Internet of Things Shaping Smart Cities: A Survey

Arsalan Shahid, Bilal Khalid, Shahtaj Shaukat, Hashim Ali and Muhammad Yasir Qadri

Abstract Driven by the advances in hardware and software technologies, the term Internet of things has emerged as a worldwide framework of 'smart' internet-based interconnected electronic devices through web having a significant impact in the betterment of our traditional living style. The use of these web connected embedded devices, as Information and communication technologies for re-shaping modern cities, lead to the concept of smart cities. This chapter surveys the most important domains of smart cities and illustrates the recent research and development in them. After identifying critical areas, the chapter also highlights and discusses the issues and research gaps in recent technologies. Finally, it presents the opportunities and research directions in future advancements of intelligent cities.

Keywords Intelligent cities · Smart grids · Applications of internet of things (IoT) · Smart homes

A. Shahid (✉)
School of Computer Science and Informatics, University College Dublin, Belfield Dublin 4, Ireland
e-mail: arsalan.shahid@ucdconnect.ie

B. Khalid · S. Shaukat
Department of Electrical Engineering, HITEC University Taxila, Taxila, Pakistan

H. Ali
Department of Computer Science & Engineering, HITEC University Taxila, Taxila, Pakistan
e-mail: hashim.ali@hitecuni.edu.pk

M.Y. Qadri
School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK
e-mail: yasirqadri@acm.org

N. Dey et al. (eds.), *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, Studies in Big Data 30,
DOI 10.1007/978-3-319-60435-0_14

1 Introduction

1.1 Background of IoT

Nowadays, around two billion individuals across the globe utilize the Internet for browsing the web, sending and receiving messages, accessing multimedia content, playing games, using social networking applications and numerous other activities [1]. While more individuals will access such a worldwide data and correspondence foundation, another huge jump forward is coming, identified with the utilization of the internet as a worldwide stage for letting intelligent devices impart, dialog, process and organize. It is unsurprising that, within the following decade, the Internet will exist as a consistent framework of great systems and organized items [2]. Sensors and embedded electronic devices will be surrounding us, generally accessible, ready to make new applications, empowering better approaches for working, interfacing, amusement and living. In such a perspective, the traditional idea of the Internet as a framework system connecting with end-clients' terminals is fading, leaving space to a thought of interconnected "smart" objects forming pervasive computing environments [3]. The Internet foundation is not vanishing. Despite, it is holding its fundamental part as global backbone for overall data sharing and dispersion, interconnecting physical objects with registering/correspondence abilities over an extensive variety of administrations and innovations. This development is getting empowered by the embedding of electronics into everyday physical objects, making them "smart" and letting them flawlessly coordinate within the global cyber-physical infrastructure. This will offer ascent to open new doors for the information and communication technologies (ICT) segment, paving the way to new administrations and applications able to influence the interconnection of physical and virtual domains. Within such perspective, the term "Internet of things" (IoT) is comprehensively used to refer the subsequent worldwide system of interconnecting smart objects by means of developed internet enhancements and prearrangement of supporting technologies to acknowledge such dream [4, 5].

Figure 1 shows a typical representation of IoT in which different physical and virtual devices are connected to the web and ultimately sharing information to form a smart network of objects.

1.2 Applications of IoT

From the past few years, the research in IoT development has enabled over billions of devices to communicate and work efficiently via internet. Some of very well-known and recent applications of IoT includes smart home appliances, intelligent wearables such as smart watches, IoT in poultry, connected automotive, efficient retailing, smart farming, smart environment control including early earth

Fig. 1 A typical concept of internet of things

quake detection and snow level monitoring, smart agriculture enabling effective monitoring of green houses and quality of water and much more. The research towards being smarter has evolved to the extent that intelligent machines, i.e., are now getting integrating with qualities of having sensations like human [6]. A very recent emergence of robot pain (can a robot feel pain?) has attracted the attention of so many researchers. Ultimately, the aim is to have the world with smartest machines interconnected with each other via internet to bring human living standards to a far next level. In addition to this, IoT has also enabled eHealth that includes automatic patient surveillance, medical refrigerators to keep medicines/vaccines in a very controlled environment and fall detection systems in rooms that help elderly or disabled people who are living independently. In short, IoT development has been making human life easier and much more comfortable than ever.

1.3 Emergence of Smart Cities

With the ever increasing trend towards development of intelligent objects, the modern world is evolving with the concept of a broader term known as "smart cities". In simple, efficient utilization of resources, enhanced quality with improved performance are the key characteristics of devices; embedded together with the sensor networks, lead to IoTs and their use, as ICT results, in shaping smart cities [7].

This chapter presents a survey on most important components of smart cities by exploring advancement in smart technology; featuring a new role model for people

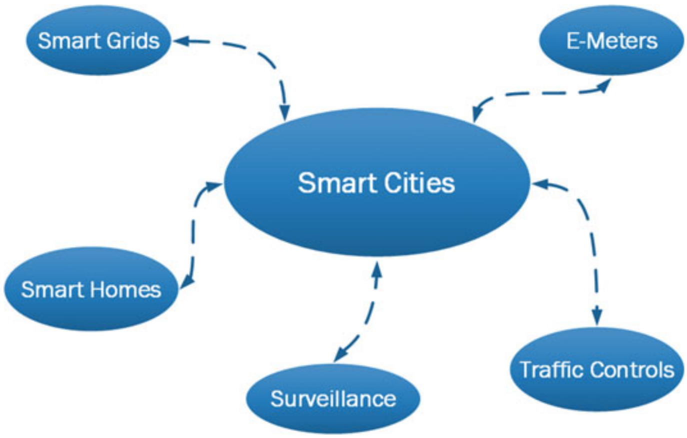

Fig. 2 A typical concept of internet of things

to make better use of the resources followed by research gaps and suggestions to further improve the living standards (see Sects. 2 and 3). Figure 2 shows the different aspects of smart cities covered in our survey. This chapter also highlights the challenges and critical shortcomings in the development in the area of smart city.

The rest of the chapter is organized as follows. Section 2 covers the major part of this chapter; starting with a detailed review of recent researches in the development of smart grids (see Sect. 2.1). Followed by, one of the major contribution of IoTs in the development of smart cities i.e. intelligent e-meters, in Sect. 2.2. Then, we illustrate smart homes that are featuring a new role model for people to make better use of the resources and improve living standards (see Sect. 2.3). In Sect. 2.4, surveillance cameras, an important product for ensuring security from thefts and serve in many other daily life applications, as well as for military purposes, have been covered. Lastly, advancements in smart traffic controls as an application of IoTs have been presented (see Sect. 2.5). In Sect. 3, we have discussed the challenges, opportunities and future directions in smart cities. Finally, in Sect. 4, conclusion is presented.

