Internet of Things frameworks for smart city applications –
a systematic review

José Joaquín Peralta-Abadía and Kay Smarsly

Institute of Digital and Autonomous Construction, Hamburg University of Technology,
Hamburg, Germany; email: {joaquin.peralta; kay.smarsly}@tuhh.de

ABSTRACT

The advent of smart monitoring and cyber-physical systems in civil engineering has significantly propelled a broad wealth of smart city applications. Representing a vital technological basis of smart city applications, Internet of Things (IoT) frameworks have been an increasing topic of research in recent years. However, different definitions of the terms “smart city” and “IoT framework” are used without consensus, and the technical aspects of IoT frameworks for smart city applications have not been fully reviewed, causing ambiguities and redundant developments in the community. This paper aims to condense the definitions of the terms “smart city” and “IoT framework” by summarizing and comparing concepts. Besides critical IoT technologies, sensor node hardware utilized in IoT frameworks is summarized in a systematic review. As a result of this study, IoT framework trends for smart city applications are provided. It is expected that the findings of trends of IoT frameworks for smart city applications presented in this study may serve as a basis for future IoT framework implementations that advance smart city applications.

Keywords: Smart cities, Internet of Things (IoT), IoT frameworks, smart monitoring, cyber-physical systems

1. INTRODUCTION

Traditional civil engineering applications are increasingly being replaced by smart city applications, driven by innovative technologies, such as cyber-physical systems and smart structures, by advancements in artificial intelligence techniques, and by recent developments related to Industry 4.0 (Luckey et al. 2020; Fritz and Smarsly 2020). Essentially, smart cities enhance the utilization of urban services by citizens (Law and Lynch 2019). A key element commonly used in smart city applications is the Internet of Things (IoT). IoT may be referred to as a world-wide network of billions of interconnected devices (“things”), which may be coupled through the Internet to connect smart cities and the citizens (Gubbi et al. 2013). IoT frameworks enable the interaction between IoT elements, providing an environment that defines the architecture of IoT applications and the functionality of IoT elements. Nevertheless, the variety of IoT technologies may render IoT framework implementations complicated and inefficient, creating sub-par results and additional costs for the users.

Several literature reviews of IoT frameworks and smart cities have been carried out, each of which placing emphasis on different aspects. Also, definitions of the term “smart city” and characteristics and domains of smart cities have been reviewed (Silva et al. 2018). Further efforts have focused on smart energy management and energy harvesting (Morello et al. 2017). Existing
IoT technologies used in smart cities have been reviewed and compared, as well as challenges and opportunities for smart cities (Talari et al. 2017). Although the reviews have presented different technical aspects of IoT frameworks, the technologies used by IoT frameworks for smart city applications have not been summarized and compared, which is the main goal of the review conducted in this study. The remainder of this paper is structured as follows. Section 2 introduces concepts of smart cities and IoT frameworks. Section 3 presents the review of IoT frameworks for smart city applications, summarizing and comparing the elements of the sensing and middleware layers. Section 4 discusses the results of the review of IoT frameworks. Finally, Section 5 provides conclusions and future work.

2. CONCEPTS AND GUIDELINES

This section analyzes concepts of smart cities and IoT frameworks necessary to review IoT frameworks for smart city applications. First, working definitions and domains of smart cities are presented. Thereupon, working definitions and architectures of IoT frameworks are illuminated.

Several definitions have been proposed for the term “smart city”. The term has been defined as a city that invests in human and social capital, political participation of citizens, management of natural resources, and traditional and modern networked infrastructure (Caragliu et al. 2011). Furthermore, the term has been defined as a city that addresses innovative socio-technical and socio-economic aspects of growth (Zygiaris 2013). As with the definitions, smart city domains have been defined in different ways. For example, smart city domains have been listed as smart economy, smart people, smart governance, smart mobility, smart environment and smart living (Giffinger et al. 2007). A further expansion of the list has included smart buildings (Neirotti et al. 2014). Proposals of smart city domains have been reviewed and described (Albino et al. 2015). Furthermore, smart city domains have been categorized as soft domains and hard domains, referring to intangible and tangible characteristics of smart cities, respectively (Neirotti et al. 2014). Building upon the characterizations presented above, this study proposes smart economy, smart governance, smart citizens (instead of smart people), and smart living as soft domains of a smart city. Furthermore, smart mobility, smart environment, and smart infrastructure (instead of smart buildings) are proposed as hard domains of a smart city.

