A systematic survey of Internet of Things frameworks for smart city applications

José Joaquín Peralta Abadía[1], Christian Walther[2], Ammar Osman[2], and Kay Smarsly[1]

[1]*Institute of Digital and Autonomous Construction*
Hamburg University of Technology
Blohmstraße 15, 21079 Hamburg, Germany

[2]*Chair of Computing in Civil Engineering*
Bauhaus University Weimar
Coudraystr. 13 b, 99423 Weimar, Germany

Abstract

Recent developments in smart sensing technologies have fostered the wide-spread utilization of smart city applications, which rely on Internet of Things (IoT) frameworks to work efficiently. The terms "smart city" and "IoT framework", however, have been given several definitions, without consensus. Consequently, definitions of the terms "smart city" and "IoT framework" need to be condensed, consolidating concepts and guidelines of smart cities and IoT frameworks, as will be shown in this study. In addition, a systematic survey of IoT frameworks for smart city applications is presented, summarizing and comparing the technologies and architectures of IoT frameworks for smart city applications. As a result of this study, trends in IoT frameworks for smart city applications and a definition of the term "smart city" are provided. Materializing the findings achieved in this study, an abstract IoT framework concept for smart city applications is proposed. It is expected that the definition of the term "smart city" may be used as a basis for a generally accepted formal definition and that the proposed IoT framework concept may provide a strong foundation for successful IoT framework implementations in the context of smart city applications.

Keywords: Smart cities; Internet of Things (IoT); Wireless sensor networks; IoT frameworks; IoT applications

List of acronyms

2G/3G	Second/third generation of wireless mobile telecommunications
6LoWPAN	IPv6 over low-power wireless personal area networks
AMQP	Advanced message queuing protocol
BLE	Bluetooth low energy
BS/BSI	British Standards Institution
CoAP	Constrained application protocol
DDS	Data distribution service
DNS	Domain name system
DNS-SD	DNS-based service discovery
ETSI	European Telecommunications Standards Institute
HTTP	Hypertext transfer protocol
IPv4/IPv6	Internet protocol v4/v6
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LTE	Long-term evolution wireless mobile telecommunications
mDNS	Multicast DNS
MQTT	Message queuing telemetry transport
MQTT-SN	MQTT for sensor networks
NFC	Near-field communication
REST	Representational state transfer
RFID	Radio-frequency identification
UNE	Spanish Association for Standardization
XMPP	Extensible messaging and presence protocol

1 Introduction

Smart city applications have spread around the world, due to the advancements of information and communication technologies (ICT) and the increase of population in urban areas. Ever since 1993, when the city-state of Singapore was described as an intelligent city by Heng and Low [1], smart cities have been discussed, without a formal definition. Several terms have been used thereafter, such as “intelligent city”, “information city”, “digital city”, and “ubiquitous

city". The term "intelligent city" represents an advanced form of a city based on innovation, collective intelligence, and artificial intelligence. The terms "information city" and "digital city" are mainly based on ICT as the main tool to deliver services. Furthermore, ICT is also extended into the concept of "ubiquitous cities", derived from the ubiquity of data availability for users [2]. However, the different terms share the same concepts and are related to each other [3]. Generally, smart cities aim to use innovative technologies to enhance urban services, improving life quality for the citizens in a user-friendly way [4]. The definitions of the term "smart city" converge on ICT as a key enabler. In this regard, one key ICT element of smart cities are networked infrastructures [3]. An example of networked infrastructure commonly used in smart city applications is the Internet of Things (IoT), which may be referred to as a world-wide network of interconnected devices (things) which may be addressed uniquely, based on standard communication protocols [5].

For over a decade, IoT has been present in research and industry, being part of Industry 4.0. Representing a trend towards automation and sensing using cyber-physical systems, Industry 4.0 facilitates self-organization of services, individualization of products, adaptation to human needs, and corporate social responsibility [6]. IoT integrates billions of devices that may be coupled through the Internet, interconnecting smart cities and the citizens [7]. Several surveys have covered IoT topics and technologies, such as platforms [8, 9], security [10], architectures [11], and communication and network protocols [11]. IoT technologies include middleware, network protocols, application protocols, gateways (or edge technology), and sensor nodes. IoT frameworks consolidate the use of the IoT technologies, defining the architecture of IoT systems and the relationships between the IoT technologies and satisfying user needs. However, the heterogeneity of technologies hinders straight-forward implementations of IoT frameworks in smart cities.

Despite the considerable research efforts undertaken in the fields of smart cities and IoT in the last decade, the definitions of “smart city” and “IoT framework” are diverse and have no consensus. In addition, the variety of IoT frameworks for smart city applications cause difficulties in selecting the most appropriate IoT framework for a specific smart city application, thus generating either under-performing results or over-head and additional costs. Therefore, both problems may hinder the success of implementations of IoT frameworks for smart city applications.

Several literature surveys have been carried out regarding IoT frameworks and smart cities. Working definitions of the term “smart city”, as well as smart city applications, the characteristics of smart cities, and the application domains of smart cities, such as smart mobility and smart governance, have been surveyed [4, 12–15]. Other efforts have focused on smart energy management and energy harvesting in smart cities, proposing new paradigms and examples of smart power grid management and HVAC system management [16]. Existing IoT technologies used in smart cities, with emphasis specifically put on technical aspects of smart cities, such as middleware, hardware and network protocols, have been surveyed and compared [12, 13, 17]. In addition, some of the surveys have presented challenges and opportunities for smart cities. Main challenges are security and privacy of the citizens, heterogeneity of IoT devices and IoT middleware, and scalability and reliability of the IoT [12].

Although some surveys present different technical aspects of IoT frameworks, a gap is identified. Surveys present technologies, current and possible applications, and cities with IoT framework implementations in specific application domains. Nevertheless, survey have not fully dwelled in the technologies and architectures used by IoT frameworks for smart city applications, which is the main goal of the survey conducted in this study. The remainder of this study is structured as follows. Section 2 introduces concepts and guidelines of smart cities

and IoT frameworks. Section 3 presents the survey methodology pursued during the survey process and the survey of IoT frameworks for smart city applications, summarizing and comparing the elements of the sensing, middleware, and application layers. Section 4, upon discussing the results of the survey of IoT frameworks, presents a definition of the term "smart city" and introduces a novel IoT framework concept for smart city applications to overcome the current limitations identified in this study. Finally, Section 6 provides conclusions drawn from the results achieved in this study.

2 Concepts and guidelines

To conduct the survey on IoT frameworks for smart city applications, smart city concepts and IoT framework concepts are analyzed. First, working definitions are presented according to peer-reviewed literature. Thereupon, a basis for new definitions is set through the concepts of each term. Finally, examples of guidelines for smart cities and IoT frameworks are presented.

2.1 Smart city concepts

For the sake of clarity, this subsection, illuminating smart city concepts, is subdivided into smart city definitions and smart city domains.

Smart city definitions

The term "smart city" first appeared in 1993 as an element of global cities and was defined as an intelligent city that portrays a technopolis and hard infrastructure [1]. Thereafter, the term

"intelligent city" gained popularity and definitions of the term "intelligent city" began to appear. For example, Komninos [18] has defined intelligent cities as territories with high capacity for learning and innovation, built upon the creativity of their population, institutions of knowledge creation, and digital infrastructure for communication and knowledge management. After the appearance of the term "intelligent city", several other terms, all sharing key elements, have been coined, such as "digital city", "knowledge city", and "smart city". The key elements of a smart city, according to Hollands [3], are

(i) Networked infrastructures, including transport, business services, housing, and ICT,

(ii) Business-led urban development,

(iii) E-governance, and

(iv) Social and environmental sustainability.

Similarly, the key elements that make up a smart city, according to Nam and Pardo [19], are technology, humans, and institutions. The technology element involves using ubiquitous and pervasive concepts and the active engagement and collaboration of the public and private sector, schools, and citizens. The human element describes an environment where life-long learning, social equality, creativity, open-mindedness, and public participation of the citizens is possible and encouraged. Finally, the institutions element interconnects the government with citizens, communities, and businesses, thus generating growth, innovation, and progress. In this regard, Nam and Pardo [19] have mentioned that the institutions element should be transparent and engage citizens in decision making and participation.

More recently, the term "smart city" has been defined by Caragliu *et al.* [20] as a city that invests in human and social capital and traditional and modern networked infrastructure,

fueling a sustainable economy and a high quality of life, managing natural resources wisely, through the political participation of citizens. Furthermore, Zygiaris [21] has interpreted the term “smart city” as an intellectual ability that addresses innovative socio-technical and socio-economic aspects of growth. Both aspects lead to four concepts:

- “Green” as in urban infrastructure for environment protection and reduction of CO_2 emission
- “Interconnected” as in revolution of broadband economy
- “Intelligent” as in the capacity to process and produce added value from sensor-based city data
- “Innovative” as in the ability to innovate based on knowledgeable and creative human capital

Another definition of smart city, proposed by Nam and Pardo [19], compares a city to a living organism, in which infrastructure is equivalent to the skeleton and the skin, telecommunication networks to the nerves, sensors and tags to the sensory organs, ubiquitous embedded intelligence to the brain, and software to the knowledge and cognitive competence.

On the one hand, most definitions have focused on using information and communication technologies to empower and optimize infrastructure, energy consumption, environment and waste management, and mobility. On the other hand, some definitions have focused on the humane aspect of the city, where education, social inclusion, governance, creativity, and the citizens are the primary factors. Based on the previous statements, it becomes clear that a consensus on the definition of the term “smart city” is necessary.

Smart city domains

Several attempts have been undertaken to define the domains that constitute smart cities. Giffinger *et al.* [22] have described a smart city as a city that performs well in six domains, smart economy, smart people, smart governance, smart mobility, smart environment and smart living, building upon endowments and active participation of citizens. Building upon the six domains proposed by Giffinger *et al.* [22], Neirotti *et al.* [23] have added smart buildings to the list, highlighting how all of the domains need to work together as a city is a single organic whole. Chourabi *et al.* [24] have established eight domains of a smart city: Management and organization, technology, governance, policy context, people and communities, economy, built infrastructure, and natural environment. Since several authors have proposed different sets of domains, Albino *et al.* [25] have surveyed and described several proposals of domains of a smart city, including the aforementioned lists of domains. The authors have mentioned that the most common elements that emerge from the proposed domains are (i) networked infrastructures enabling political efficiency and social development, (ii) promotion of urban development and growth via economy and culture, (iii) social inclusion, and (iv) the wellbeing of the natural environment.

Smart city domains may be categorized as soft domains and hard domains [23]. Soft domains refer to the intangible characteristics of smart cities, such as smart citizens and smart living. Hard domains refer to the tangible characteristics, such as smart environment and smart mobility. Soft domains, being intangible, are more difficult to measure than hard domains. Thus, a city may be more motivated to invest in hard domains, because the results are easier to measure. Consequently, an explanatory analysis provided by Neirotti *et al.* [23] has identified a negative correlation between smart cities investing in the soft domains and smart cities investing in the hard domains. The explanatory analysis has found that a smaller percentage of

cities invest in the soft domains, compared to the higher percentage of cities that invest in the hard domains. Nevertheless, the decision to develop a domain of a smart city will depend on the necessities and country-specific factors of a city.

On closer observation, an aspect of critique regarding smart cities has been identified. Many cities have been self-proclaimed as smart cities for promotional purposes, prioritizing informational business interests while hiding a growing social polarization [3]. Therefore, a fundamental challenge for smart cities, according to Law and Lynch [4], is to lead to fair outcomes for all citizens. Human individuals and living beings in general, as well as the urban context, should be prioritized when designing smart cities. Technologies, such as IoT frameworks, must facilitate the ease of life and convenience of communities, imitating the natural growth of the specific urban space. To this end, the following subsection presents IoT framework concepts, subdivided into definitions and architectures.