2 Smart Cities

The term “smart cities” refers to the aspect of availability and use of technology in a society or a region, which determine how much energy is being consumed and what ratio of output is being achieved by the use of such technology. All data, collected from embedded devices, sensors and other machines is gathered and analysed to extract meaningful information to output intelligent set of systems and to provide new services to the business, citizens and public administrations. The idea of smart city is not only restricted to the industrialization and administrative domains but is effectively related to the environment and atmosphere as well. Monitoring and control over the contaminants, caused by the industrial or instrumental components, is a major consideration which smart cities developers are taking into account. The ever increasing population and geographical boundaries of cities and towns also plays an important role in the communication of humans and thus effecting their daily life actions [8, 9]. In this section, we present the most trending R&D in the development of smart cities and its main features.

2.1 Smart Grids

Technological advancements are not restricted to any particular field or industry. Modern cities demand an infrastructure that is completely integrated and can balance efficiently the potential to meet the innovative challenges and competitions [10]. These challenges include the way from how we drive cars to how we make purchases and even how we get energy for our homes, from sharing of large data to the utilization of information into work, from management and administration and implementation of plans, from transportation to the medical services and many more. Internet infrastructural advancement along with the technological limits and its modification is the interest of scientists and researchers in modern world. In this section, we discuss a recently emerged form of power grid, i.e., smart gird (SG).

Generally, the term grid or power grid is used for electrical power infrastructure that may control all or a portion of the accompanying four electricity operations, i.e., (1) power generation, (2) power transmission, (3) power distribution, and (4) power control. A smart grid, is also referred to as intelligent grid, which is an upgrade of the classical twentieth century power grid [11]. The conventional grids are by and large used to transfer power from a couple of focal generators to clients. Interestingly, the SG utilizes two-route path of power as well as data to make a robotized and efficient network. Apart from two-way communication, some other important features of SG include its digital design nature, complete sensors integration, distributed generation, self-monitoring and provision of many customer choices [12]. Although a complete and accurate definition of smart grids has not been presented yet; but, National Institute of Standards and Technology (NIST) has presented a conceptual model of intelligent power grids, shown in Fig. 3. This applied model partitions the SG into several functional areas. Each area incorporates one or more SG on-screen characters, including gadgets, frameworks, or projects that settle on choices and trade data that is vital for performing applications. The customers are the end users of all the smart power transmission facilities whereas the service providers are the companies providing electrical facilities. Markets are the operators of these smart facilities who regulate the transmission and supply them to individuals through distribution section.

Unlike traditional power grids, smart grid transmission enable two-way electricity and information flow. An important power generation mechanism adapted in smart grids is distributed generation (DG). The key advantage of DG is the

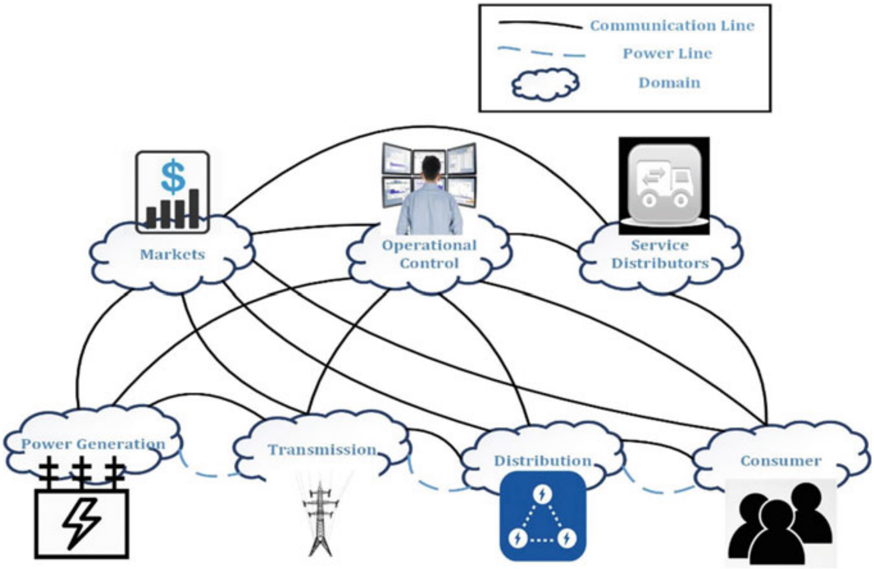

Fig. 3 Conceptual design of smart grids by NIST (adapted from [13])

distributed energy resources (DER) in the form of micro grids, i.e., small solar panels and wind turbines (ranging from 4 kW up to 10,000 kW) to improve quality, reliability and efficiency. This prevents the power distribution problems among users even if some small micro-grid fails operation or is removed from the system. Just like the advancements of power distribution systems, the transmission section of these modern grids are also improved driven by the modern power electronic technology and infrastructure challenges such as increasing load demands. As described in Byun et al. [10], on the basis of functionality, transmission part of SG can be further divided into three subsections, i.e., smart control centers, smart substations and intelligent transmission networks. The modern control centers are smart in a sense that they provide additional facilities of analysis and visualization with power flow monitoring. The smart substations are yet to be evolved with an expectation to have features like digitalization, self-healing and automatization. Finally, the new transmission networks have been enhanced by the improved electronics, sensing and communication technology helping to obtain improved quality of power and system security.

With the introduction of telecommunication phenomena in power grids, there comes a need of dealing with possible cyber security threats that may arise in smart grids [14]. Security analysts are required to pay attention on mechanism of power grids to meet the arising security issues. Therefore, cyber security is one of the main concerns in smart grids. In addition to this, the grid developers and operators also need to have a strong understanding of cyber security problems of SG era. Some of the very well-known attacks includes *stuxnet* and *night dragon*. Stuxnet causes harm to control system by reprogramming the system and hiding the specific changes. Whereas, night dragon is a mixture of techniques like social engineering, phishing, and system exploitation to harm sensible SG information.

Genge et al. [15] presented a middleware technique (SCYAMIX) having common features of HERMIX [16] and AMICI [17] platform for bringing in the real-time simulation capabilities. SCYAMIX was aimed to specifically ensure the real-time cyber security of smart grid architecture by considering its advanced features of energy management, distribution and metering. Authors claim SCYAMIX to be the first presented system for bringing in a Sensei/IoT compliant implementation. The system is to view communication protocols in detail with real-time software simulation. Their work also presented the efficiency of middleware through detailed demonstrations; and, a case study to overview the integration of other platforms such as ADHOC networks and HERMIX modules interaction with extensible messaging and presence protocol (XMPP) servers. However, their work lack the proper explanation of performance capabilities and tests in relation to real-world scenario.

Furthermore, security issues and challenges for the IoT-based smart grid for creating a secure network in order to keep track the real-time performance of the energy consumption and energy generation are discussed by the Bekara in his survey [18]. His work proposed a series of security challenges, i.e., the identity spoofing of smart meters, data modification to gain unauthorized rights by damaging them physically or remotely, and malicious software injections in order to manipulate smart grids' software. However, there are other challenges that need to be addressed such as scalability, mobility and development of the networks at a large scale. Further challenges are the incorporation of the already deployed system and adaptation of the existing gateways and the accommodation of the constrained resources.