IoT frameworks have been defined as agents between IoT elements that serve as application interfaces, enabling interaction between the IoT elements (Cheruvu et al. 2020). However, the terms “IoT framework”, “IoT platform”, and “IoT middleware” are used interchangeably. Based on the usage and general definitions of the terms used in the context of information and communication technologies, this study adapts the terms to the IoT framework concept. Consequently, IoT platforms host IoT middleware, and IoT frameworks provide the environment for the communication between IoT middleware and other IoT elements. The IEEE Internet Initiative (2015) has proposed a three-layered IoT framework architecture composed of application layer, networking and data communications layer, and sensing layer. Furthermore, Guth et al. (2016) have proposed an IoT framework architecture comprising application layer, integration middleware layer, gateway layer, device layer, and sensor and actuator layer. The IoT integration middleware layer and gateway layer of Guth et al. is analogous to the networking and data communications layer of the IEEE Internet Initiative. The sensing layer of the IEEE Internet Initiative is equivalent to the 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.
3. REVIEW OF IOT FRAMEWORKS FOR SMART CITY APPLICATIONS

This section reviews IoT frameworks for smart city applications. First, the methodology pursued in the review process is presented. Then, the review of IoT frameworks for smart city applications, summarizing and comparing smart city domains and the IoT elements of the sensing and middleware layers, is detailed. For the sake of brevity, the application layer of the IoT frameworks will be omitted, since the main purpose of the application layer is data visualization for users and does not have IoT elements and technologies to be reviewed. Full details of the IoT frameworks and of the review results will be shown in the presentation at the conference.

3.1 Methodology

The review methodology comprises three steps, (i) data collection, (ii) data organization, and (iii) data analysis. The data collection involves studies indexed in the Web of Science Core Collection, supplemented by conference papers indexed in the Scopus database. During the data collection step, 54 studies have been identified. In the data organization step, the IoT elements of the IoT frameworks have been tabulated. Finally, the data analysis has been carried out and is presented in the following subsections.

3.2 Smart city domain applicability

Smart cities are characterized by seven domains, as introduced in Section 2. Several studies report IoT frameworks that are created for being used in some or in all smart city domains (Calderoni et al. 2019). However, most IoT frameworks for smart city applications are usually used in solely one of the seven domains. Figure 1 presents the categorization of IoT frameworks into the smart city domains. Hard domains are presented in red, soft domains are presented in cyan, and an extra category for IoT frameworks that belong to all domains is presented in gray. From the IoT frameworks reviewed in this study, 50 IoT frameworks are used in hard domains of a smart city and eight IoT frameworks are used in soft domains. Finally, ten IoT frameworks may be used in all domains of a smart city.

![Figure 1. Categorization of IoT frameworks into the smart city domains.](image-url)
3.3 Sensing layer

The sensing layer provides functionality for using IoT devices that sense and actuate in the real world. Figure 2 presents the IoT devices used in the sensing layer of the IoT frameworks reviewed in this study, in which some IoT frameworks accept any IoT devices and other IoT frameworks are tested and defined for specific IoT devices. On the one hand, aiming at interoperability, 16 IoT frameworks are able to use any IoT device. On the other hand, 38 IoT frameworks are designed and tested to work with specific IoT devices, in which some IoT frameworks may use more than one specific IoT device type, as in Hussain et al. (2015). From the IoT frameworks that use specific IoT devices, custom IoT devices are used 16 times, Arduino-based IoT devices are used ten times, smartphones are used nine times, and Raspberry Pi-based IoT devices are used seven times, mostly as gateways between other IoT devices and the middleware layer. Some of the IoT devices are resource-constraint, which may affect the longevity and autonomy of the IoT device. Nevertheless, only six studies dwell in resource optimization, e.g. in Verdouw et al. (2019).

