications. Some of these specifications are sensing parameters, smart device throughput, network traffic, deployed environment, power supply availability, internet download/upload speed, and communication technology. In the recent years, the amount of the stored data in third-party software and hardware is increasing. In this case, the amount of data that is saved in local servers reduces. Internet infrastructure of IoT guarantees access of this data anywhere and anytime using cloud services with external servers.

Cloud services refers to a data management where the internet is such a cloud in which IoT experts, researchers, companies and end-node customers use to save and process big data in remote, reliable and low-cost servers [54], [55]. Cloud computing enables a ubiquitous and on-demand access to shared processing resources. Cloud computing may be the best choice for internet-enabled smart devices to save and process big data. However, it encounters some practical challenges such as standardization, synchronization between different real-time services, security and privacy issues [56].

Smart device design: ever-increasing number of smart devices (sensor nodes) for IoT applications is inevitable. In the near future, every person will carry on several smart devices that require power sources to achieve sensing, computation and communication tasks. Regardless of the discussed software challenges, a smart device encounters many issues at the hardware level. However, many designed sensor nodes consume low-power, still using power hungry protocols such as ZigBee for short-range applications or LTE for mobile communication demand regular battery replacement or battery recharging. In general, smart devices for IoT applications should be ultra-low-power to work for a long time with a small size battery or enable permanent operation with scavenging energy from the environment. However, the available energy sources to supply battery-less devices are limited in most of the environments. Thus, many researches on energy scavenging techniques, power management in sensor nodes and low-power circuit design are ongoing to enable integration of long lifetime smart devices into an IoT system.

Moreover, cost of smart devices should be low enough for private customers. Currently, many off-the-shelf IoT products for smart home, agriculture, industrial or e-health applications are expensive which for many private customers is not economic. Another challenging specific requirement for smart devices is long range communication

requirement which can be limited by surrounding obstacles, environmental barriers, and signal interferences. A wireless smart device may be applied to a harsh environment, for example inside a factory. A robust and reliable smart device should operate correctly at this type of environments. Modularity and scalability of smart device circuits is another challenge when utilized in an IoT system. The ad-hoc networks offer a modular structure in which a smart device can be deployed as a plugin concerning the instant requirements and limitations of an application. In total, a smart device with sensing, computing and communication blocks should be power efficient, low size and cost efficient.

6. Conclusions

It is anticipated that in the near future the Internet of Things will widely be used as the network to connect billions of objects. All the services and contents will be available around us for current and upcoming applications. The new connection structure enables new ways for doing the tasks, working, social networking and entertainment, hence enabling a new lifestyle. The Internet of Things offers many possible applications, only few of which are currently deployed. In the future, there will be many applications for smart cities, such as intelligent energy control for buildings. An IoT system should be able to connect many heterogeneous devices through the internet, which explains the critical need for a flexible layered architecture. In this paper, an IoT architecture model has been described in which the things, the people and the cloud services are combined to facilitate application tasks. The architecture's key components have been described with the application of smart cities in mind. After an overview of IoT software platforms and enabling technologies, some of the IoT challenges coming from IoT software and hardware immaturity have been described. The main promises of an efficient IoT system will be realizable when these problems will be overcome, hence establishing a secure, reliable and user-friendly IoT system, offering daily comfort and convenience to users.