Another survey in the field of cyber security of the smart grids was presented by Wang et al. [19]. Their work briefs the effectiveness of network protocols and web standards such as World Wide Web (WWW), distributed network protocol (DNP3), International Electrotechnical Commission (IEC 61850), Internet protocol version 4 (IPv4) and Internet protocol version 6 (IPv6) and the challenges that are being faced in smart grid networking. Major components for the network security and integration, such as availability of network and its confidentiality, are also presented; preceding the methods of cyber-attacks. Among the cyber-attacks various layers of the attacks are explained targeting the layer layout of networks. Denial of service (DoS) attack is a method in which author explains the testing of the networks integrity by investigating the vulnerabilities in the smart grids at different layers, such as physical layer's channel jamming, to show how attackers can use it to connect to the networks and exploit it. Network and transport layer are one of the main component of network which follows the TCP/IP protocol model and can be affected by DoS attacks.

In [20], Marta presented the ways of handling big amount of data which is generated as a result of computations in intelligent grids. Marta conducted his research on a local smart grid to present realistic solutions. The work described the effective role of IoT in smart grid development for improving energy consumption of grid. The work also showed that by using IoT as an alternative for the reduction in energy consumption and increasing the output efficiency of smart grid technology can be improved as it involves insertion of sensors and smart networks. These smart networks include renewable energy sources (RES) and radio-frequency identification (RFID) for the monitoring of data flow and usage at consumer end. A multilayer schematic proposal was presented to incorporate the demand response and the management for the system at different levels such as industry, aggregator and household usage. An economic overview for the IoT in smart grids is presented by Cedric [21] for advanced technology in the market. The study showed how smart grid is promoting the use and integration of RES and advanced technologies for optimal usage of the new energy products. They also highlighted the trend of smart meters' implementation in the European states. Policies and consumer demand management presenting the investors' interest and the consumer response, towards the pricing variation and their impact on the market, are detailed by various percentage ratios of strategies and plans.

In [22], Momoh presented design and control of flexible power network systems and optimization and adaptability methods to achieve reliable and efficient power systems. Multiple techniques and methods such as adaptive dynamic programming (ADP), action network and critic network methods were provided. The work presents some of smart grid challenges including supply side and demand side management technologies. The author also discusses the cases for the development of the stochastic dynamic optimal power flow, which includes different applications such as as assessment of power system reliability, adaptive control and optimization of power systems. The concluding part explains some possible solutions and strategies and an ongoing research in the field.

Energy management and its optimization on producer, buffer and consumer level can play a vital role in having a global control over the reliability of sources and its supply. Molderink et al. [23] in their work propose an algorithm for controlling and storing of the electricity and heat demand by dividing the horizon into intervals. The algorithms set an optimal combination of sources to the cost functions by selecting the number of devices and comparing it to the transients of the devices. It uses integer linear problem (ILP) to find the best solution modelled for the heat demand. However, their research gap lies in explaining the implementation of smart application devices with the system. Also, all the resources were switched-on; considering full load on the system and assuming that there was no short fall or surplus storage capacity, which could lead to a false identification of the current consumption on consumer end. The overall work presents a good model in making a choice for selecting the cost effective and optimized solution for the controlling the electricity consumption and consequently providing a margin on pricing to the consumers.

2.2 Residential E-Meters

Electricity consumption is increasing day by day at residential sector of modern cities as reported in many of reports and researches [24–26, 66]. The increase in electricity demand has urged researchers and power engineers to work and plan for overcoming the needs. Therefore, many energy efficient programs have been launched. But, to effectively plan for these programs, a strong understanding of household equipment participating in electricity consumption is needed and there should be a reliable mechanism to record those readings. In such a scenario, special energy monitoring machines is a requirement. Therefore, smart meters have been introduced in market.

The trend of using mechanical or analog energy meters that uses a rotating metallic disk, nonmagnetic in nature, to measure power passing through it, is now being replaced by electronic energy meters that shows the reading on a screen or a LCD display [27–29]. With the introduction of these meters in the industry, domestic sector has brought a smart change since these meters are capable of recording the maximum usage at peak and off-peak hours. Meter voltage and current levels are processed digitally to determine different parameters such as power factor and reactive factor. One feature that makes this device very much scalable is the capability of measuring reading at every instant of time which makes it possible to have electricity usage data record at peak and off-peak timings, thus providing a benefit to the consumers to have defined pricing for the time of the day. Some of recent advancements in the field of smart energy metering, their shortcomings and research trends have been described in this section.

One of the major issues in smart e-meters is the ever existing problem of security [30]. Li et al. [31] articulated the homomorphic encryption methods to perform data aggregation on smart meters. A distributed aggregation method was presented to collect data at instantaneous points at multiple levels in order to allocate and balance the load along with resources. It also provides with the essential information in controlling and monitoring the power consumption. The homomorphic encryption used was Paillier cryptosystem [59], which uses additive homomorphic encryption functions. An aggregation tree based network topology ensures the transmission of data from destination to the nodes where destination is the in-network operations of smart meters and grids which passes through some keys which serve as the encryption for the data moving towards the destination node. This method ensures the privacy of electricity data usage along with the correct implementation of data aggregation.

Flavio et al. [32] discusses the security issues of smart e-meters with a special focus on secure communication and fraud detection. They propose a technique to obtain friendly and secret meter readings without interference in the privacy of users. The proposed idea is to measure the energy consumption of neighborhood level rather than at individual level, which would also help in identifying the behavior of consumer's energy use. Particularly it checks the time, in a day, when electricity usage is maximum, and further, it could also predict the type of devices used at a particular region. Paillier's additive encryption technique [59] has been incorporated with additive sharing methodology to perform the data measuring task at the same time to keep the privacy of the consumer. The scheme also takes care for the current leakage by reporting back reading after some instants, which can be compared to the pre-allocated factor assigned to an area by the supplier. One issue related to this scheme is the assumption that two out of N consumers are uncorrupted free consumers since the system is dealing with an order of hundreds of consumers at a time which could switch at any time. So, if the number of users fall below the above figure the privacy could be compromised. Since, the behavior of the consumer could be identified by subtracting the usage from the rest.

Another survey was presented by Le Blond et al. on a project in UK on 3eHouses in [33], regarding the smart metering implementation in domestic sector in order to demonstrate the decrease in the energy consumption by the use of information and communication technology. The paper discusses the ZigBee [34] technology, used for the meters, their developed system use IEEE 802.15.4 standard for connecting to the meters via an Ethernet link. One problem that was faced in this approach is the user's firewall protection, which prevents from sending interrupts in a public sector, however, it can be resolved by adding some additional rules to the firewall properties. Secure Shell (SSH) protocol is connected to R-tunnel which monitors the participant networks by setting up a TCP port on a ZigBee access point.