![Figure 2. IoT device types used in the sensing layer of IoT frameworks.](image)

3.4 Middleware layer

Within the middleware layer, services necessary for the operation of the sensing and the application layer are provided. Figure 3 presents the services that are provided by the middleware layer in the IoT frameworks reviewed in this study. Database management is the most provided service, used in 42 IoT frameworks. Aiming to satisfy security requirements, 38 IoT frameworks provide authentication services and 14 IoT frameworks provide encryption functions. Furthermore, event and alert management is offered in 33 IoT frameworks. Regarding the management and registration of IoT devices (resources) in the sensing layer, resource management and resource discovery is provided in 30 and 26 IoT frameworks, respectively. Targeting the recent popularity of machine learning (ML), 12 IoT frameworks incorporate machine learning algorithms for data analytics and predictions of future trends in the smart cities. Finally, the least provided service is code management, used only by five IoT frameworks.
4. DISCUSSION AND IMPLICATIONS

This section discusses the results of the review of smart city domains, the sensing layer, and the middleware layer presented in Section 3. Discussions of smart city domains and both layers are presented individually as follows.

In the **smart city domains**, the majority of IoT frameworks are used in the hard domains of a smart city. Since hard domains of smart cities refer to tangible characteristics, such as built infrastructure and the environment, IoT technologies are easier to be implemented and quantified in the hard domains. By contrast, soft domains, representing intangible characteristics, are more difficult to quantify, entailing less attraction for smart cities to invest in IoT frameworks to be used in soft domains.

In the **sensing layer**, the majority of IoT frameworks work with specific IoT devices, which are mostly microcomputers and resource-constrained devices. The downside of using specific IoT devices is the lack of interoperability, limiting the type of IoT devices that can be used, and limiting the portability of the IoT frameworks to other smart city applications and domains. On the contrary, several IoT frameworks can work with any IoT device, providing interoperability and portability. In addition, smartphones have proven to be capable of being used in the sensing layer of IoT frameworks, owing to integrated sensors, usability, and wide-spread availability in the citizenship.

In the **middleware layer**, database management is the most offered service, representing a service necessary for other services, such as resource management and resource discovery. Furthermore, database management allows using historic data for data analytics and machine learning algorithms, both being research areas of increasing interest in recent years. Regarding security services, the majority of IoT frameworks offer authentication services, preventing unauthorized access to the smart city applications, while other frameworks, however, may suffer from security vulnerabilities related to data encryption that may lead to data hijacking and violation
of data privacy. Finally, a few IoT frameworks offer code management services, limiting upgradeability and flexibility of the IoT frameworks for smart city applications.

5. SUMMARY AND CONCLUSIONS

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

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 violations by unauthorized third parties. Although most IoT frameworks offer authentication services, just a few offer encryption functions, revealing security vulnerabilities. Interoperability and code management have to also be targeted, supporting the use of emerging IoT devices and IoT technologies and the upgradeability of existing IoT devices. Based on the findings of this study, a need for an IoT framework concept addressing decentralization, autonomy, security, and modularity has been identified.

Future research may focus on proposing a new IoT framework concept to overcome the drawbacks of current IoT frameworks revealed in this study, targeting interoperability and decentralization of the services as well as functionality offered by IoT frameworks for smart city applications. Furthermore, a more formal definition of the term “smart city” may be proposed, consolidating existing definitions and limiting the self-promotion of smart cities that focus only on business interests, instead of the well-being of the citizens.

ACKNOWLEDGMENTS

The work conducted in this study is partially supported by the German Research Foundation (DFG) through grant SM 281/12 and grant SM 281/17. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of DFG.

REFERENCES