2.2 IoT framework concepts

The Internet of Things is a paradigm that has gained considerable attention in the last two decades. IoT devices (i.e., “things”), interconnected in a world-wide network, are uniquely addressable based on standard application protocols, such as WiFi, Bluetooth, or mobile networks [5]. IoT leverages on the availability of heterogeneous “things” and solutions to connect the “things”, providing a shared global-scale information base, supporting the design of applications that involves, at virtual level, both people and representations of the things [26]. IoT elements, such as IoT devices and IoT middleware, require a framework to orchestrate the interactions. Therefore, IoT frameworks function as agents between IoT elements and serve as application interfaces to enable interaction between the IoT elements [27]. Uviase and Kotonya

[28] have described IoT frameworks as being capable of supporting up to billions of devices, facilitating ease of testing and development, providing a user-friendly environment to develop and test new functionalities, and offering a lightweight implementation easily installable and updatable. The remainder of this subsection is subdivided into IoT framework definitions and IoT framework architectures.

IoT frameworks definitions

The term "IoT framework", due to the lack of a proper definition, has been used interchangeably with the terms "IoT platform" and "IoT middleware". For example, as stated before, Cheruvu *et al.* [27] have defined an IoT framework as the communication intermediary between one or more IoT elements. Ammar *et al.* [10] have defined an IoT framework as a structure that coordinates and controls processes conducted by various IoT elements. Guth *et al.* [29] have described an IoT middleware as the IoT element responsible for receiving data from devices, processing the data, providing the data to applications, and sending commands to be executed by actuators. Regarding the term "IoT platform", Ray [8] has defined IoT platforms as enablers of advanced services by interconnecting physical and virtual IoT elements based on interoperable information and communication technologies. The intermediation between the different IoT elements surfaces as the general idea in the aforementioned definitions. Therefore, a foundation should be laid for defining "IoT framework" and disambiguate the terms "IoT framework", "IoT middleware", and "IoT platform".

Regarding information and communication technologies, platforms refer to environments (hardware and software) in which software applications are hosted and executed. Middleware refers to software applications that provide services to other software applications. Finally, frameworks refer to software environments that provide application-specific software that

enables a specific functionality. Therefore, the terminology may be adapted to the IoT framework concept. Consequently, IoT platforms host the IoT middleware, and IoT frameworks provide the environment that enables the communication between IoT middleware and other IoT elements, such as applications, sensors, and actuators.

IoT framework architectures

Because of the large number of heterogeneous devices the Internet of Things integrates, flexible layered IoT framework architectures are necessary to connect the physical and digital world [11]. Figure 1 shows two examples of IoT framework architectures. Figure 1a presents a three-layered IoT framework architecture approved by the [30]. The three-layered IoT framework architecture is comprised of application layer, networking and data communications layer, and sensing layer. Figure 1b depicts the IoT framework architecture proposed by Guth *et al.* [29], which is closely related to the three-layered architecture proposed by the IEEE shown in Figure 1a. The IoT integration middleware layer of Guth *et al.* comprises the networking and data communications layer of the IEEE Internet Initiative, as well additional services, such as alerts, ontologies, and resource management. The sensing layer of the IEEE Internet Initiative is equivalent to the gateway, device, and sensor and actuator layers of Guth *et al.*. Merging both architectures into a single IoT framework architecture, a more general three-layered architecture may be achieved, composed of sensing layer, middleware layer, and application layer, described as follows.

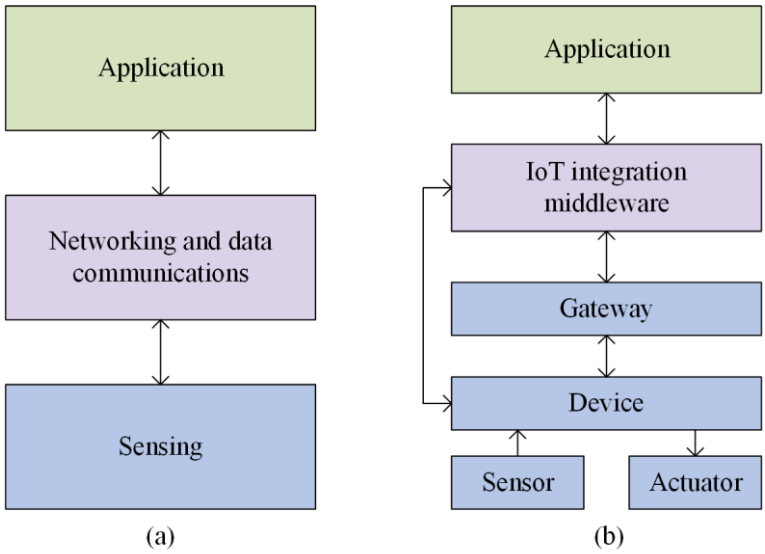

Figure 1. Three-tiered IoT framework architecture proposed by the IEEE Internet Initiative [30] (a) and IoT framework architecture proposed by Guth *et al.* [29] (b).

- **Sensing layer**: The sensing layer, also referred to as perception layer or object layer, integrates the physical devices, i.e., hardware (such as sensors, actuators, sensor nodes and gateways) of the IoT framework. Sensors act as measurement tools of the physical environment and convert the measurements into electrical signals. Actuators control physical objects, based on commands received from sensor nodes. Sensor nodes are usually resource-constrained, optimized for low energy consumption, have sensors and actuators connected, either by wires or by wireless connection, and may perform local processing. In addition, sensor nodes form sensor networks, communicating with other sensor nodes and with gateways. Sensor networks are scalable and highly dynamic, thus requiring availability, reliability, and quality of service. Gateways (or edge technology) collect the data from sensor nodes and may perform data aggregation and data processing algorithms. Finally, gateways and sensor nodes communicate with the middleware layer, via network protocols, such as WiFi, 2G/3G, and Long-Term Evolution (LTE). For the communication between the sensing layer and the middleware layer, security aspects should be considered to avoid threats, such as data-privacy violations and hardware hacking.

- **Middleware layer**: The middleware layer comprises the software that connects the sensing and application layer [9], intermediating the communication between the sensing and application layer. In addition, the middleware layer processes and stores the data received from the sensing layer. Thus, security borders are required to protect the middleware layer against unauthorized access from either the application or the sensing layer, encrypting data and limiting access to authorized users and devices. Razzaque *et al.* [31] list the following functional requirements of the middleware layer:

    - Resource discovery: Registration of IoT devices
    - Resource management: Management of the status of the IoT devices
    - Data management: Storing and processing of data received from the sensing layer
    - Event management: Generation of alerts and scheduling of tasks
    - Code-upgrade management: Remote upgrading of firmware of IoT devices

    As with the sensing layer, the middleware layer requires scalability, availability, and reliability. Scalability is the capability of accommodating growth of IoT devices and applications/services involved in the IoT framework. Availability in the middleware layer involves the ability to support different IoT devices and protocols, enabling interoperability in the sensing layer. Reliability refers to remaining operational during the life cycle of the IoT framework, even during failures and errors.

- **Application layer**: The application layer serves diverse-domain applications that may require delivery of data, either in real time or in a delayed manner. The applications allow users visualizing and analyzing data and, via the middleware layer, sending commands

to the sensing layer [28]. Additionally, the application layer aims to utilize the components of the sensing and the middleware layer to control the specific physical environment [29]. Therefore, the application layer must provide security and protection against unauthorized users or devices, as well as protection from data-privacy leakage.

Because several communication and network protocols are available for IoT, Al-Fuqaha *et al.* [11] have listed the most prominent IoT protocols used in the three-layered IoT framework architecture, as shown in Table 1. It should be noted that the protocols shown in Table 1 have been updated according to recent developments.

Table 1. Most prominent IoT protocols, as listed by Al-Fuqaha *et al.* [11].

Protocol type	Protocol
Application	DDS, CoAP, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST
Service discovery	mDNS, DNS-SD
Middleware layer network protocol	IPv4/IPv6
Sensing layer network protocol	2G/3G/LTE, 6LoWPAN, BLE, DASH7, IEEE 802.15.4, LoRA, RFID, Sigfox, Wize, Z-Wave, Zigbee

2.3 Guidelines related to smart cities and IoT frameworks

Due to the variability of smart city applications, guidelines suggest ways to implement smart city applications and the best practices to follow. Therefore, this subsection presents the main results of an analysis of guidelines for both smart cities and IoT frameworks by means of two illustrative examples, namely guidelines presented by the European Innovation Partnership on Smart Cities and Communities (EIP-SCC) and the Smart Cities Council Australia New Zealand

(SCCANZ). Both guidelines are exemplarily illuminated due to the completeness of the implementation process and the standard recommendation, respectively.

2.3.1 European Innovation Partnership on Smart Cities and Communities (EIP-SCC)

EIP-SCC [32] have published a guideline, the *Smart city guidance package: A roadmap for integrated planning and implementation of smart city projects*, which proposes steps required to implement smart cities. The guideline is built upon the experiences and expertise of cities, businesses, citizens, research institutes, and non-governmental organizations that work together in the EIP-SCC. The guideline proposes seven steps listed below, each step including a checklist, a "how-to" for every item of the checklist, stakeholders, and examples of methodologies and successful implementations.

1. **Envision**: Long-term vision and objectives are developed or adjusted. In addition, possibilities for collaboration within the city are explored.
2. **Decide and commit**: The long-term vision is materialized as a strategy. The parties decide and commit on how to start preparing the plan for the smart city implementation.
3. **Plan**: Based on the strategy of the previous step, a plan with concrete actions, targets, milestones, and key performance indicators (KPI) is elaborated.
4. **Do**: The actual implementation of the plan is performed. Adjustments, alterations, and amendments are expected.
5. **Check**: The progress is monitored, based on the KPI established in the plan step. If problems surface, solutions are explored.
6. **Act**: Solutions to the problems in the previous step are implemented.

7. **Replicate and scale up**: Experience is shared and communicated, facilitating replication and upscaling of successful solutions.

2.3.2 Smart Cities Council Australia New Zealand (SCCANZ)

The Smart Cities Council Australia New Zealand [33] has developed a guideline, the *Best practice guide – Smart cities standards*, detailing the smart city standards available globally. The guideline categorizes the standards into smart cities, sustainable communities, IoT, and building information modeling (BIM). Furthermore, the standards are grouped into three levels, (i) strategic level, (ii) process level, and (iii) technical level. Strategic-level standards are of relevance to the city leaders, whereas process-level and technical-level standards are of relevance to people in management positions. Table 2 presents examples of cities and countries that, according to the guideline, have adopted standards in the smart city implementation process. Table 3 shows a matrix of the standards reported by the guideline, grouped vertically by category and horizontally by standard level.

Table 2. Standards adopted by cities and countries, as reported by the Smart Cities Council Australia New Zealand [33]

City/Country	Standards implemented in the city/country
India	BSI PAS 181, Smart City Framework
Melbourne	ISO 37120
Johannesburg	ISO 37120
London	BSI PAS 180, BSI PAS 181, BSI PAS 182, BSI PAS 183, BSI PAS 184, BSI PD 8100, BSI PD 8101, BS 8904, BS 11000, BS BIP 2228
Dubai	ITU Focus Group on Smart Sustainable Cities
South Korea	ISO/TC 268

Singapore	3 Types of IoT standards, ISO, ITU defined standards

Table 3. Standards matrix by category and standard level, as reported by the Smart Cities Council Australia New Zealand [33]

Category	Strategic standards	Process standards	Technical standards
Smart cities	BSI PAS 180:2014 BSI PD 8100:2015 BSI PD 8101:2014 ISO 37101:2016 ISO 37120:2014 ISO/IEC 30182:2017 ISO/TR 37150 ISO/TR 37152	BSI PAS 181:2014 BSI PAS 182:2014 BSI PAS 183:2017 BSI PAS 184:2017 ETSI GS OEU 019 V1.1.1 ETSI TR 103 290 V1.1.1	UNE 178303 ETSI TS 104 001 V2.1.1
Sustainable communities	BSI 8904:2011 ISO/TR 37121:2017 ISO 37102:2016	ISO 14001 ISO 20121 ISO 50001	ISO 16745-1:2017 ISO 16745-2:2017 IEEE Standard 1547.3 IPWEA Model LED Public Lighting Specification
IoT		ISO 27001	BSI PAS 212:2016 IEEE Standard 1686 ISO 8000-8:2015 ISO/TS 8000-1:2011 ISO/TS 8000-150:2011
Building information modeling (BIM)		ISO 16739	BSI 1192:2007+A2:2016 BSI 1192-4:2014 BSI 8536-1:2015 BSI 8536-2:2016 BSI PAS 1192-2:2013 BSI PAS 1192-3:2014 BSI PAS 1192-5:2015 ISO 15686 ISO 16739:2013 ISO 29481-1:2016

			ISO/TS 12911:2012

Having presented concepts of smart cities and IoT frameworks as a basis for the survey of IoT frameworks for smart city applications, the following section will present the survey results.