Travis et al. [35] presented Api-do, i.e., tools in their paper for exploring the wireless attack surface in smart meters to explain the methods and techniques along with a number of tools that are used for network exploitation, which could cause a security challenge for the smart meters. To start with, network identification is a first step leading towards the network hacking, different tools were used in order to identify the network; among which, OpenEar is a tool which monitors 16 channels simultaneously but at the same time assigns a unique number to each device. In this way, all connected devices become able to log data from SQL database. Another device which they present is zbWarDrive to capture the network traffic by injecting a beacon request to connected devices for monitoring purposes. For a more advanced analysis of network, ArcMap was used to interpolate the network range; even if a limited number of sample and strength points are available.

Energy metering policies is another factor that counts in when smart meters are discussed. Pupillo et al. [36], put forth the details in this area by highlighting energy metering policy approaches. Their work focuses on the details and results of a project called "E-cube project" funded by Italian Ministry and is a joint consortium of 12 major universities related to the energy fields. The main goal of the project was to create an equilibrium in rationalizing energy consumption by creating optimized and scalable infrastructure for smart meters. The project also aims to extend their domain at worldwide level and present an overview with various systems already working in leading world countries. Certain policies were assessed in order to tell the consumer response and the effect on the stakeholders to maintain a balance in the prices of metering, which in turn would make it feasible for the system implementation at a wider range. Policies regarding the system identification and consumer identity protection along with determining the personal behavior pattern, performing real time surveillance, providing accidental invasions and determining the use of specific devices are some key points to be considered by the policy makers.

Another system for smart metering is RF mesh system presented by Lichtensteiger et al. [37] for describing the smart metering systems' performance and architecture which works on frequency hopping spread spectrum (FHSS) and provides an advantage over direct sequence spread spectrum (DSSS) by having increased sensitivity and improved link budget. Figure 4 shows their typical representation of RF mesh network architecture.

The presented work also describes the simulation behavior of the performance of Landis+Gyr's GridstreamTM RF mesh based metering systems, showing the minimum time intervals of meter reading and the maximum amount of data transferred. Ad hoc networking communication is one key feature of RF mesh systems making it a valuable asset for dynamically linking with the neighboring nodes. One main thing that is considered in design is having established nodes in a neighborhood, when a node transmits data it waits to get acknowledgement and if fails to retrieve the information, it needs to resend the data or choose an alternative node to transmit data; which is a more efficient choice, practically. Hence, the down link could be altered without wasting time on resending data to a particular node again and again.

In the previous decade a lot of research has been done by companies and individual researchers to develop the suitable intelligent components that could take human living standards to a far next level. Sensors starting from wash basins to Bluetooth aware smart sofas and comfortable beds have turned out to be the most captivating innovations for everyone. The following section illustrates one of the most interesting components of smart cities, i.e., smart homes.

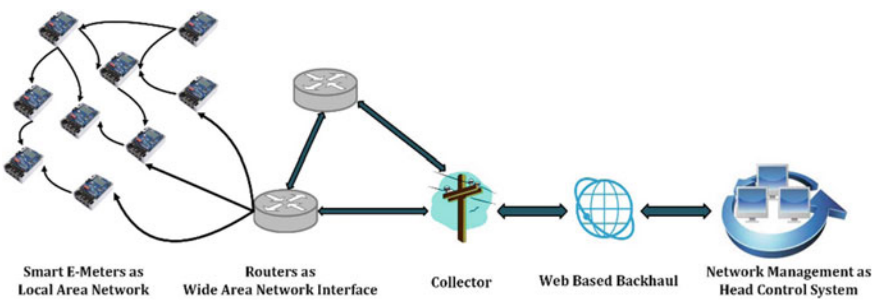

Fig. 4 RF mesh network representation

2.3 *Smart Homes*

Smart homes constitute an important branch of computing that includes bringing smartness into home appliances, medicinal services, wellbeing, and security [38]. Remote monitoring frameworks are regular segments of intelligent homes, which use telecommunication and web innovations to control home remotely and help the patients who are away from their caregivers. Home automation network provides a communication protocol for electronic devices that are connected to sensors and switches via a central hub or a gateway. Earlier concept of smart homes devices can be seen as automatic garage doors, coffee makers, timers and many other remote control devices [39–41]. But, technology advancements of present era have brought sensor networks integrated with many or almost all electronic devices being controlled through some application on a smartphone or through web. Which ultimately provides a seamless connection throughout a home system rather than devices working individually. In short, smart homes offer a superior personal satisfaction by presenting computerized apparatus control and assistive administrations [42].

A home needs three most important things to make it intelligent, i.e., (1) an internet network-either wired or wireless, (2) an intelligent gateway to manage sensors and system and (3) smart sensors or home automation in general with a link to devices inside home and external services. Figure 5 shows some of major concerned areas and focuses that motivates to contribute in smart homes. Three of the services are comfort, healthcare and security. One of the main objectives of smart homes, i.e., comfort can be achieved by mainly two things. First is human or gadgets activity identification and event automation and the second one is remote access and control of different areas of home. Second major objective i.e. healthcare can be obtained by intelligent indoor surveillance systems and local or remote monitoring. Finally, security services are always considered to be desired objectives and can be active by different identification methods.

Optimizing sensor technology is one of the key concern in research on smart homes. Byun et al. [44] propose an intelligent smart self-adjusting sensor for smart home services based on ZigBee communication using ZiSAS for the implementation of real-time situational based intelligent wireless sensor network (WSN).

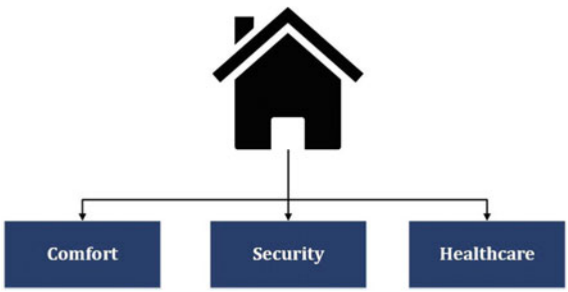

Fig. 5 Components/services of smart homes (adapted from [43])

However, some challenges considering the wireless sensor networks are the power consumption and battery lifetime along with some hardware limitations. Also the bandwidth of the network plays important role in defining the reliability and working. Some key features which ZigBee technology provides to the solution of above issue are as:

- Flexible architecture to reduce the hardware limitations.
- A situational event based control system behaviour to gather data and sense node density which was not the case in previous versions of WSN.
- A context awareness system to provide adaptable services by analysing the surroundings.
- Situational based self-adjustment so that the network can judge various parameters such as network topology, sensor density and sensitivity to the environment and can adapt to it.

ZigBee based ZiSAS architecture comprises of two parts one is self-adjusting sensor (SAS) which plays its role in sensing sensor rate, modifying topology and also gathering data and transmission according to the situation and the other is sensor management agent (SMA) which plays its role in sensor management, pattern learning and reasoning. The design of system is classified into three layers as management, network and interface. The bed test of the device shows that overall consumption of energy due to use of SAS and SMA is 3–12 and 8–34% depending on the number of devise used.