References

[1] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw*. 2012 Sep 30;10(7):1497-516.
[2] Santucci G. From internet of data to internet of things. In Paper for the International Conference on Future Trends of the Internet 2009 Jan 28 (Vol. 28).
[3] Digital Agenda for Europe: IoT Architecture. Available online: https://ec.europa.eu/digital-single-market/en
[4] IoT Applications. Available online: http://iotworm.com/internet-of-things-applications-area/
[5] Rosenzweig C, Solecki W, Hammer SA, Mehrotra S. Cities lead the way in climate-change action. *Nature*. 2010 Oct 21;467(7318):909-11.
[6] Komninos N, Pallot M, Schaffers H. Special issue on smart cities and the future internet in Europe. *Journal of the Knowledge Economy*. 2013 Jun 1;4(2):119-34.
[7] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. *IEEE IoT-J*. 2014 Feb;1(1):22-32.
[8] 2015 state of the Smart Home Report. Available online: https://www.icontrol.com/wp-content/uploads/2015/06/Smart_Home_Report_2015.pdf
[9] Gartner Information technology predictions, report 2014. http://www.gartner.com/imagesrv/pdf/Gartner_2014_annual_report.pdf
[10] EU energy efficiency directive. Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l27042
[11]SEEMPubS FP7 project. Available online: https://ec.europa.eu/digital-single-market/en/news/seempubs-maximum-energy-savings-minimum-intervention-historic-buildings.
[12] DIMMER FP7 project,. Available online: http://dimmer.polito.it
[13] AIM FP7 project. Available online: http://www.ict-aim.eu
[14] IntUBE FP7 project. Available online: http://zuse.ucc.ie/intube/
[15] DEHEMS project. Available online: http://www.dehems.eu
[16] Khajenasiri I, Patti E, Jahn M, Acquaviva A, Verhelst M, Macii E, Gielen G. Design and implementation of a multi-standard event-driven energy management system for smart buildings. In 3rd IEEE Global Conference on Consumer Electronics (GCCE) 2014 (pp. 20-21). IEEE.
[17] Khajenasiri I, Virgone J, Gielen G. A presence-based control strategy solution for HVAC systems. In 2015 IEEE International Conference on Consumer Electronics (ICCE) 2015 Jan 9 (pp. 620-622). IEEE.
[18] IoT for automotive. Available online: http://www.ti.com/ww/en/internet_of_things/iot-applications.html
[19] Liu T, Yuan R, Chang H. Research on the Internet of Things in the Automotive Industry. In *ICMeCG*, 2012 International Conference on 2012 Oct 20 (pp. 230-233). IEEE.
[20] Li S, Da Xu L, Zhao S. The internet of things: a survey. *Inform Syst Front. 2015* Apr 1;17(2):243-59.
[21] Wang XV, Xu XW. DIMP: an interoperable solution for software integration and product data exchange. *Lect Notes Bus Inf*. 2012 Aug 1;6(3):291-314.