3 Results of the survey of IoT frameworks for smart city applications

This section surveys IoT frameworks for smart city applications. First, the methodology pursued during the survey process is presented. Second, the domains are described on which research, so far, has put primary emphasis. Finally, the survey of IoT frameworks for smart city applications, summarizing and comparing the IoT elements of the sensing, middleware, and application layers is detailed.

3.1 Methodology

The survey methodology consists of three steps, (i) data collection, (ii) data organization, and (iii) data analysis. The data collection involves searching for studies indexed in the Web of Science Core Collection as well as conference papers indexed in the Scopus database. In an initial search, 41 indexed studies were found, which involved IoT frameworks in smart city applications, using the search string: (“smart cities” OR “smart infrastructure” OR “smart living” OR “smart environment” OR “smart mobility” OR “smart economy” OR “smart citizens” OR “smart governance”) AND (“Internet of Things” OR “IoT” OR “IoT framework” OR “IoT platform”). Next, a forward and backward search has been carried out on each of the results of the initial search, entailing 17 additional studies for a total of 58 studies. Finally, 12 studies published before 2016 were omitted, to avoid surveying obsolete trends and

technologies. Then, in the data organization step, the IoT elements described in the studies have been tabulated, according to the concepts presented in Section 2. For the sensing layer, focus on the physical IoT devices used in the IoT frameworks is given. For the middleware layer, focus on the IoT services provided by the IoT frameworks is given. Finally, an analysis of the organized data has been carried out, as presented in the following subsections.

3.2 Smart city domain applicability

Smart cities are constituted by seven domains, as will be presented in Subsection 4.2. Although several studies report IoT frameworks that are created for being applied to all smart city domains [34], most IoT frameworks for smart city applications are usually situated in one of the seven domains. Some studies cannot easily be categorized, as the IoT frameworks may involve aspects of more than one domain. For example, some studies focus on monitoring elderly citizens, where elderly citizens are trained to use and interact with the IoT devices required for data collection (smart citizens) and the IoT framework provides health benefits to the users (smart living) [35]. Other examples include monitoring traffic congestion (smart mobility) and environmental pollution (smart environment) [36].

Table 4 presents the categorization of IoT frameworks into the smart city domains, with a visual representation shown in Figure 2. Hard domains are presented in green and soft domains are presented in purple. It can be observed that 44 studies apply to the hard domains of a smart city (i.e., smart mobility, smart environment, and smart infrastructure) because, as described earlier, hard domains are the most invested on. The soft domains only account for ten of the studies (i.e., smart economy, smart governance, smart citizens, and smart living), and nine studies present IoT frameworks that may be applied to all domains of a smart city.

Table 4. Categorization of IoT frameworks into the smart city domains.

IoT framework	Applies to all domains	Smart economy	Smart governance	Smart citizens	Smart living	Smart mobility	Smart infrastructure	Smart environment
Datta *et al.* [37]	X							
Kamilaris *et al.* [38]		X						
Latre *et al.* [36]	X					X		X
Pasini *et al.* [39]							X	
Mainetti *et al.* [40]					X			
Pacheco *et al.* [41]							X	
Khan *et al.* [42]					X			
Brincat *et al.* [43]						X		
Han *et al.* [44]								X
Jokinen *et al.* [45]	X							
Basso *et al.* [46]							X	
Rinaldi *et al.* [47]							X	
Sembroiz *et al.* [48]							X	X
Anjana *et al.* [49]							X	
Dong *et al.* [50]							X	
Rathore *et al.* [51]	X							
Gheisari *et al.* [52]	X							
Verdouw *et al.* [53]		X						
Tao *et al.* [54]							X	
Yassine *et al.* [55]							X	
Han *et al.* [56]							X	
Chen *et al.* [57]								X
Badii *et al.* [58]	X							
Mulero *et al.* [35]				X	X			
Filippi *et al.* [59]			X	X				
Rahman *et al.* [60]		x						
Sotres *et al.* [61]						X		X
Wang *et al.* [62]							X	

Tripathy *et al.* [63]					X			
Tripathy *et al.* [64]					X	X		X
Santos *et al.* [65]						X		X
Mrozek *et al.* [66]				X	X			
Verma *et al.* [67]					X			
Calderoni *et al.* [34]	X							
Maatoug *et al.* [68]							X	
Jayaraman *et al.* [69]		X						
Bustamante *et al.* [70]	X							
Campos *et al.* [71]								X
Badii *et al.* [72]						X		
Chang *et al.* [73]					X			X
Roduit *et al.* [74]							X	
Lohokare *et al.* [75]							X	
Gautam *et al.* [76]							X	X
Mocnej *et al.* [77]	X							
Slaný *et al.* [78]							X	X
Luckner *et al.* [79]			X	X		X		

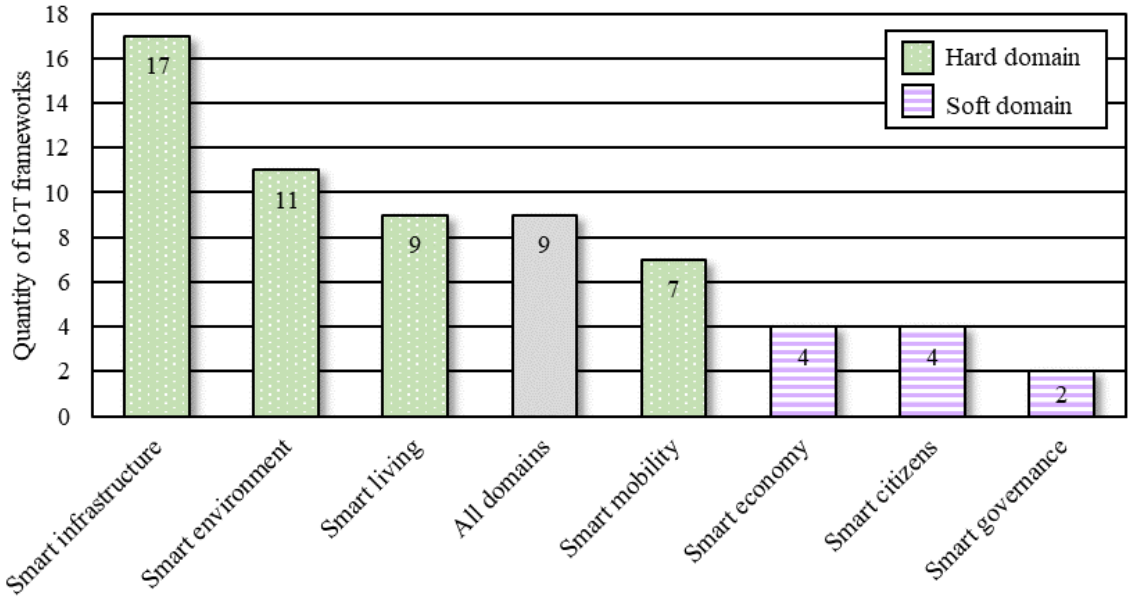

Figure 2. Categorization of IoT frameworks into the smart city domains.

3.3 IoT elements of the IoT frameworks

As shown in Figure 1, the structure of an IoT framework generally consists of three layers, each layer providing services and functions within the framework. The following subsections present a quantitative summary and comparison of the IoT elements of the sensing, middleware, and application layer. Based on the summary and comparison, Section 4 then presents a qualitative analysis in the form of results and discussion.

3.3.1 Sensing layer

The sensing layer provides functionality for using sensors and actuators. IoT devices collect and process data through sensors. Subsequently, the IoT devices, via network and messaging protocols, transmit the data in specific data structures to the middleware layer. Moreover, elements of the real world may be controlled by actuators connected to the IoT devices. To this end, control signals are transmitted from the middleware layer to the corresponding IoT devices of the sensing layer.

The sensing layer of an IoT framework may be defined to work with any or with specific IoT devices. Table 5 presents the IoT devices that may be used in the sensing layer of the IoT frameworks surveyed in this study, with a visual representation shown in Figure 3. It is important to point out that IoT frameworks may use more than one IoT device type in the sensing layer. Thus, the sum of all IoT devices used in the IoT frameworks is greater than the total number of IoT frameworks surveyed in this study. It can be observed that 17 IoT frameworks have defined the sensing layer to be able to work with any IoT device, providing interoperability to the whole framework. Arduino- and Raspberry Pi-based IoT devices are the favored vendor-specific IoT device types, as both have been used in eight IoT frameworks each. However, Raspberry Pi-based IoT devices have been used mostly as gateways between other

IoT devices and the middleware layer. Smartphones have been used in six IoT frameworks, mainly due to the sensors incorporated in modern smartphones. Finally, 13 studies have reported other types of IoT devices, and five studies did not specify IoT devices used in the sensing layer.

Table 5. IoT device types used in the sensing layer of IoT frameworks.

IoT framework	Arduino-based	Raspberry Pi-based	Any IoT device	Smartphone	Other	N/A
Datta *et al.* [37]			X			
Kamilaris *et al.* [38]			X			
Latre *et al.* [36]			X			
Mainetti *et al.* [40]	X	X		X		
Pacheco *et al.* [41]	X	X				
Khan *et al.* [42]		X				
Brincat *et al.* [43]					X	
Han *et al.* [44]						X
Jokinen *et al.* [45]						X
Basso *et al.* [46]					X	
Rinaldi *et al.* [47]						X
Anjana *et al.* [49]			X			
Dong *et al.* [50]	X					
Rathore *et al.* [51]			X			
Gheisari *et al.* [52]			X			
Verdouw *et al.* [53]						X
Tao *et al.* [54]			X			
Yassine *et al.* [55]			X			
Han *et al.* [56]			X			
Chen *et al.* [57]					X	
Badii *et al.* [58]			X			
Mulero *et al.* [35]				X		
Filippi *et al.* [59]	X					

Rahman *et al.* [60]				X	X	
Sotres *et al.* [61]						
Wang *et al.* [62]					X	
Tripathy *et al.* [63]						X
Tripathy *et al.* [64]					X	
Santos *et al.* [65]		X		X	X	
Mrozek *et al.* [66]				X		
Verma *et al.* [67]				X	X	
Calderoni *et al.* [34]	X				X	
Maatoug *et al.* [68]			X			
Jayaraman *et al.* [69]	X		X			
Bustamante *et al.* [70]			X			
Campos *et al.* [71]		X				
Badii *et al.* [72]	X	X	X			
Chang *et al.* [73]	X					
Roduit *et al.* [74]					X	
Lohokare *et al.* [75]			X			
Gautam *et al.* [76]		X			X	
Mocnej *et al.* [77]			X			
Slaný *et al.* [78]		X			X	
Luckner *et al.* [79]			X			

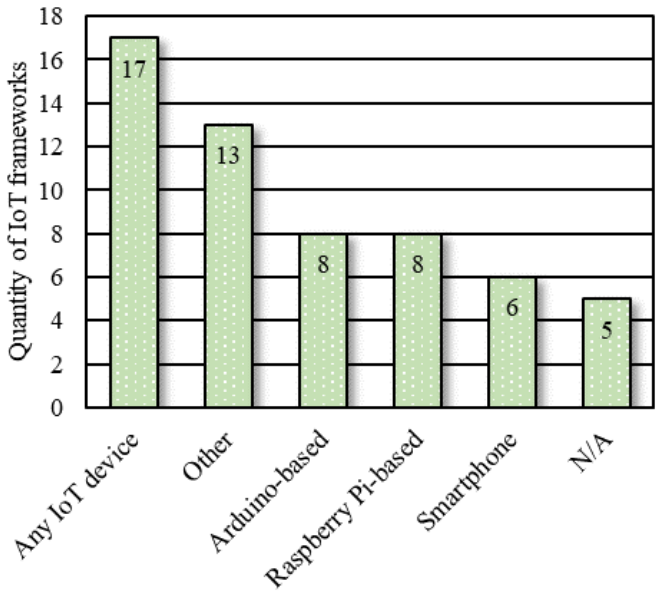

Figure 3. IoT device types used in the sensing layer of IoT frameworks.

