IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 29, 2020, accepted November 21, 2020, date of publication November 30, 2020,
date of current version December 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3041326

bIoTope: Building an IoT Open Innovation Ecosystem for Smart Cities

ASAD JAVED[1], (Member, IEEE), SYLVAIN KUBLER[2], (Member, IEEE), AVLEEN MALHI[1], ANTTI NURMINEN[1], JÉRÉMY ROBERT[3], AND KARY FRÄMLING[1,4], (Member, IEEE)

[1]Department of Computer Science, Aalto University, 02150 Espoo, Finland
[2]CNRS, CRAN, Université de Lorraine, F-54000 Nancy, France
[3]Interdisciplinary Centre for Security, Reliability, and Trust, University of Luxembourg, L-2721 Luxembourg, Luxembourg
[4]Department of Computing Science, Umeå University, Mit-huset, 901 87 Umeå, Sweden

Corresponding author: Asad Javed (asad.javed@aalto.fi)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme under Grant 688203, in part by the Academy of Finland, Open Messaging Interface, under Grant 296096, and in part by the H2020 Project FINEST TWINS under Grant 856602.

ABSTRACT The Internet of Things (IoT) has led towards a digital world in which everything becomes connected. Unfortunately, most of the currently marketed connected devices feed vertically-oriented closed systems (commonly referred to as *vertical silos*) which prevent the development of a unified global IoT. This issue is all the more valid in complex environments, such as smart cities, in which exceedingly large amounts of heterogeneous sensor data are collected, and in which platforms and stakeholders should also be able to interact and cooperate. Therefore, it is of utmost importance to move towards the creation of open IoT ecosystems to support efficient smart city service integration, discovery and composition. This paper contributes to the specifications of such an ecosystem, which has been developed as part of the EU's H2020 bIoTope project. The novelty of this ecosystem compared with the current literature is threefold: (i) it is based on the extensive use of open communication and data standards, *notably O-MI and O-DF standards*, that foster technical, syntactic and semantic interoperability over domains; (ii) it proposes an innovative service marketplace for data/service publication, discovery and incentivization; (iii) it integrates security functionalities at the IoT gateway level. The practicability of our ecosystem has been validated through several smart city proofs-of-concept set up in three distinct cities: Helsinki, Lyon and Brussels. Given the five major themes defined in the CITYKeys (a smart city performance indicator framework), namely People, Planet, Prosperity, Governance and Propagation, bIoTope mainly contributes to Prosperity-related metrics, as discussed in this paper.

INDEX TERMS Internet of Things, smart city, service discovery, open IoT ecosystem, communication standards.

I. INTRODUCTION

Information and Communication Technologies (ICT) are revolutionizing cities. More connected and optimally managed, smart cities seek to enhance the economic, social, cultural and urban development, while fostering competitive environments for the development of new businesses [1]. More efficient and transparent, they respond to the new expectations of citizens, who increasingly prefer to take a more active role in managing their cities. A smart city is a complex ecosystem, comprising many sub-systems, vast amounts of heterogeneous data from sensors and other devices, and a wide range of interacting and cooperating city stakeholders such as citizens, governments, companies, hardware and software providers, and logistic centers [2], [3]. Given this complexity, it is not an easy task to define the attributes of a smart city, its core components, and ways to evaluate the *smartness* of a city [4]–[8]. Several Key Performance Indicator (KPI) frameworks measure the outcome of smart city programs [9], [10]. ICT technologies such as IoT (Internet of Things), Cloud Computing, Big Data and AI (Artificial Intelligence) are the key in such measurement but also improve some of those KPIs. For example, particle matter and CO2 sensors, combined with online decision support systems, can help cities to analyze outdoor air quality and take actions to mitigate CO2 emissions (e.g., by suggesting

The associate editor coordinating the review of this manuscript and approving it for publication was A. Taufiq Asyhari.