In [45], Darianian et al. presented an RFID based IoT system and services for smart homes. Their work introduces a system known as RF Energy Generator which limits the power consumption at room or appliances level. RFID master slave architecture allows the system to carry out reader services provided by the smart home, to initialize the wake up or a read process and then manipulate the ID information tags. Then, master performs the former task and latter one is done by the slave. However, many master readers can be interconnected in a system to collect item information and transmit them to further analyze and process. Another aspect of this system is mobile RFID (MRFID) reader which decreases the power consumption of multiple tag collision processes by using a master slave proxy network to answer the wake ups for the right tag by navigating to the location of desired appliance or a device. Authors [39] also gave examples to show how these devices could be connected to machines and devices to facilitate household services such as washing, cooking and even healthcare.

2.3.1 Human Activity Detection

The craving to enhance the personal satisfaction for handicapped and the fast growth of elderly individuals has provoked a tremendous effort from both scholarly world and industry to create smart home innovation [46]. For such individuals one of the most important development in smart home technology is the recognition of daily routine activities, i.e., sleeping, bathing, eating, drinking, exercising [47, 50, 51, 67] etc. It has been demonstrated that the ability to accurately distinguish the everyday exercises of people may have critical applications in healthcare [48]. For instance it might assist independent living of oldies at low medicinal services costs. Furthermore, detection of daily life activities may also contribute in indication of arising medical problems.

The development of system to detect the human activity and adapt itself accordingly to provide the most optimal services can be achieved by using adaptive neural networks (ANN). A challenging task is to track the human behavior since humans have a periodic variation in their daily life activities; and they also perform simultaneous tasks at the same time which is difficult to track. A very powerful method to tackle such problem is the data mining techniques for which different sensor networks are used to study the behavior through collected data. Zheng et al. [49] presented a growing self-organizing maps (GSOM) based on self-adaptive neural networks (SANN), which provides a brief study on data mining by using computational approach to monitor behavior of human activity within a closed environment of smart home. GSOM was proved to be dynamic since it can branch out various nodes after recognizing and visualizing patterns and thus has a self-evolving nature, which provides a good measure to handle large sets of data. The experiment conducted showed the detailed behavior of human activities at different time in various parts of home. One good feature of this system is having a record of activities and its ability to tell if there is any abnormal activity performed, that helps in maintaining and securing homes.

2.4 Surveillance Cameras

The growth of the IoTs in the development of smart cities has seen a massive advancement in wearable, non-computing devices, business to business (B2B) IoT technology and consequential momentum in the last few years. One subset of the IoT that has brought a significant growth is the internet-enabled surveillance cameras [40, 41]. A video camera used to monitor an area or building by transmitting recorded images to a central control room is known as surveillance camera. In this section we present some of the developments and researches in the advancements of these security cameras.

Perpetual video camera for IoT is proposed by Chen et al. [52]. In their tutorial, they highlighted the importance of perpetual video camera whose net energy consumption is approximately zero. They also presented the design challenges of such cameras, which include:

- High power consumption
- High data rate
- Heavy loading and maintenance cost of distributed cameras

They also provided the possible solutions of the above mentioned issues to design a camera with the properties of energy harvesting module, low power consumption, distributed video analysis engine and distributed video coding.

Chien et al. [53] introduce the concept of distributed computing and SoC design for smart cameras to reduce the transmission bandwidth requirement and to off-load the computation from the cloud servers. Figure 6 shows a simplified smart camera based distributed architectures in a smart city.

The end gadgets of this system are smart cameras. Advances in semiconductor technology has enabled to integrate more complex computations in intelligent cameras. Figure 7 shows that the cameras are associated locally to an aggregator or a passage. Next, they are further attached to a cloud networks. It is basically a demonstration of distributed resources (cameras) that are attached to each other in a city. By the help of different case studies, they observed that their proposed design can not only achieve greater coverage area but also power efficiency. They use the methodology to embed more computations into sensors and aggregators so that on every node computation can be distributed and we get rid of to employ centralized solutions on cloud servers.

Satyanarayanan et al. [54] analyze the technical issues that are implicated in creating an Internet-scale searchable repository for crowd sourced video content in edge analytics in a machine-to-machine/IoT network. The authors consider a hybrid cloud architecture to overcome the high cumulative data rate of incoming videos from different cameras and automated modification of video streams to sustain privacy. Methodology used was of sampling video frames, metadata-based filters with low computational complexity.

In [55], Liu et al. introduces the technology that represents video from different perspectives and describe the principle and coding structure of multi-view video. They pay a great attention on the application of intelligent security system and the

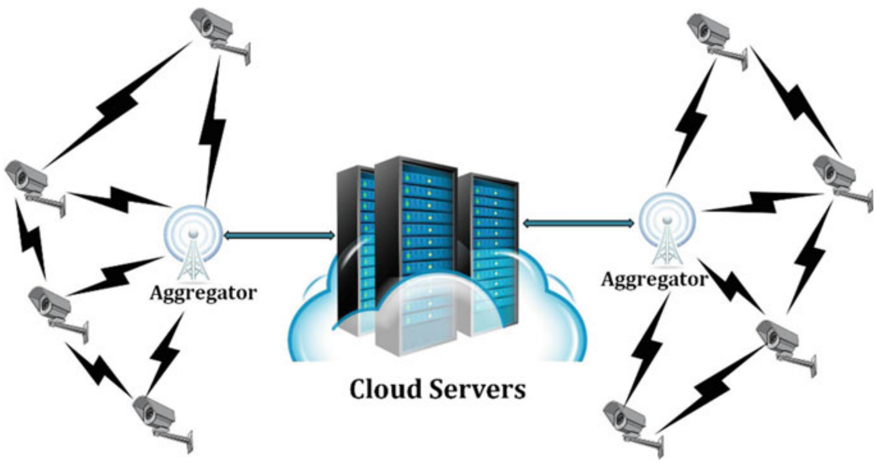

Fig. 6 Distributed smart cameras in a network

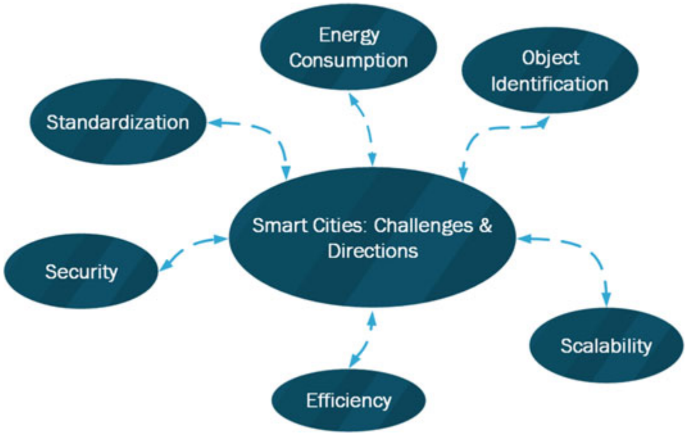

Fig. 7 Major challenges, opportunities and directions of IoTs in smart cities

challenges faces in this field. They observe the results by comparing data of single view video with multi-view video and proposed the concept of multi-view video coding. The research gap is large capacity data compression, information data extraction, and information data security management.