IoT devices make use of predefined network protocols, based on the design and hardware of the IoT device, that may affect the interoperability of an IoT framework. Therefore, an IoT framework should be designed to work with the majority of network protocols. Table 6 presents the network protocols used in the sensing layer of the IoT frameworks, with a visual representation shown in Figure 4. As with the IoT devices, IoT frameworks may use more than one network protocol, thus the sum of all network protocols compatible with the IoT frameworks is greater than the total number of studies surveyed herein. In the studies, the trending network protocols are WiFi, 3G/4G/5G, 6LoWPAN/LoRA, Zigbee, and Bluetooth, being used in 13, 12, 11, 11, and ten IoT frameworks respectively.

Table 6. Network protocols used in the sensing layer of the IoT frameworks.

IoT framework	Zigbee	6LoWPAN/LoRA	Bluetooth	RFID	NFC	WiFi	3G/4G/5G	Other
Latre *et al.* [36]		X	X					X
Pasini *et al.* [39]								X
Mainetti *et al.* [40]			X		X	X	X	
Pacheco *et al.* [41]						X		
Brincat *et al.* [43]		X						
Han *et al.* [44]							X	
Jokinen *et al.* [45]	X	X						
Basso *et al.* [46]	X							
Sembroiz *et al.* [48]	X	X	X					
Anjana *et al.* [49]	X					X		
Dong *et al.* [50]		X						
Rathore *et al.* [51]	X					X	X	
Gheisari *et al.* [52]								
Verdouw *et al.* [53]				X		X	X	X
Tao *et al.* [54]	X		X	X		X	X	
Yassine *et al.* [55]	X	X	X			X		

Han *et al.* [56]	X	X	X			X		
Mulero *et al.* [35]			X				X	
Filippi *et al.* [59]							X	
Rahman *et al.* [60]	X		X			X	X	
Sotres *et al.* [61]					X			
Tripathy *et al.* [64]		X					X	
Santos *et al.* [65]						X	X	X
Mrozek *et al.* [66]						X		
Verma *et al.* [67]			X				X	
Calderoni *et al.* [34]					X			
Maatoug *et al.* [68]	X	X		X	X			
Roduit *et al.* [74]	X							
Lohokare *et al.* [75]						X		
Gautam *et al.* [76]		X						
Luckner *et al.* [79]		X						

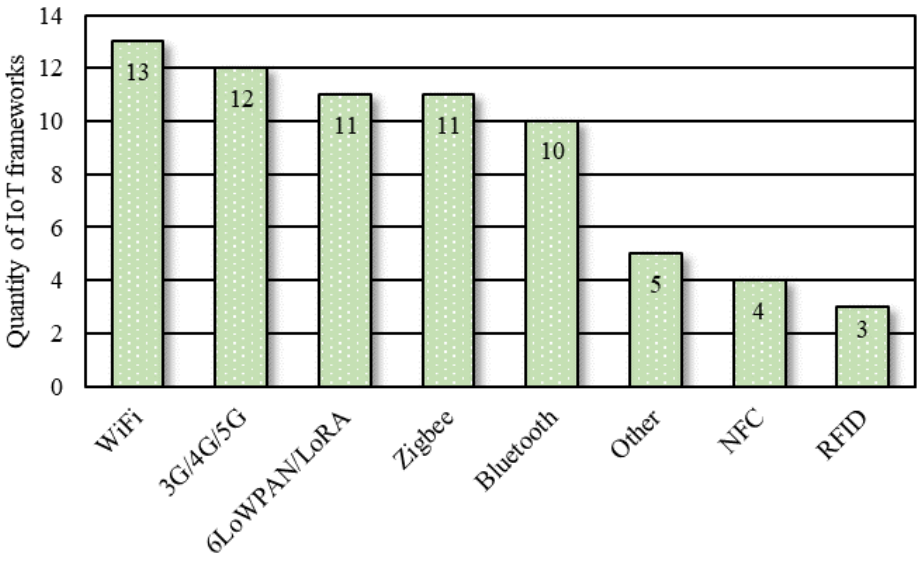

Figure 4. Network protocols used in the sensing layer of the IoT frameworks.

IoT devices may have resource constraints and limited power-supply availability. Nevertheless, low-power consumption seems to lack focus, as only eight studies have addressed this topic: Software and hardware optimizations have been proposed, such as extended sleep mode [53], hardware component disablement [71], and software optimizations [61]. In addition, other

studies have proposed the use of batteries with an additional solar-power energy supply to recharge the batteries [80, 81].

3.3.2 Middleware layer

The middleware layer is used to provide the data recorded by the sensors of the sensing layer to the application layer or to forward control signals from the application layer to the actuators connected to IoT devices in the sensing layer. Therefore, the middleware layer establishes a connection between IoT devices of the sensing layer and users or third-party systems of the application layer. The middleware layer is also responsible for consistent data storage in IoT frameworks. Within the middleware layer, basic services, accessible by the sensing and the application layer, are provided. Table 7 presents the services that are provided by the middleware layer in the IoT frameworks surveyed in this study, with a visual representation shown in Figure 5; the description follows in the subsequent paragraphs. Furthermore, Table 8 presents the technical challenges that were overcome by the middleware layer in the IoT frameworks surveyed in this study, with a visual representation shown in Figure 6.

Table 7. Services provided by the middleware layer of the IoT frameworks.

IoT framework	Resource discovery	Resource management	Database management	Event / alert management	Upgrade management	Machine learning	Encryption	Authentication
Datta *et al.* [37]	X	X	X					
Kamilaris *et al.* [38]	X	X	X	X				X
Latre *et al.* [36]	X	X	X		X			X

Mainetti *et al.* [40]				X				X
Pacheco *et al.* [41]								X
Brincat *et al.* [43]				X		X	X	X
Han *et al.* [44]			X			X		X
Jokinen *et al.* [45]	X	X	X	X			X	X
Basso *et al.* [46]	X	X	X	X			X	X
Rinaldi *et al.* [47]	X	X	X					
Sembroiz *et al.* [48]				X				
Anjana *et al.* [49]	X	X	X	X	X			
Dong *et al.* [50]	X	X	X	X			X	X
Rathore *et al.* [51]	X	X	X			X		X
Verdouw *et al.* [53]			X					X
Tao *et al.* [54]	X	X	X	X				X
Yassine *et al.* [55]			X	X		X		X
Han *et al.* [56]			X	X		X		X
Chen *et al.* [57]	X		X	X				X
Badii *et al.* [58]	X	X	X				X	X
Mulero *et al.* [35]	X	X	X				X	X
Filippi *et al.* [59]			X	X				X
Rahman *et al.* [60]				X		X	X	X
Sotres *et al.* [61]	X	X	X	X	X			X
Tripathy *et al.* [63]		X	X	X				
Tripathy *et al.* [64]								X
Santos *et al.* [65]			X			X	X	X
Mrozek *et al.* [66]			X	X		X		
Verma *et al.* [67]	X	X	X	X		X	X	X
Calderoni *et al.* [34]		X	X	X				X
Maatoug *et al.* [68]	X	X	X	X				X
Jayaraman *et al.* [69]	X	X	X	X				X
Bustamante *et al.* [70]	X	X	X	X				X
Campos *et al.* [71]	X	X	X	X		X		X
Badii *et al.* [72]	X	X	X	X		X	X	X
Chang *et al.* [73]			X	X		X		X
Roduit *et al.* [74]	X	X	X	X			X	X
Lohokare *et al.* [75]		X	X	X				X
Gautam *et al.* [76]			X			X	X	X
Mocnej *et al.* [77]	X	X	X	X		X		
Luckner *et al.* [79]			X			X		X

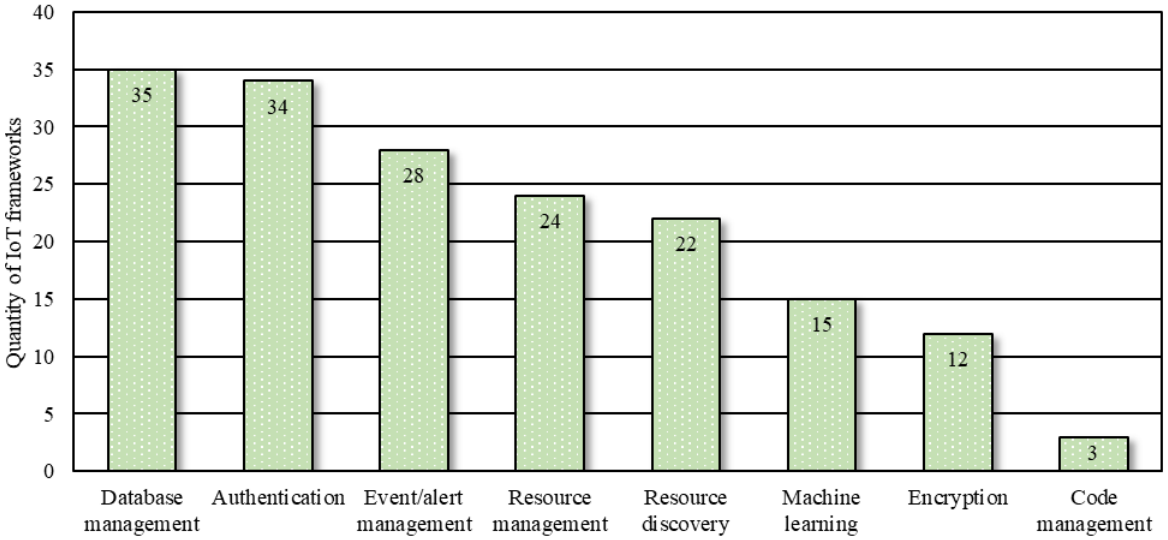

Figure 5. Services provided by the middleware layer of the IoT frameworks.

Table 8. Technical challenges that were overcome by the middleware layer of the IoT frameworks.