[22] Atzori L, Iera A, Morabito G. The internet of things: A survey. *Comput Netw*. 2010 Oct 28;54(15):2787-805.
[23] Khajenasiri I, Zhu P, Verhelst M, Gielen G. A Low-Energy Ultra-Wideband Internet-of-Things Radio System for Multi-Standard Smart-Home Energy Management. *IEIE SPC*. 2015;4(5):354-65.
[24] Patti E, Acquaviva A, Jahn M, Pramudianto F, Tomasi R, Rabourdin D, Virgone J, Macii E. Event-driven user-centric middleware for energy-efficient buildings and public spaces. *IEEE Systems Journal*. 2016 Sept 1137-1146 (10).
[25] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. ICST. 2015 Nov 18;17(4):2347-76.
[26] Kushalnagar N, Montenegro G, Schumacher C. IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. 2007.
[27] Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 packets over IEEE 802.15. 4 networks. 2007.
[28] Want R. An introduction to RFID technology. IPC. 2006 Jan;5(1):25-33.
[29] Fisher M, inventor; Blaze Mobile, Inc., assignee. Conducting an online payment transaction using an NFC enabled mobile communication device. United States patent US 8,352,323. 2013 Jan 8.
[30] Kshetrimayum RS. An introduction to UWB communication systems. IEEE POTENTIALS. 2009 Mar;28(2):9-13.
[31] McDermott-Wells P. What is bluetooth?. *IEEE potentials*. 2004 Dec;23(5):33-5.
[32] Press releases detail: Bluetooth technology website. Bluetooth Technol. Website, Kirkland, WA, USA, Sep. 2014, available online: http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=197
[33] Karapistoli E, Pavlidou FN, Gragopoulos I, Tsetsinas I. An overview of the IEEE 802.15. 4a standard. *IEEE Commun Mag*. 2010 Jan;48(1):47-53.
[34] ZigBee verified product. Available online: http://www.zigbee.org/zigbee-products-2/
[35] 3G vs. 4G. Available online: http://ee.co.uk/articles/4g-vs-3g--what_s-the-difference-
[36] Levis P, Madden S, Polastre J, Szewczyk R, Whitehouse K, Woo A, Gay D, Hill J, Welsh M, Brewer E, Culler D. Tinyos: An operating system for sensor networks. In *AMB INT* 2005 (pp. 115-148). Springer Berlin Heidelberg.
[37] Cao Q, Abdelzaher T, Stankovic J, He T. The liteos operating system: Towards unix-like abstractions for wireless sensor networks. In IPSN'08. 2008 Apr 22 (pp. 233-244). IEEE.
[38] Chen YK. Challenges and opportunities of internet of things. In17th *ASIA S PACIF DES AUT* 2012 Jan 30 (pp. 383-388). IEEE.
[39] Billure R, Tayur VM, Mahesh V. Internet of Things-a study on the security challenges. In IACC, 2015 IEEE International 2015 Jun 12 (pp. 247-252). IEEE.
[40] Favaro J. Strategic research challenges in the Internet of Things. In2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS) 2015 May 13 (pp. 1-1). IEEE.
[41] Blaauw D, Sylvester D, Dutta P, Lee Y, Lee I, Bang S, Kim Y, Kim G, Pannuto P, Kuo YS, Yoon D. IoT design space challenges: Circuits and systems. In *VLSI Technology*: Digest of Technical Papers, 2014 Symposium on 2014 Jun 9 (pp. 1-2). IEEE.
[42] Costa DG, Silva I, Guedes LA, Vasques F, Portugal P. Availability issues in wireless visual sensor networks. *Sensors*. 2014 Feb 12;14(2):2795-821.
[43] Maalel N, Natalizio E, Bouabdallah A, Roux P, Kellil M. Reliability for emergency applications in internet of things. In 2013 IEEE International Conference on Distributed Computing in Sensor Systems 2013 May 20 (pp. 361-366). IEEE.
[44] Dunkels A, Eriksson J, Tsiftes N. Low-power Interoperability for the IPv6-based Internet of Things. In Proceedings of the ADHOC'11, Stockholm, Sweden 2011 May 11 (pp. 10-11).
[45] Ishaq I, Carels D, Teklemariam GK, Hoebeke J, Abeele FV, Poorter ED, Moerman I, Demeester P. IETF standardization in the field of the internet of things (IoT): a survey. *Journal of Sensor and Actuator Networks*. 2013 Apr 25;2(2):235-87.
[46] Kiljander J, D'elia A, Morandi F, Hyttinen P, Takalo-Mattila J, Ylisaukko-Oja A, Soininen JP, Cinotti TS. Semantic interoperability architecture for pervasive computing and internet of things. *IEEE access*. 2014;2:856-73.
[47] Gyrard A, Datta SK, Bonnet C, Boudaoud K. A semantic engine for Internet of Things: cloud, mobile devices and gateways. InInnovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015 9th International Conference on 2015 Jul 8 (pp. 336-341). IEEE.
[48] Rajan MA, Balamuralidhar P, Chethan KP, Swarnahpriyaah M. A self-reconfigurable sensor network management system for internet of things paradigm. InDevices and Communications (ICDeCom), 2011 International Conference On 2011 Feb 24 (pp. 1-5). IEEE.
[49] Van den Abeele F, Hoebeke J, Moerman I, Demeester P. Fine-grained management of CoAP interactions with constrained IoT devices. In 2014 IEEE Network Operations and Management Symposium (NOMS) 2014 May 5 (pp. 1-5). IEEE.
[50] Xu T, Wendt JB, Potkonjak M. Security of IoT systems: Design challenges and opportunities. In Proceedings of the 2014 *IEEE IC CAD* 2014 Nov 3 (pp. 417-423). IEEE Press.
[51] Weber RH. Internet of Things–New security and privacy challenges. *Computer Law & Security Review*. 2010 Jan 31;26(1):23-30.
[52] Dierks T. The transport layer security (TLS) protocol version 1.2.
[53] Riggins FJ, Wamba SF. Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In System Sciences (HICSS), 2015 48th Hawaii International Conference on 2015 Jan 5 (pp. 1531-1540). IEEE.
[54] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM. 2010 Apr 1;53(4):50-8.
[55] Mell P, Grance T. The NIST definition of cloud computing.
[56] Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. *IEEE SECUR PRIV*. 2011 Mar;9(2):50-7.