2.5 Traffic Controls

Traffic congestion has become one of the major problems in downtown areas. Due to rash traffic, horrible incident takes place and urban areas are facing several challenges because of alarming trend of growing populations. Therefore, smart traffic controls systems are considered to be a promising approach to avoid many road side accidents. IoT serves as the major component in making traffic control mechanism smart and intelligent.

Many solutions for improving traffic light systems have been introduced by researches and many of these techniques have been employed in the system. An IoT based solution for traffic light, where the traffic behavior changes dynamically is presented by Misbahuddin et al. [56]. This paper proposes that traffic flow can be dynamically controlled by on site traffic officers through their smart gadgets. They used an intelligently configured web server on hardware machine, i.e., Raspberry Pi (RPi), for the traffic signal controlling algorithm. In order to control the traffic lights in one of the patterns or to enforce any new pattern, the onsite traffic officer can access RPi's GPIO interface through a smart phone, utilizing the WebIoPi framework installed on RPi. In their work, one of the shortcoming is that the traffic situational information does not automatically pass to the RPi unit controlling the lights at an intersection. So, the authorities cannot take a quick decision. It is likely that prioritizing certain roads or certain directions for longer durations may cause traffic problems on other roads.

Nowadays, the navigation aids that do not work properly may cause fatal maritime accidents due to the rapidly increasing maritime traffic volume. Lighthouse and buoy tender method cannot check the real-time condition of maintenance aids. In [57], Cho et al. highlight the issues and complexity of maritime transportation and also suggests an efficient method to manage navigation aids based on IoT technologies in their work. The IoT-based navigation aids management system provides relevant data to comprehensive navigation aids management center and maritime traffic control center. Particularly, it sends a relevant data such as the identification service, the location identification and tracking service, as well as the operation status notification service to major relevant entities with the help of real-time information delivery service. By the use of IoT technology, time and expenses which can be correlated with extensive amount of maritime accidents are expected to be reduced. Moreover, the reliability and stability of the navigation aids will rise because no loss of information will occur through this method. In addition, on real-time basis a research on processing, analysis, and utilization of the various data collected using an IoT equipment will be carried out in the future.

The advancements in cloud computing and IoT have provided a promising opportunity to resolve the challenges caused by increasing the transportation issues. He et al. [58], supports the advances in IoT to resolve the transportation issues by using cloud computing and IoT technologies. Two innovative vehicular data cloud services describe a number of benefits such as car maintenance, to overcome road congestion, traffic management and enhancing road safety. As a consequence, remote security for disabling engine and remote diagnosis, have been developed to enhance driver's safety, convenience, and enjoyment. The proposed IoT-based layered architecture supports three new cloud services as follows:

- Vehicle provide their networking and data processing capabilities to other vehicles through the cloud.
- Some vehicles may need some specific application that require large amount of storage space.
- Thus vehicles that have unused storage space can share their storage space as a cloud-based service.

As a community, vehicular data clouds offer a variety of cooperative information, hazard location warning, lane change warning and parking availability. By using the two modified data mining models, the authors [49] demonstrate how data mining cloud service could be used to identify hidden potential issues to avoid accidents. But a research gap in their work is not to address the solution of complexity involved to enable the vehicular clouds. Due to this a number of challenges such as scalability, security, reliability, privacy, quality of service, and lack of global standards still exist.

In the field of IoT the metropolitan traffic management act as a vital role for highly integrated organizational processes. Foschini et al. [59] present and discuss the design and implementation of an M2M application in the field of road traffic management that assimilate, for the sake of efficiency. Their work demonstrates both the technical and organizational processes viewpoints which is already available service in IoT technology. In restricted city areas based on standard infrastructure and software components, the design of an integrated IoT retractable bollard management is present. Precisely, to simplify system maintenance and management a standard solution of integrating IoT-based services is presented.

Chen et al. [60] introduced a cyber-transportation systems for convalescent of road safety and efficiency. They also proposed the machine to machine (M2M) system consolidating intelligent road with unmanned automobile. In this article, the authors propose a solution which is applicable on an unmanned vehicle in the form of cyber physical system (CPS). They mentioned the cellular and capillary M2 M challenges, which comprise of the complexity, power, data rates, delays, security and peer-to-peer traffic. For the future work, the speed of the unmanned vehicle is correlated with performance of the system. By increasing speed many factors affect its response. To counter this, a new technique for the safety of system should be established.

3 Smart Cities: Challenges and Opportunities

Communication and connectivity is a major concern in any professional, commercial or industrial field [2]. Modern trends in smart cities have brought a revolution in communication worldwide; further contributing to change and improve living perspectives of entire human race. In the greater part of the presented areas in this chapter, we have highlighted some of the most important researches that have contributed to develop intelligent urban communities (smart cities). In this section, we discuss and summarize the most challenging areas of smart cities, the research opportunities and the future directions that would further take the concept of smart cities to a far next level. Figure 7 highlights the recent research opportunities, major challenges and directions in various applications of IoTs in smart cities.

3.1 Standardization Limitation

Internet of things is entirely related to internet, web protocols, and host identity protocols (HIP); but, due such large number of consumers, a lot of limitations occur while using Internet protocol version 4 (IPv4) [61]. One of such limitations involves the problem of identification and naming management to the users, as each consumer has to be assigned a unique identity [62] co-existence of the networks creates a problem for the identification of mobile and radio broadcasting, and other service spectrums at various nodes by use of techniques as dynamic spectrum access (DSA). Standards for bilateral communication techniques are being considered to interpolate the semantic web cross platforms such as XML, ASN.1 and many other web services. Research in the past decade has been conducted in this area on a very large scale and a lot of improvement is brought forward to replace IPv4 with IPv6. The essential capacity of IPv6 is to take into account more unique TCP/IP address identifiers, as we have come up short on the 4.3 billion addresses made with IPv4. Therefore, IPv6 is such a critical advancement for the Internet of things (IoT). Web associated items are turning out to be progressively prominent, keeping in mind IPv4 addresses couldn't take care of the demand for IoT items, IPv6 gives IoT items a stage to work on for quite a while. While IPv6 is a phenomenal and important overhaul from IPv4, it is still not an end to all research problems for the IoT. One major issue that organizations face is deciding how to get IPv4 and IPv6 gadgets to impart and dialogue appropriately and meaningfully.

3.2 Object Identification

Another limitation in this sector is object/human identification and detection [63]. Numerous electronic devices are embedded by RFID tags and contain huge amount of data, to be sensed and identified by other devices. And, the information is processed to detect whether it is about location, orientation, motion, temperature or any chemical change. IoT devices identify the objects and determines the objects on the basis of their identification capabilities, since all the objects would be containing the identification tags so it is a demanding challenge for the network to differentiate among such a huge number of objects.