IoT framework	Scalable	Interoperability / Heterogene
Kamilaris *et al.* [38]		X
Latre *et al.* [36]	X	X
Mainetti *et al.* [40]		X
Khan *et al.* [42]	X	
Han *et al.* [44]	X	
Jokinen *et al.* [45]		X
Basso *et al.* [46]	X	
Sembroiz *et al.* [48]	X	
Anjana *et al.* [49]	X	X
Rathore *et al.* [51]		X
Tao *et al.* [54]	X	X
Yassine *et al.* [55]	X	X
Han *et al.* [56]	X	X
Mulero *et al.* [35]	X	X
Rahman *et al.* [60]		X
Sotres *et al.* [61]	X	X
Mrozek *et al.* [66]	X	X
Jayaraman *et al.* [69]	X	X
Bustamante *et al.* [70]		X

Badii *et al.* [72]	X	X
Roduit *et al.* [74]	X	
Lohokare *et al.* [75]	X	X
Gautam *et al.* [76]	X	X
Mocnej *et al.* [77]	X	X
Luckner *et al.* [79]	X	X

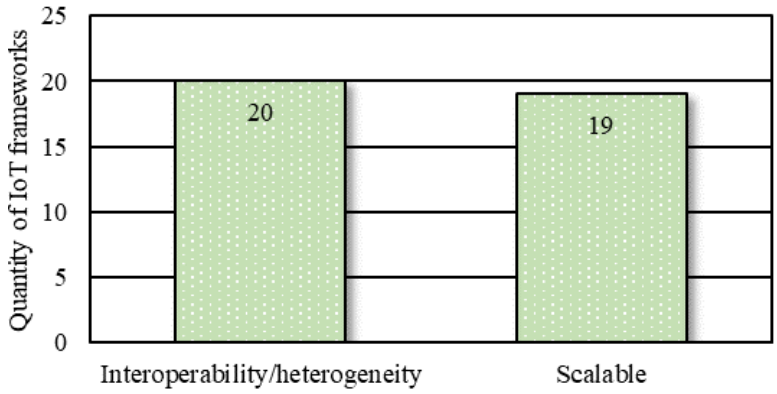

Figure 6. Technical challenges that were overcome by the middleware layer of the IoT frameworks.

Persistent and available data storage is a basic service in most IoT frameworks for smart city applications. As such, the service that has been provided the most by the middleware layer is database management, being provided in 35 IoT frameworks. Access to data provided through the database management system of IoT frameworks must be limited due to security and privacy reasons. To this end, in 34 IoT frameworks surveyed in this study, an authentication service has been provided to limit the access to data and administrative services of the middleware layer. An example of administrative services provided in the middleware layer is event and alert management, which should only be programmed by authorized users and has been offered in 28 IoT frameworks. Another aspect of data security is encryption. Encrypted data transfer is a security measure that the middleware layer should provide. Fulfilling the encryption security requirement, 12 IoT frameworks have mentioned including encryption functions for data transfer and storage. Furthermore, smart city applications may require using heterogeneous IoT devices. Therefore, the middleware layer of IoT frameworks may provide

resource management and resource discovery, to manage and register IoT devices being used. Resource management and resource discovery have been made available in 24 and 22 IoT frameworks, respectively. Finally, in connection with the current state of the art, it is expected that some IoT frameworks have been designed to use machine learning algorithms. From the IoT frameworks surveyed in this study, 15 IoT frameworks incorporate services to enable machine learning. Finally, the service that has been provided the least is upgrade management; only three IoT framework have an integrated code manager.

IoT devices may be varied and may use varied technologies. As such, 20 IoT frameworks surveyed in this study have targeted the technical challenge of interoperability (heterogeneity), by providing services such as ontologies [54]. As mentioned previously, smart city applications may require using heterogeneous IoT devices and the amount of IoT devices can be in the order of hundreds or thousands [81]. Thus, IoT frameworks for smart city applications should be scalable to manage the growing amount of (heterogeneous) IoT devices being connected. In the IoT frameworks surveyed in this study, 19 IoT frameworks have provided scalable solutions.

Since the middleware layer of IoT frameworks is in charge of mediating the communication between the sensing layer and application layer, messaging protocols have to be adopted to specify the ways the two layers communicate with the middleware layer. Table 9 shows the messaging protocols that have been adopted in the IoT frameworks surveyed in this study, with a visual representation shown in Figure 7. Overall, the middleware layer can be designed based on two approaches. On the one hand, the middleware layer of the IoT frameworks exposes only specific messaging protocols for specific IoT devices, for security and interoperability reasons. On the other hand, the middleware layer of the IoT frameworks may expose any messaging protocol, allowing to integrate devices of the sensing and application layer from different manufacturers into the IoT frameworks. In this study, 21 IoT frameworks have adopted the

HTTP REST messaging protocol, in accordance to trends in the ICT industry. Furthermore, 17 IoT frameworks have adopted the MQTT messaging protocol, which is useful in smart city applications, in which hundreds or thousands of IoT devices are connected, and broadcasting of messages is necessary. The other IoT frameworks in this study have used the protocols CoAP, AMQP, Websockets, and others, as presented in Table 9.

Table 9. Messaging protocols adopted by the middleware layer of the IoT frameworks.

IoT framework	HTTP REST	MQTT	CoAP	AMQP	Websockets	Other
Datta *et al.* [37]						X
Latre *et al.* [36]	X		X			
Pasini *et al.* [39]	X					
Mainetti *et al.* [40]						X
Khan *et al.* [42]		X				
Brincat *et al.* [43]	X	X				
Jokinen *et al.* [45]	X					
Basso *et al.* [46]		X		X		
Rinaldi *et al.* [47]	X	X		X		
Sembroiz *et al.* [48]	X	X				
Dong *et al.* [50]	X	X				
Verdouw *et al.* [53]	X					X
Yassine *et al.* [55]		X	X	X	X	
Han *et al.* [56]		X	X	X	X	
Chen *et al.* [57]		X				
Badii *et al.* [58]	X	X	X	X	X	
Mulero *et al.* [35]	X					
Rahman *et al.* [60]	X					
Sotres *et al.* [61]	X					
Santos *et al.* [65]	X					X
Mrozek *et al.* [66]	X				X	
Calderoni *et al.* [34]	X				X	
Jayaraman *et al.* [69]						X
Bustamante *et al.* [70]	X	X	X		X	

Campos *et al.* [71]	X	X	X			
Badii *et al.* [72]	X	X				X
Roduit *et al.* [74]		X		X		
Lohokare *et al.* [75]	X	X	X			
Mocnej *et al.* [77]	X	X		X		
Slaný *et al.* [78]		X				
Luckner *et al.* [79]	X					

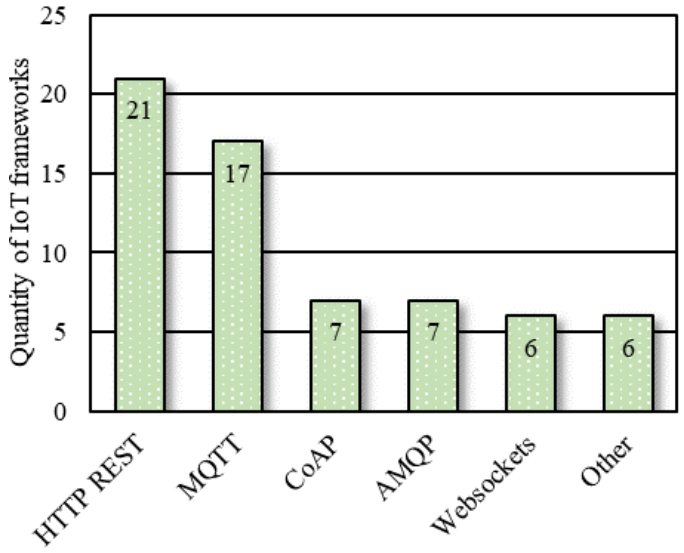

Figure 7. Messaging protocols adopted by the middleware layer of the IoT frameworks.

3.3.3 Application layer

The application layer serves to provide an interface for users/applications or third-party systems to interact with IoT elements of the IoT framework via the middleware layer. Interfaces for users are normally materialized as applications on end devices, such as desktop computers or mobile devices, enabling evaluation and visualization of data and providing control of actuators connected to IoT devices in the sensing layer. Within the application layer, data from the sensing layer may be visualized and analyzed by means of dashboards and data science tools. Furthermore, commands for actuators connected to IoT devices may be sent, enabling users to interact with the physical world.

Interfaces for end users may be categorized into three types, (i) web interfaces, (ii) mobile application interfaces, and (iii) personal computer (PC) application interfaces. On the one hand, web interfaces are developed for any type of device capable of executing a web browser and are hosted in web servers, reducing the memory and processor footprint in the device executing the interface. On the other hand, mobile and PC application interfaces are developed for specific mobile devices or software platforms. Mobile and PC applications are usually made available via software repositories, software stores, or software services that are available on the target system. In addition, sometimes it is also possible to install mobile applications directly on the target system. One advantage of developing mobile application interfaces for specific software and hardware platforms over web and PC application interfaces is the possibility to use integrated peripherals in the platform as sensors. In this case, devices connected to the application layer, primarily intended to provide a user interface, may also be part of the sensing layer of the IoT framework, allowing integrated sensors and actuators to be deployed. Table 10 presents the interfaces used in the application layer of the IoT frameworks surveyed in this study, with a visual representation shown in Figure 7. Mobile application interfaces and web interfaces are most favored, being enabled in 23 and 22 studies, respectively. PC application interfaces are only used in four studies.

Table 10. Interfaces enabled in the application layer of the IoT frameworks.

IoT framework	Web interface	Mobile application interface	PC application interface
Kamilaris *et al.* [38]		X	
Latre *et al.* [36]	X		
Pasini *et al.* [39]			X
Mainetti *et al.* [40]		X	
Khan *et al.* [42]		X	
Brincat *et al.* [43]	X		

Han *et al.* [44]	X	X	
Rinaldi *et al.* [47]	X		
Anjana *et al.* [49]	X	X	
Dong *et al.* [50]	X	X	
Verdouw *et al.* [53]	X		X
Tao *et al.* [54]		X	
Chen *et al.* [57]	X		
Badii *et al.* [58]	X	X	
Mulero *et al.* [35]	X		
Filippi *et al.* [59]	X	X	
Rahman *et al.* [60]		X	
Sotres *et al.* [61]	X	X	
Tripathy *et al.* [63]		X	
Tripathy *et al.* [64]		X	
Santos *et al.* [65]		X	
Mrozek *et al.* [66]	X	X	X
Verma *et al.* [67]	X	X	
Calderoni *et al.* [34]	X	X	X
Maatoug *et al.* [68]		X	
Jayaraman *et al.* [69]	X		
Bustamante *et al.* [70]	X		
Campos *et al.* [71]	X	X	
Badii *et al.* [72]	X	X	
Chang *et al.* [73]		X	
Gautam *et al.* [76]	X		
Mocnej *et al.* [77]	X	X	
Luckner *et al.* [79]	X	X	

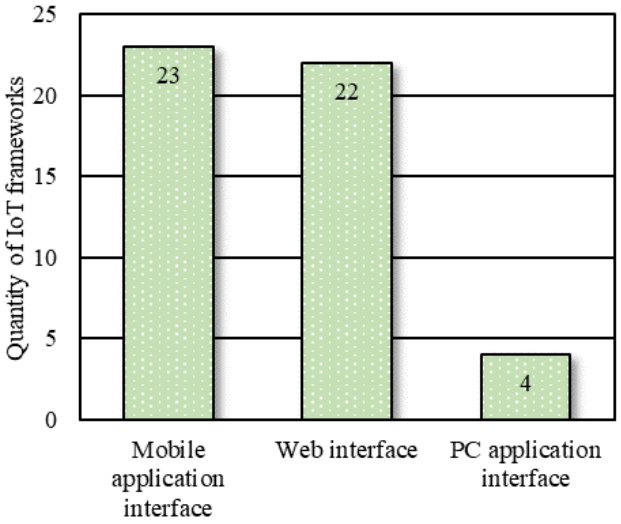

Figure 7. Interfaces enabled in the application layer of the IoT frameworks.

Data delivery in the application layer may be executed in real time or on demand, based on the need of users and the objective of the IoT framework. Table 10 presents the type of data delivery used in the studies, with a visual representation shown in Figure 8. It is observed that, with 28 studies, the majority of applications involve real-time data delivery, while on-demand data delivery is implemented in 15 studies.

Table 11. Data delivery in the application layer of the IoT frameworks.

IoT framework	On demand	Real-time
Kamilaris *et al.* [38]		X
Latre *et al.* [36]		X
Pasini *et al.* [39]	X	X
Khan *et al.* [42]		X
Brincat *et al.* [43]		X
Han *et al.* [44]		X
Basso *et al.* [46]	X	X
Anjana *et al.* [49]		X
Dong *et al.* [50]		X
Rathore *et al.* [51]	X	X
Yassine *et al.* [55]	X	X

Han *et al.* [56]	X	X
Chen *et al.* [57]	X	X
Badii *et al.* [58]		X
Mulero *et al.* [35]	X	
Rahman *et al.* [60]		X
Sotres *et al.* [61]	X	X
Tripathy *et al.* [63]		X
Tripathy *et al.* [64]		X
Santos *et al.* [65]	X	X
Mrozek *et al.* [66]	X	X
Verma *et al.* [67]	X	X
Calderoni *et al.* [34]	X	
Bustamante *et al.* [70]	X	X
Campos *et al.* [71]		X
Badii *et al.* [72]	X	X
Chang *et al.* [73]		X
Roduit *et al.* [74]	X	X
Gautam *et al.* [76]		X
Mocnej *et al.* [77]		X

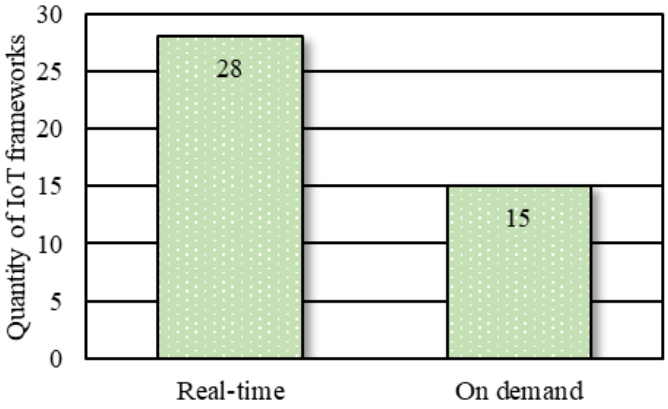

Figure 8. Data delivery in the application layer of the IoT frameworks.

4 Discussion and implications

This section presents the results of the survey of IoT frameworks for smart city applications. First, the findings and trends of each layer of the IoT frameworks surveyed in this study are

discussed. Second, a definition of the term “smart city” is suggested, alongside seven smart city domains, to be used as a basis for a generally accepted formal definition of a smart city. Finally, a novel IoT framework concept for smart city applications is proposed, based on the findings of the survey, in an attempt to provide a strong foundation for successful IoT framework implementations in the context of smart city applications.

4.1 Discussion of the survey

This subsection discusses the results of the survey process of each layer, i.e., sensing layer, middleware layer, and application layer of the IoT frameworks, which have been presented in Section 3. Discussions on each individual layer are developed and presented. Findings and trends observed during the survey process are presented, and strengths and weaknesses are identified.

In the ***sensing layer***, it has been identified that a variety of different devices are used, as shown in Figure 3. On the one hand, several IoT frameworks propose a sensing layer where any or most IoT devices may be used, rendering the IoT frameworks heterogeneous and attractive for utilization in different smart city applications. On the other hand, other IoT frameworks propose proprietary and self-assembled IoT devices, in Figure 3 labelled “others”, restricting the use of the IoT devices to the IoT framework that the IoT devices were designed for. Furthermore, in recent years, microcomputers and single-board computers have gained popularity in industry and research, which is reflected in the results of the survey, where many IoT devices of the sensing layer are Arduino-based and Raspberry Pi-based. However, it may be possible that several of the IoT frameworks have used Arduino- and Raspberry Pi-based IoT devices as prototypes, as the studies have also reported being designed to support a variety of devices. As

such, the great majority of IoT frameworks may be regarded as heterogeneous and usable in different smart city applications. In addition, smartphones are popular in the sensing layer of IoT frameworks for smart city applications, probably due to the ease of access, user friendliness, compact system design, and integrated sensor technology.

Regarding network protocols used by the IoT frameworks in the sensing layer, WiFi, 3G/4G/5G, 6LoWPAN/LoRA, ZigBee, and Bluetooth are used most, which may be due to the high commercial availability of hardware compatible with these network protocols. For example, WiFi modules often include hardware compliant with 6LoWPAN, Bluetooth, or the 3G/4G/5G standards. It is also observable that both energy efficient and energy demanding network protocols are used by the IoT frameworks. The balance in the usage of protocols may be attributed to the domain in which the IoT frameworks are used. For example, for IoT frameworks used in the smart infrastructure domain, it is easier to access a continuous power supply. However, for IoT frameworks used in the smart environment domain, it may be challenging to access continuous power supply and energy saving strategies must be implemented. It has also been found that RFID and NFC (based on RFID technology) are not popular in the IoT frameworks surveyed in his study, in spite of low cost and high availability of RFID technology, and may be attributed to the short range of communication.

In the ***middleware layer***, data storage for smart city applications is the most important (and mostly offered) service in the IoT frameworks surveyed in this study. Owing to the database management, historic data is stored and provides information for data analytics and machine learning algorithms, which are increasingly used in the IoT frameworks surveyed in this study. Historic data may help identify patterns in citizen activities and in the environment. Problems and threats may be analyzed and correlated with other historic data, revealing possible solutions in case of future occurrences. In addition, IoT device administration requires storing data

required to provide information about entities registered in the IoT frameworks. Many frameworks provide resource discovery and management, allowing a dynamic configuration of IoT devices, while advancing system robustness. However, it has been found that less than half of the IoT frameworks surveyed in this study target the technical challenges of interoperability and scalability. The lack of interoperability and scalability reduces the capability of the middleware layer of handling different sensing technologies, different application protocols, high quantities of sensors registered in the IoT framework, and demands of high processing power. It has also been identified that a few IoT frameworks, the majority being testbeds, target code management, revealing another caveat regarding the possibility of updating the functionality of the sensing layer remotely.

Regarding security, authentication is a fundamental service for the IoT middleware layer of IoT frameworks for smart city applications. Authentication is offered in most IoT frameworks surveyed in this study, providing data privacy and user access control. In addition, data should be encrypted in case of data hijacking or authentication breaches. Nevertheless, encryption is offered seldom, revealing security vulnerabilities in most IoT frameworks surveyed in this study.

The middleware layer of the IoT frameworks surveyed in this study offer a variety of messaging protocols. It has been found that the most popular messaging protocols are HTTP REST and MQTT, which goes in accordance to technology trends. CoAP has not been used frequently, in spite of being developed specifically for constraint devices. The lack of popularity of CoAP may be due to not being standardized, which in turn may make it difficult to integrate with different technologies. As such, the middleware layer of IoT frameworks should implement standardized messaging protocols, facilitating the integration of different technologies.

Finally, in the ***application layer***, web and mobile application interfaces have been observed to be equally enabled, while PC application interfaces are the least used type of interface. The difference between web and mobile application interfaces and PC application interface may be justified by the increased use of web applications and mobile phones in recent years. In addition, data delivery in the application layer of IoT frameworks tends towards real-time delivery of data. As such, real-time data encryption becomes more important, to provide improved security and data privacy.

4.2 Proposed smart city definition

In this subsection, the definition and concepts of smart cities are discussed. A definition of the term "smart city" and seven smart city domains are suggested, aiming to provide a basis for a generally accepted formal definition of a smart city.

As has been observed in the survey, a smart city should be able to optimize the use and exploitation of both tangible and intangible characteristics (hard and soft domains of smart cities). In addition, the implementation of a smart city differs depending on the region and the political situation. Therefore, the following smart city definition is suggested:

A smart city is a city, which provides transparency and an optimal setting for the development of the citizens, the economy, and the environment, using information and communication technologies in harmony with politics, infrastructure, natural resources, and human capital.

Alongside the smart city definition, seven smart city domains are proposed, building upon the characterizations introduced by Giffinger *et al.* [22], Lombardi *et al.* [82], and Neirotti *et al.* [23], as follows:

- **Smart economy**: Innovation, entrepreneurship, productivity and flexibility of labor market, and integration in the national and international market
- **Smart governance**: Political participation of citizens, public and social services, and transparent governance
- **Smart citizens**: Educational level, social integration and plurality, lifelong learning, creativity, flexibility, and participation in public life
- **Smart living**: Quality of life, such as cultural facilities and activities, healthcare, safety, housing, and tourism
- **Smart mobility**: Local and international accessibility, sustainable, innovative and safe transport systems, live traffic congestion management, and smart parking
- **Smart infrastructure**: Smart energy grids, smart buildings, public and private lighting, smart monitoring, waste management, smart cleaning, and comfort monitoring
- **Smart environment**: Attractive natural conditions, pollution, environmental protection, sustainable resource management, and sustainable resource management

It must be emphasized that, depending on the perspective, the domains may not be clearly delimited. For example, from the civil and environmental engineering perspective, smart infrastructure may be merged with smart environment. Figure 9 shows a visual representation of the smart city domains presented in this paper.

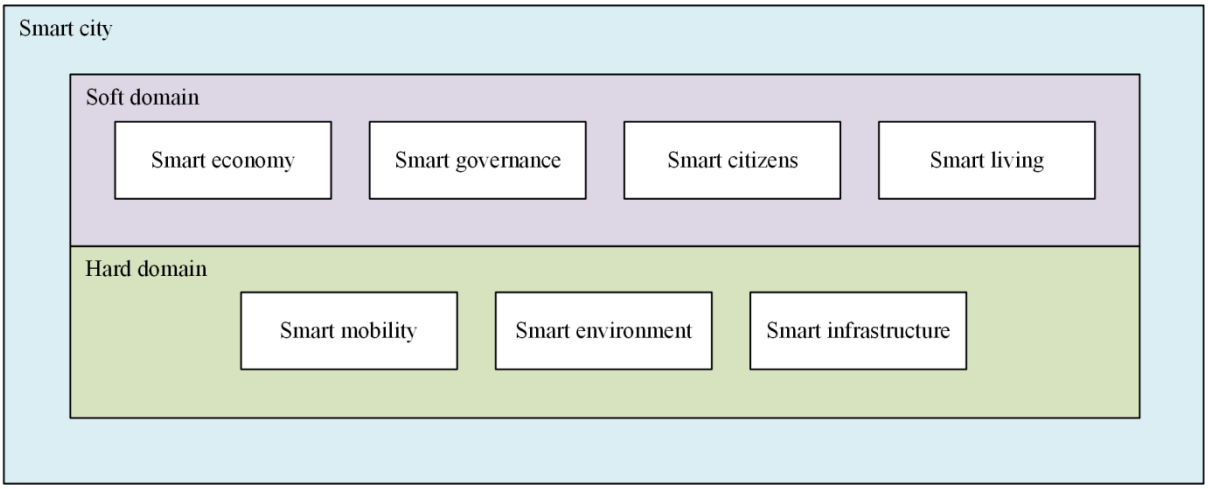

Figure 9. Characteristics of a smart city associated with the hard and soft domain.

4.3 An abstract IoT framework concept

Based on the survey results presented above, an abstract IoT framework concept for smart city applications is proposed, in an attempt to address the needs of smart city applications and to provide a strong foundation for successful IoT framework implementations. Figure 10 shows the proposed IoT framework concept, building upon the results and discussion presented in Sections 3 and 4, respectively. The main aspects addressed by the IoT framework concept are decentralization, autonomy, security, and modularity. In the ***middleware layer***, a decentralized service approach is suggested, hosted in a cloud and coordinated by a decentralized-service directory. The basic services are presented in Figure 10 as ellipses, with an additional ellipse representing other services that may be required, such as machine learning and ontologies; services of the middleware layer and the other layers are enabled to request functions, and the directory forwards the request to the corresponding decentralized service. Due to cloud hosting and decentralization, it is possible to provide scalability, availability, reliability, and modularity. The ***sensing layer*** should be able to integrate all types of IoT devices, from smartphones to single-board computers. In the case of IoT devices with low processing power, a gateway is proposed, enabling local processing capabilities and autonomy. Furthermore, all

IoT devices should be capable of using encryption mechanisms when transmitting private user data, securing data in case of communication hijacking. Finally, in the ***application layer***, encryption mechanisms are used when transmitting private user data, as in the sensing layer. In addition, the application layer provides a user interface capable of changing the processing logic of the sensing layer via the code management service provided in the middleware layer.