3.3 Security and Ethics Challenges

With billions of new intelligent items being developed every day, security is an essential thought in the back of all IoT architects' minds [19, 64]. The earlier security networks were designed to only incorporate the privacy of humans; but, with the emerging concept of IoT, the security of the devices is also considered to be an important issue. As this technology is capable of human to things (H2T) communication and hence is not a suitable measure for this system in most of the cases [65], a proper encryption is needed to make sure that who can access the data and to prevent external sources to monitor or interfere.

3.4 Transmission Reliance and Efficiency

Wireless sensor networks (WSNs) and communication flows have become an integral part of IoT based communication in intelligent devices. Therefore, another considered research problem is the transmission of data within a specified spectrum. As data is to be transferred via many mediums like wireless networks, GPS, and Bluetooth etc., the communication should be efficient enough to transmit data without any loss of information. Efficiency of data transmission with a particular hardware is a crucial criterion for a wireless system and hence system efficiency and better/reliable communication flows is also under development.

3.5 Energy Consumption

The billions, and eventually trillions, of sensors and electronic devices are interacting with each other in modern IoT based cities. The efficiency, i.e., the consumption of resources among which the energy being the most important, is to be taken into account while designing an IoT based architecture of the system [57, 58]. The consumption of energy determines which type of technology is being used and how much it is contributing towards green environment.

3.6 Scalability and Existing Networks

As per a report put out by Gartner, 25 billion "smart devices" will be associated with the web by the year 2020. That is a really staggering estimation, considering the same report noticed that 4.9 billion intelligent gadgets will be associated in 2015. It can be estimated that about 400% expansion in development in just five years reveals some insight into the amount of exponential IoT development; we can hope to find in the following 10, 20, or even 50 years. Due to an already existence of a large number of smart products, another focused research domain is the incorporation of these devices and their scalability at such a large network. An efficient middleware is to be incorporated to effectively manage these devices at a common place; also a proficient semantic user interface is required to easily differentiate between the existing and new devices.

4 Conclusion

The current research is investigating the concept of smart city and related factors, which have enormous impact in our daily life, with an emphasis on improving its framework's ability to provide customized IoT functionalities. In this survey, we have presented some of the most advanced and trending researches in the fields of smart IoT based products that are ultimately shaping smart cities. The chapter covered five distinct areas in development of a smart city. We started with highlighting the improvements in smart grids' architecture and its research motivation;

followed by a very similar product of modern world, i.e., intelligent e-meters. We have discussed about how researchers are focusing to find out the solutions related to security threats in these smart e-meters. At that point, we examined the most intriguing advancements in smart homes and also illustrated research gaps in them. Moreover, we presented some critical features of surveillance cameras and traffic control systems. Finally, we discussed overall challenges, research directions and opportunities in developing smart cities.

References

1. Aazam, M., Khan, I., Alsaffar, A. A., & Huh, E.-N. (2014). Cloud of things: Integrating Internet of things and cloud computing and the issues involved. In *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th–18th January*, 2014 (pp. 414–419). IEEE.
2. Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42,* 1190–1203.
3. Aldrich, F. K. (2003). Smart homes: Past, present and future. In *Inside the smart home* (pp. 17–39). Berlin: Springer.
4. Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine, 3,* 34–41.
5. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54,* 2787–2805.
6. Augusto, J. C., & Nugent, C. D. (2006). Smart homes can be smarter. In *Designing smart homes* (pp. 1–15). Berlin: Springer.
7. Bekara, C. (2014). Security issues and challenges for the IoT-based smart grid. *Procedia Computer Science, 34,* 532–537.
8. Benzi, F., Anglani, N., Bassi, E., & Frosini, L. (2011). Electricity smart meters interfacing the households. *IEEE Transactions on Industrial Electronics, 58,* 4487–4494.
9. Berbers, Y., De Decker, B., Moons, H., & Verbaeten, P. (1987). The design of the HERMIX distributed system. In *Proceedings of the 34th ISMM International Symposium Mini and Microcomputers*.
10. Byun, J., Jeon, B., Noh, J., Kim, Y., & Park, S. (2012). An intelligent self-adjusting sensor for smart home services based on ZigBee communications. *IEEE Transactions on Consumer Electronics, 58,* 794–802.
11. Chan, M., Campo, E., Estève, D., & Fourniols, J.-Y. (2009). Smart homes—Current features and future perspectives. *Maturitas, 64,* 90–97.
12. Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91,* 55–81.
13. Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things Journal, 1,* 349–359.
14. Chen, Y.-K., & Chien, S.-Y. (2012). Perpetual video camera for Internet-of-things. In *Visual communications and image processing (VCIP), 2012 IEEE* (pp. 1–7). IEEE.
15. Genge, B., Haller, P., Gligor, A., & Beres, A. (2014, May). An approach for cyber security experimentation supporting sensei/iot for smart grid. In *2nd International Symposium on Digital Forensics and Security*.

16. Chien, S.-Y., Chan, W.-K., Tseng, Y.-H., Lee, C.-H., Somayazulu, V. S., & Chen, Y.-K. (2015). Distributed computing in IoT: System-on-a-chip for smart cameras as an example. In *The 20th Asia and South Pacific Design Automation Conference* (pp. 130–135). IEEE.
17. Cho, M., Choi, H. R., & Kwak, C. (2015). A study on the navigation aids management based on IoT. *International Journal of Control and Automation, 8,* 193–204.
18. Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., et al. (2012). Understanding smart cities: An integrative framework. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2289–2297). IEEE.
19. Cities, S. (2013). Trace analysis and mining for smart cities: Issues, methods, and applications. *IEEE Communications Magazine, 51,* 121.
20. Clastres, C. (2011). Smart grids: Another step towards competition, energy security and climate change objectives. *Energy Policy, 39,* 5399–5408.
21. Darianian, M., & Michael, M. P. (2008). Smart home mobile RFID-based Internet-of-things systems and services. In *2008 International Conference on Advanced Computer Theory and Engineering* (pp. 116–120). IEEE.
22. Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid—The new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials, 14,* 944–980.
23. Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine, 8,* 18–28.
24. Fischer, C. (2008). Feedback on household electricity consumption: A tool for saving energy? *Energy Efficiency, 1,* 79–104.
25. Foschini, L., Taleb, T., Corradi, A., & Bottazzi, D. (2011). M2M-based metropolitan platform for IMS-enabled road traffic management in IoT. *IEEE Communications Magazine, 49,* 50–57.
26. Garcia, F. D., & Jacobs, B. (2010). Privacy-friendly energy-metering via homomorphic encryption. In *International Workshop on Security and Trust Management* (pp. 226–238). Berlin: Springer.
27. Genge, B., Haller, P., Gligor, A., & Beres, A. (2014). An approach for cyber security experimentation supporting sensei/IoT for smart grid. In *2nd International Symposium on Digital Forensics and Security*.
28. Genge, B., Siaterlis, C., & Hohenadel, M. (2012). Amici: An assessment platform for multi-domain security experimentation on critical infrastructures. In *International Workshop on Critical Information Infrastructures Security* (pp. 228–239). Berlin: Springer.
29. Goodspeed, T., Bratus, S., Melgares, R., Speers, R., & Smith, S. W. (2012). Api-do: Tools for exploring the wireless attack surface in smart meters. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2133–2140). IEEE.
30. Guesgen, H. W., & Marsland, S. (2016). Using contextual information for recognising human behaviour. *International Journal of Ambient Computing and Intelligence (IJACI), 7,* 27–44.
31. Hall, P. (1988). *Cities of tomorrow*. Oxford: Blackwell Publishers.
32. Harrison, C., & Donnelly, I. A. (2011). A theory of smart cities. In *Proceedings of the 55th Annual Meeting of the ISSS-2011, Hull, UK*.
33. He, W., Yan, G., & Da Xu, L. (2014). Developing vehicular data cloud services in the IoT environment. *IEEE Transactions on Industrial Informatics, 10,* 1587–1595.
34. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security challenges in the IP-based Internet of things. *Wireless Personal Communications, 61,* 527–542.
35. Internet of things and big data technologies for next|Chintan Bhatt| Springer, n.d.
36. Jabłońska, M. R. (2014). Internet of things in smart grid deployment. *Rynek Energii, 2,* 111.
37. Kimbahune, V. V., Deshpande, A. V., & Mahalle, P. N. (2017). Lightweight key management for adaptive addressing in next generation Internet. *International Journal of Ambient Computing and Intelligence (IJACI), 8,* 50–69. doi:10.4018/IJACI.2017010103
38. Kinney, P., et al. (2003). Zigbee technology: Wireless control that simply works. In *Communications Design Conference* (pp. 1–7).
39. Kinzer, S. (2004). Chicago moving to "smart" surveillance cameras. *New York Times,* A18.
40. Kopetz, H. (2011). Internet of things. In *Real-Time Systems* (pp. 307–323). Berlin: Springer.

41. Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). Smart objects as building blocks for the internet of things. *IEEE Internet Computing, 14,* 44–51.
42. Le Blond, S. P., Holt, A., & White, P. (2012). 3eHouses: A smart metering pilot in UK living labs. In *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)* (pp. 1–6). IEEE.
43. Li, F., Luo, B., & Liu, P. (2010). Secure information aggregation for smart grids using homomorphic encryption. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* (pp. 327–332). IEEE.
44. Lichtensteiger, B., Bjelajac, B., Müller, C., & Wietfeld, C. (2010). RF mesh systems for smart metering: System architecture and performance. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* (pp. 379–384). IEEE.
45. Liu, Z., & Yan, T. (2013). Study on multi-view video based on IOT and its application in intelligent security system. In *Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on* (pp. 1437–1440). IEEE.
46. Misbahuddin, S., Zubairi, J. A., Saggaf, A., Basuni, J., Sulaiman, A., Al-Sofi, A., et al. (2015). IoT based dynamic road traffic management for smart cities. In *2015 12th International Conference on High-Capacity Optical Networks and Enabling/Emerging Technologies (HONET)* (pp. 1–5). IEEE.
47. Molderink, A., Bakker, V., Bosman, M. G., Hurink, J. L., & Smit, G. J. (2009). Domestic energy management methodology for optimizing efficiency in smart grids. In *PowerTech, 2009 IEEE Bucharest* (pp. 1–7). IEEE.
48. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). Private memoirs of a smart meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (pp. 61–66). ACM.
49. Momoh, J. A. (2009). Smart grid design for efficient and flexible power networks operation and control. In *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES* (pp. 1–8). IEEE.
50. Najjar, M., Courtemanche, F., Hamam, H., Dion, A., & Bauchet, J. (2009). Intelligent recognition of activities of daily living for assisting memory and/or cognitively impaired elders in smart homes. *International Journal of Ambient Computing and Intelligence (IJACI), 1,* 46–62. doi:10.4018/jaci.2009062204
51. Odella, F. (2016). Technology studies and the sociological debate on monitoring of social interactions. *International Journal of Ambient Computing and Intelligence (IJACI), 7,* 1–26. doi:10.4018/IJACI.2016010101
52. Poland, M. P., Nugent, C. D., Wang, H., & Chen, L. (2011). Smart home research: Projects and issues. In *Ubiquitous Developments in Ambient Computing and Intelligence: Human-Centered Applications* (pp. 259–272). IGI Global.
53. Pupillo, L., D'Amelia, B., Garino, P., & Turolla, M. (2010). Energy smart metering and policy approaches: The E-cube project.
54. Satyanarayanan, M., Simoens, P., Xiao, Y., Pillai, P., Chen, Z., Ha, K., et al. (2015). Edge analytics in the internet of things. *IEEE Pervasive Computing, 14,* 24–31.
55. Shapiro, J. M. (2006). Smart cities: Quality of life, productivity, and the growth effects of human capital. *The Review of Economics and Statistics, 88,* 324–335.
56. Sigg, S., Shi, S., & Ji, Y. (2014). Teach your WiFi-device: Recognise simultaneous activities and gestures from time-domain RF-features. *International Journal of Ambient Computing and Intelligence (IJACI), 6,* 20–34.
57. Solanki, V. K., Katiyar, S., BhashkarSemwal, V., Dewan, P., Venkatasen, M., & Dey, N. (2016). Advanced automated module for smart and secure city. *Procedia Computer Science, 78,* 367–374.
58. Tamane, S., Solanki, V. K., & Dey, N. (2001). *Privacy and security policies in big data*. IGI Global.
59. van Rysewyk, S. (2014). Robot pain.

60. Vlacheas, P., Giaffreda, R., Stavroulaki, V., Kelaidonis, D., Foteinos, V., Poulios, G., et al. (2013). Enabling smart cities through a cognitive management framework for the internet of things. *IEEE Communications Magazine, 51,* 102–111.
61. Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks, 57,* 1344–1371.
62. Weiss, M., Mattern, F., Graml, T., Staake, T., & Fleisch, E. (2009). Handy feedback: Connecting smart meters with mobile phones. In *Proceedings of the 8th International Conference on Mobile and Ubiquitous Multimedia* (p. 15). ACM.
63. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of things—A survey of topics and trends. *Information Systems Frontiers, 17,* 261–274.
64. Wolde-Rufael, Y. (2006). Electricity consumption and economic growth: A time series experience for 17 African countries. *Energy Policy, 34,* 1106–1114.
65. Wolf, W., Ozer, B., & Lv, T. (2002). Smart cameras as embedded systems. *Computer, 35,* 48–53.
66. Yoo, S.-H. (2005). Electricity consumption and economic growth: Evidence from Korea. *Energy Policy, 33,* 1627–1632.
67. Zheng, H., Wang, H., & Black, N. (2008). Human activity detection in smart home environment with self-adaptive neural networks. In *Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on* (pp. 1505–1510). IEEE.