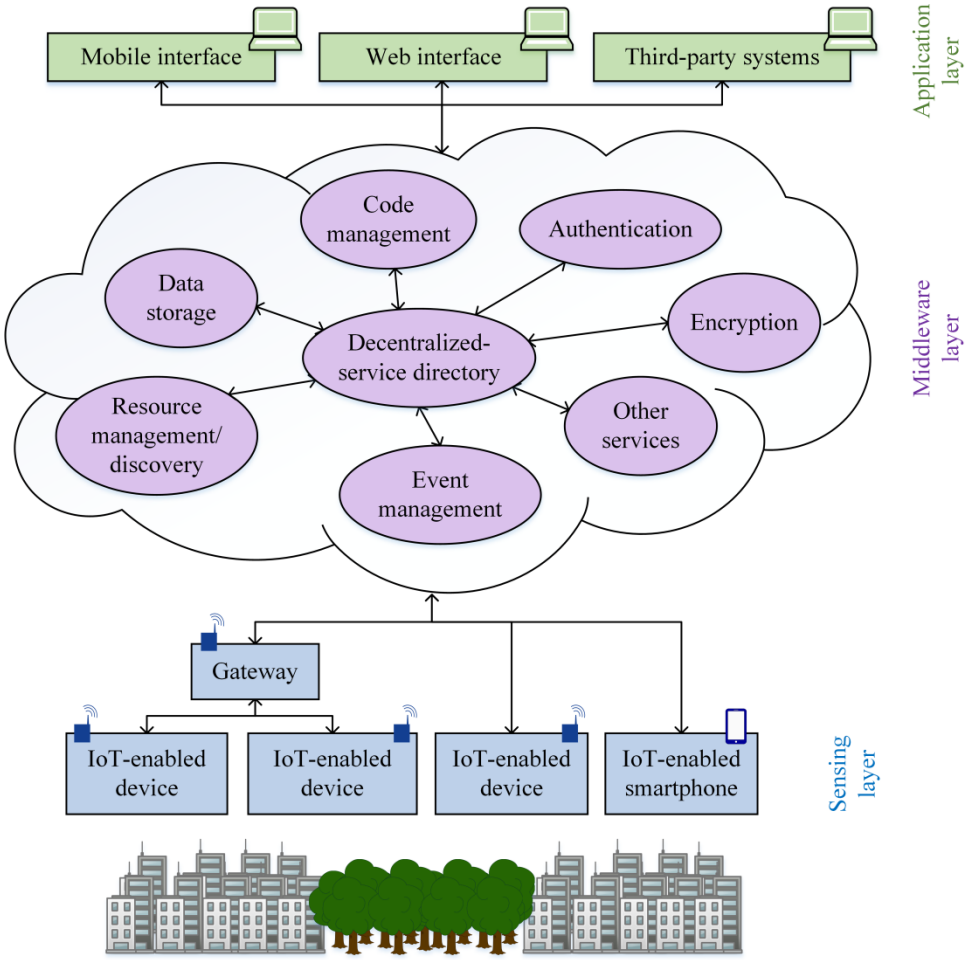

Figure 10. IoT framework concept for smart city applications proposed in this study.

5. Conclusions and future work

In this study, a survey of IoT frameworks for smart city applications has been presented, summarizing and comparing the technologies and architectures of IoT frameworks for smart city applications. In addition, definitions of the terms “smart city” and “IoT framework” have

been presented, based on existing concepts and guidelines, and best practices regarding IoT frameworks and smart cities have been discussed, complemented by an abstract IoT framework concept proposed based on the results of the survey.

IoT frameworks follow, in general, a three-layered architecture composed of sensing layer, middleware layer, and application layer. The communication between the layers requires strong security measures to protect data of being violated by unauthorized third parties. Although several IoT frameworks are available in the market, not all frameworks are suited for smart city applications. Special attention needs to be paid to decentralization, autonomy, security, and modularity in smart city applications. In addition, interoperability and hardware/software dependency has to be taken into account when implementing IoT frameworks for smart city applications, to offer a platform that copes with the heterogeneity of components, avoids vendor lock-in, and supports seamless use of different sensor data formats. Last, but not least, hardware and software capabilities and limitations of the IoT technologies have to be taken into account to address the user needs.

As a result of this study, the term “smart city” has been defined denoting the provider of transparency and an optimal setting for the development of the citizens, the economy, and the environment, using information and communication technologies in harmony with politics, infrastructure, natural resources, and human capital. The definition covers the definitions and concepts of current research and sets a foundation for further research. Furthermore, a novel IoT framework concept is proposed targeting the limitations of exciting frameworks and taking into account technology trends.

Future research may be conducted in regards of power consumption and energy harvesting to extend sensor autonomy, enabling long-lasting smart city applications. Furthermore, data

integration needs to be addressed, preferably via the inclusion of ontologies or sensor markup languages in the middleware layer. Finally, as the field of IoT frameworks for smart city applications is rapidly evolving, it must be emphasized that the active participation of city administrations is recommended in the process of choosing and implementing IoT frameworks for smart city applications.

Acknowledgments

This research is partially supported by the German Research Foundation (DFG) under grants SM 281/12-1, SM 281/14-1, SM 281/15-1, and SM 281/17-1. Any opinions, findings, conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the view of DFG.

2 References

[1] T. M. Heng and L. Low, "The intelligent city: Singapore achieving the next lap," *Technology Analysis & Strategic Management*, vol. 5, no. 2, p. 187, 1993, doi: 10.1080/09537329308524129.

[2] J. H. Lee, M. G. Hancock, and M.-C. Hu, "Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco," *Technological Forecasting and Social Change*, vol. 89, pp. 80–99, 2014, doi: 10.1016/j.techfore.2013.08.033.

[3] R. G. Hollands, "Will the Real Smart City Please Stand Up? Intelligent, progressive or entrepreneurial?," *City*, vol. 12, pp. 303–320, 2008, doi: 10.1080/13604810802479126.

[4] K. H. Law and J. P. Lynch, "Smart City: Technologies and Challenges," *IT Professional*, vol. 21, no. 6, pp. 46–51, 2019, doi: 10.1109/MITP.2019.2935405.

[5] A. Bassi and G. Horn, "Internet of Things in 2020: A Roadmap for the Future," *European Commission: Information Society and Media*, vol. 22, 2008.

[6] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, “Industry 4.0,” *Business & Information Systems Engineering*, vol. 6, no. 4, pp. 239–242, 2014, doi: 10.1007/s12599-014-0334-4.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[8] P. P. Ray, “A survey of IoT cloud platforms,” *Future Computing and Informatics Journal*, vol. 1, 1-2, pp. 35–46, 2016, doi: 10.1016/j.fcij.2017.02.001.

[9] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, “A Reference Model for Internet of Things Middleware,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 871–883, 2018, doi: 10.1109/JIOT.2018.2796561.

[10] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.

[11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[12] S. Talari, M. Shafie-khah, P. Siano, V. Loia, A. Tommasetti, and J. Catalão, “A Review of Smart Cities Based on the Internet of Things Concept,” *Energies*, vol. 10, no. 4, p. 421, 2017, doi: 10.3390/en10040421.

[13] B. N. Silva, M. Khan, and K. Han, “Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities,” *Sustainable Cities and Society*, vol. 38, pp. 697–713, 2018, doi: 10.1016/j.scs.2018.01.053.

[14] H. Arasteh *et al.*, "IoT-based smart cities: A survey," in *Proceedings of the 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Florence, Italy, Jun. 2016.

[15] P. Chamoso, A. González-Briones, S. Rodríguez, and J. M. Corchado, "Tendencies of Technologies and Platforms in Smart Cities: A State-of-the-Art Review," *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, 2018, doi: 10.1155/2018/3086854.

[16] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, "Advances on Sensing Technologies for Smart Cities and Power Grids: A Review," *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7596–7610, 2017, doi: 10.1109/JSEN.2017.2735539.

[17] H. Zhu *et al.*, "Review of state-of-the-art wireless technologies and applications in smart cities," in *Proceedings of the IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, China, Oct. 2017.

[18] N. Komninos, "The architecture of intelligent cities: integrating human, collective and artificial intelligence to enhance knowledge and innovation," in *Proceedings of the 2nd International Conference on Intelligent Environments (IE 06)*, Athens, Greece, Jul. 2006.

[19] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times – dg.o '11*, College Park, Maryland, 2011, p. 282.

[20] A. Caragliu, C. Del Bo, and P. Nijkamp, "Smart Cities in Europe," *Journal of Urban Technology*, vol. 18, no. 2, pp. 65–82, 2011, doi: 10.1080/10630732.2011.601117.

[21] S. Zygiaris, "Smart City Reference Model: Assisting Planners to Conceptualize the Building of Smart City Innovation Ecosystems," *Journal of the Knowledge Economy*, vol. 4, no. 2, pp. 217–231, 2013, doi: 10.1007/s13132-012-0089-4.

[22] R. Giffinger, C. Fertner, H. Kramar, and E. Meijers, *Smart cities – Ranking of European medium-sized cities*: Vienna University of Technology, 2007. [Online]. Available: http://curis.ku.dk/ws/files/37640170/smart_cities_final_repoit.pdf

[23] P. Neirotti, A. de Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in Smart City initiatives: Some stylised facts," *Cities*, vol. 38, pp. 25–36, 2014, doi: 10.1016/j.cities.2013.12.010.

[24] H. Chourabi *et al.*, "Understanding Smart Cities: An Integrative Framework," *45th Hawaii International Conference on System Sciences*, pp. 2289–2297, 2012, doi: 10.1109/HICSS.2012.615.

[25] V. Albino, U. Berardi, and R. M. Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives," *Journal of Urban Technology*, vol. 22, no. 1, pp. 3–21, 2015, doi: 10.1080/10630732.2014.942092.

[26] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, vol. 56, pp. 122–140, 2017, doi: 10.1016/j.adhoc.2016.12.004.

[27] S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, "IoT Frameworks and Complexity," in *Demystifying Internet of Things Security*, S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, Eds., Berkeley, CA: Apress, 2020.

[28] O. Uviase and G. Kotonya, "IoT Architectural Framework: Connection and Integration Framework for IoT Systems," *Electronic Proceedings in Theoretical Computer Science*, vol. 264, 2018, doi: 10.4204/EPTCS.264.1.

[29] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, "Comparison of IoT platform architectures: A field study based on a reference architecture," in *Proceedings of the 2nd Cloudification of the Internet of Things*, Paris, France, Nov. 2016.

[30] IEEE Internet Initiative, "Towards a definition of the Internet of Things (IoT)," Institute of Electrical and Electronics Engineers (IEEE) Internet Initiative, 2015. Accessed: Jun. 30

2020. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[31] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016, doi: 10.1109/JIOT.2015.2498900.

[32] *Smart City Guidance Package*, 2019, EIP-SCC, 2019. [Online]. Available: https://eu-smartcities.eu/news/smart-city-guidance-package

[33] *Best practice guide – Smart cities standards*, 2018, Smart Cities Council Australia New Zealand, Australia New Zealand, May. 2018. [Online]. Available: https://anz.smartcitiescouncil.com/resources/guidance-note-smart-cities-standards

[34] L. Calderoni, A. Magnani, and D. Maio, "IoT Manager: An open-source IoT framework for smart cities," *Journal of Systems Architecture*, vol. 98, pp. 413–423, 2019, doi: 10.1016/j.sysarc.2019.04.003.

[35] R. Mulero *et al.*, "An IoT-Aware Approach for Elderly-Friendly Cities," *IEEE Access*, vol. 6, pp. 7941–7957, 2018, doi: 10.1109/ACCESS.2018.2800161.

[36] S. Latre, P. Leroux, T. Coenen, B. Braem, P. Ballon, and P. Demeester, "City of things: An integrated and multi-technology testbed for IoT smart city experiments," in *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2)*, Trento, Italy, Sep. 2016.

[37] S. K. Datta, R. P. Ferreira da Costa, C. Bonnet, and J. Harri, "oneM2M architecture based IoT framework for mobile crowd sensing in smart cities," in *Proceedings of the 2016 European Conference on Networks and Communications (EuCNC)*, Athens, Greece, Jun. 2016.

[38] A. Kamilaris, F. Gao, F. X. Prenafeta-Boldu, and M. I. Ali, "Agri-IoT: A semantic framework for Internet of Things-enabled smart farming applications," in *Proceedings of*

the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, Dec. 2016.

[39] D. Pasini, S. M. Ventura, S. Rinaldi, P. Bellagente, A. Flammini, and A. L. C. Ciribini, "Exploiting Internet of Things and building information modeling framework for management of cognitive buildings," in *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2)*, Trento, Italy, Sep. 2016.

[40] L. Mainetti, L. Patrono, A. Secco, and I. Sergi, "An IoT-aware AAL system for elderly people," in *Proceedings of the 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, Split, Croatia, Jul. 2016.

[41] J. Pacheco, D. Ibarra, A. Vijay, and S. Hariri, "IoT Security Framework for Smart Water System," in *Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, Hammamet, Tunisia, Oct. 2017.

[42] T. Khan, S. Ghosh, M. Iqbal, G. Ubakanma, and T. Dagiuklas, "RESCUE: A Resilient Cloud Based IoT System for Emergency and Disaster Recovery," in *Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Exeter, United Kingdom, Jun. 2018.

[43] A. A. Brincat, F. Pacifici, S. Martinaglia, and F. Mazzola, "The Internet of Things for Intelligent Transportation Systems in Real Smart Cities Scenarios," in *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, Apr. 2019.

[44] Y. Han, B. Park, and J. Jeong, "A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications," *Procedia Computer Science*, vol. 155, pp. 728–733, 2019, doi: 10.1016/j.procs.2019.08.105.

[45] J. Jokinen, T. Latvala, and J. L. Martinez Lastra, “Integrating smart city services using Arrowhead framework,” in *Proceedings of the IECON 2016 – 42nd Annual Conference of the IEEE Industrial Electronics Society*, Florence, Italy, Oct. 2016.

[46] G. Basso, D. Gabioud, and P. Roduit, “IoT Architecture for Decentralised Heating Control in Households,” in *Proceedings of the 7th International Conference on Smart Cities and Green ICT Systems*, Madeira, Portugal, Mar. 2018.

[47] S. Rinaldi, A. Flammini, L. C. Tagliabue, and A. L. C. Ciribini, “An IoT framework for the assessment of indoor conditions and estimation of occupancy rates: results from a real case study,” *ACTA*, vol. 8, no. 2, pp. 70–79, 2019, doi: 10.21014/acta_imeko.v8i2.647.

[48] D. Sembroiz, S. Ricciardi, and D. Careglio, “A Novel Cloud-Based IoT Architecture for Smart Building Automation,” in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*: Elsevier, 2018.

[49] M. S. Anjana, M. V. Ramesh, A. R. Devidas, and K. Athira, “Fractal IoT: A Scalable IoT Framework for Energy Management in Connected Buildings,” in *Proceedings of the 1st ACM International Workshop on Technology Enablers and Innovative Applications for Smart Cities and Communities – TESCA'19*, New York, NY, USA, 2019.

[50] Z. Dong, A. M. Abdulghani, M. A. Imran, and Q. H. Abbasi, “Artificial Intelligence Enabled Smart Refrigeration Management System Using Internet of Things Framework,” in *Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things*, Sanya, China, Apr. 2020.

[51] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, “Urban planning and building smart cities based on the Internet of Things using Big Data analytics,” *Computer Networks*, vol. 101, pp. 63–80, 2016, doi: 10.1016/j.comnet.2015.12.023.

[52] M. Gheisari, G. Wang, and S. Chen, “An Edge Computing-enhanced Internet of Things Framework for Privacy-preserving in Smart City,” *Computers & Electrical Engineering*, vol. 81, p. 106504, 2020, doi: 10.1016/j.compeleceng.2019.106504.

[53] C. Verdouw, H. Sundmaeker, B. Tekinerdogan, D. Conzon, and T. Montanaro, "Architecture framework of IoT-based food and farm systems: A multiple case study," *Computers and Electronics in Agriculture*, vol. 165, p. 104939, 2019, doi: 10.1016/j.compag.2019.104939.

[54] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, pp. 1040–1051, 2018, doi: 10.1016/j.future.2016.11.011.

[55] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Generation Computer Systems*, vol. 91, pp. 563–573, 2019, doi: 10.1016/j.future.2018.08.040.

[56] Y. Han, B. Park, and J. Jeong, "Fog Based IIoT Architecture Based on Big Data Analytics for 5G-networked Smart Factory," in *Lecture Notes in Computer Science, Computational Science and Its Applications – ICCSA 2019*, S. Misra et al., Eds., Cham: Springer International Publishing, 2019.

[57] L.-J. Chen *et al.*, "An Open Framework for Participatory PM2.5 Monitoring in Smart Cities," *IEEE Access*, vol. 5, pp. 14441–14454, 2017, doi: 10.1109/ACCESS.2017.2723919.

[58] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects," *IEEE Access*, vol. 8, pp. 23601–23623, 2020, doi: 10.1109/ACCESS.2020.2968741.

[59] F. de Filippi *et al.*, "MiraMap: A We-Government Tool for Smart Peripheries in Smart Cities," *IEEE Access*, vol. 4, pp. 3824–3843, 2016, doi: 10.1109/ACCESS.2016.2548558.

[60] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy

Services in a Smart City," *IEEE Access*, vol. 7, pp. 18611–18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[61] P. Sotres, J. R. Santana, L. Sanchez, J. Lanza, and L. Munoz, "Practical Lessons From the Deployment and Management of a Smart City Internet-of-Things Infrastructure: The SmartSantander Testbed Case," *IEEE Access*, vol. 5, pp. 14309–14322, 2017, doi: 10.1109/ACCESS.2017.2723659.

[62] T. Wang, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and J. Cao, "Big Data Reduction for a Smart City's Critical Infrastructural Health Monitoring," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 128–133, 2018, doi: 10.1109/MCOM.2018.1700303.

[63] A. K. Tripathy, P. K. Tripathy, N. K. Ray, and S. P. Mohanty, "iTour: The Future of Smart Tourism: An IoT Framework for the Independent Mobility of Tourists in Smart Cities," *IEEE Consumer Electronics Magazine*, vol. 7, no. 3, pp. 32–37, 2018, doi: 10.1109/MCE.2018.2797758.

[64] A. K. Tripathy, P. K. Tripathy, A. G. Mohapatra, N. K. Ray, and S. P. Mohanty, "WeDoShare: A Ridesharing Framework in Transportation Cyber-Physical System for Sustainable Mobility in Smart Cities," *IEEE Consumer Electronics Magazine*, vol. 9, no. 4, pp. 41–48, 2020, doi: 10.1109/MCE.2020.2978373.

[65] P. M. Santos *et al.*, "PortoLivingLab: An IoT-Based Sensing Platform for Smart Cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 523–532, 2018, doi: 10.1109/JIOT.2018.2791522.

[66] D. Mrozek, A. Koczur, and B. Małysiak-Mrozek, "Fall detection in older adults with mobile IoT devices and machine learning in the cloud and on the edge," *Information Sciences*, vol. 537, pp. 132–147, 2020, doi: 10.1016/j.ins.2020.05.070.

[67] P. Verma, S. K. Sood, and S. Kalra, “Cloud-centric IoT based student healthcare monitoring framework,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 5, pp. 1293–1309, 2018, doi: 10.1007/s12652-017-0520-6.

[68] A. Maatoug, G. Belalem, and S. Mahmoudi, “Fog computing framework for location-based energy management in smart buildings,” *Multiagent and Grid Systems*, vol. 15, no. 1, pp. 39–56, 2019, doi: 10.3233/MGS-190301.

[69] P. P. Jayaraman, A. Yavari, D. Georgakopoulos, A. Morshed, and A. Zaslavsky, “Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt,” *Sensors*, vol. 16, no. 11, p. 1884, 2016, doi: 10.3390/s16111884.

[70] A. L. Bustamante, M. A. Patricio, and J. M. Molina, “Thinger.io: An Open Source Platform for Deploying Data Fusion Applications in IoT Environments,” *Sensors*, vol. 19, no. 5, p. 1044, 2019, doi: 10.3390/s19051044.

[71] N. G. S. Campos, A. R. Rocha, R. Gondim, T. L. Coelho da Silva, and D. G. Gomes, “Smart & Green: An Internet-of-Things Framework for Smart Irrigation,” *Sensors*, vol. 20, no. 1, p. 190, 2019, doi: 10.3390/s20010190.

[72] C. Badii, P. Bellini, A. Difino, and P. Nesi, “Sii-Mobility: An IoT/IoE Architecture to Enhance Smart City Mobility and Transportation Services,” *Sensors*, vol. 19, no. 1, p. 1, 2018, doi: 10.3390/s19010001.

[73] B. R. Chang, H.-F. Tsai, H.-C. Kuo, and C.-F. Huang, “Smart iAIR System with Integration of the Internet of Things and Mobile Applications,” *Sensors and Materials*, vol. 31, no. 8, pp. 2451–2462, 2019, doi: 10.18494/SAM.2019.2405.

[74] P. Roduit, D. Gabioud, G. Basso, G. Maitre, and P. Ferrez, “cloud.iO: A Decentralised IoT Architecture to Control Electrical Appliances in Households,” in *Communications in Computer and Information Science, Smart Cities, Green Technologies and Intelligent Transport Systems*, B. Donnellan, C. Klein, M. Helfert, and O. Gusikhin, Eds., Cham: Springer International Publishing, 2019.

[75] J. Lohokare, R. Dani, A. Rajurkar, and A. Apte, “An IoT ecosystem for the implementation of scalable wireless home automation systems at smart city level,” in *Proceedings of the 2017 IEEE Region Ten Conference*, Penang, Malaysia, Nov. 2017.

[76] G. Gautam, G. Sharma, B. T. Magar, B. Shrestha, S. Cho, and C. Seo, “Usage of IoT Framework in Water Supply Management for Smart City in Nepal,” *Applied Sciences*, vol. 11, no. 12, p. 5662, 2021, doi: 10.3390/app11125662.

[77] J. Mocnej *et al.*, “Quality-enabled decentralized IoT architecture with efficient resources utilization,” *Robotics and Computer-Integrated Manufacturing*, vol. 67, p. 102001, 2021, doi: 10.1016/j.rcim.2020.102001.

[78] V. Slaný, A. Lučanský, P. Koudelka, J. Mareček, E. Krčálová, and R. Martínek, “An Integrated IoT Architecture for Smart Metering Using Next Generation Sensor for Water Management Based on LoRaWAN Technology: A Pilot Study,” *Sensors*, vol. 20, no. 17, p. 4712, 2020, doi: 10.3390/s20174712.

[79] M. Luckner, M. Grzenda, R. Kunicki, and J. Legierski, “IoT Architecture for Urban Data-Centric Services and Applications,” *ACM Trans. Internet Technol.*, vol. 20, no. 3, pp. 1–30, 2020, doi: 10.1145/3396850.

[80] M. T. Lazarescu, “Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45–54, 2013, doi: 10.1109/JETCAS.2013.2243032.

[81] L. Sanchez *et al.*, “SmartSantander: IoT experimentation over a smart city testbed,” *Computer Networks*, vol. 61, pp. 217–238, 2014, doi: 10.1016/j.bjp.2013.12.020.

[82] P. Lombardi, S. Giordano, H. Farouh, and W. Yousef, “Modelling the smart city performance,” *Innovation: The European Journal of Social Science Research*, vol. 25, no. 2, pp. 137–149, 2012, doi: 10.1080/13511610.2012.660325.