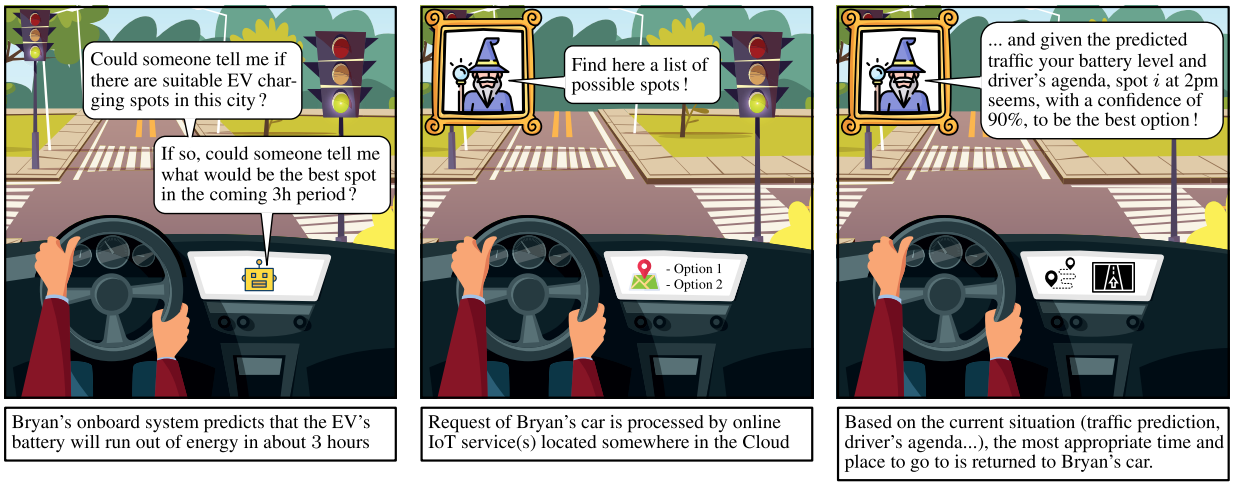


FIGURE 1. Illustration of an ideal IoT world in which smart city data and services can be easily integrated, discovered and used by a wide range of city stakeholders (incl., citizens, and public and private institutions).

different commute alternatives to citizens). Ultimately this contributes to pollution- and health-related KPIs.

To efficiently achieve such KPIs, it is critical for cities to configure a viable IoT infrastructure, both technologically and business-wise. In an ideal IoT world, smart city infrastructures must provide the means to create, when and as needed, ad hoc and loosely coupled information flows between any kinds of smart connected objects, databases and users. The operation of such an ideal world is illustrated with a comic-style scenario in FIGURE 1, in which an Electric Vehicle (EV) enters a city and predicts that the EV battery will run out of energy in about 3*h*. In an ideal IoT world, the car should be able to discover the optimal time and EV charging spot in the city for re-charging the car (depending for instance on the predicted traffic, driver's agenda and weather forecasts). Unfortunately, the reality is not that simple especially in heterogeneous and constantly changing environments, such as smart cities. For example, how should the car proceed to discover the available services in the city? Conversely, how could the car spin up (i.e., publish) its own digital avatar[1]? How does the car communicate with online platforms/systems that implement different types of communication protocols? How does the car communicate car and driver-related data without compromising security and privacy? These challenges are more severe and magnified in a smart city context as smart city programs are often driven by corporate goals and large technological conglomerates which, in most cases, rely on closed and vendor lock-in solutions for profit purposes.

To overcome the aforementioned challenges, this article introduces an open IoT ecosystem that fosters horizontal integration (i.e., cross-domain and cross-platform development) for smart cities. This ecosystem is developed in the bIoTope project funded under the EU's Horizon 2020 Research and Innovation Programme. The novelty of this ecosystem compared with the current state-of-the-art is threefold: (i) it is based on open standards for communication and data that improve cross-domain interoperability at the technical, syntactic and semantic levels; (ii) it proposes a service marketplace that incentivizes developers/businesses to join the ecosystem and share/consume IoT services; and (iii) it integrates security functionalities at the IoT gateway level. The practicability of our ecosystem has been validated through several smart city proofs-of-concept, set up in three distinct cities: Helsinki, Lyon and Brussels. In addition, the bIoTope ecosystem is evaluated by considering Prosperity-related metrics of the CITYKeys framework. It should also be noted that this paper is more engineering- and practical-oriented than theoretical but still could be of value to many entry-level readers on the subject with its literature review, and could serve as benchmark for comparison with future smart city frameworks.

Section II elaborates on the above-initiated discussion of the remaining challenges in the literature. This allows us to analyze and discuss in Section III the extent to which state-of-the-art smart city initiatives meet key ICT infrastructural and architectural requirements. To meet these requirements, an open IoT ecosystem, developed as part of the bIoTope project, is introduced in Section IV. The practicability and replicability of the bIoTope ecosystem have been showcased in Section V by demonstrating several smart city pilots set up in three distinct cities. The bIotope project impact and achievements based on several KPIs are presented in Section VI, followed by conclusions in Section VII.

II. BUILDING BLOCKS FOR EFFICIENT SERVICE INTEGRATION, DISCOVERY AND COMPOSITION

IoT systems are challenged by unsolved issues related to sustainable energy systems [12], reliable communication [13],

[1] A "digital avatar", sometimes considered as "digital shadow", refers to a virtual counterpart [11] of a physical object, which implies mechanisms for synchronizing both views (virtual and physical).

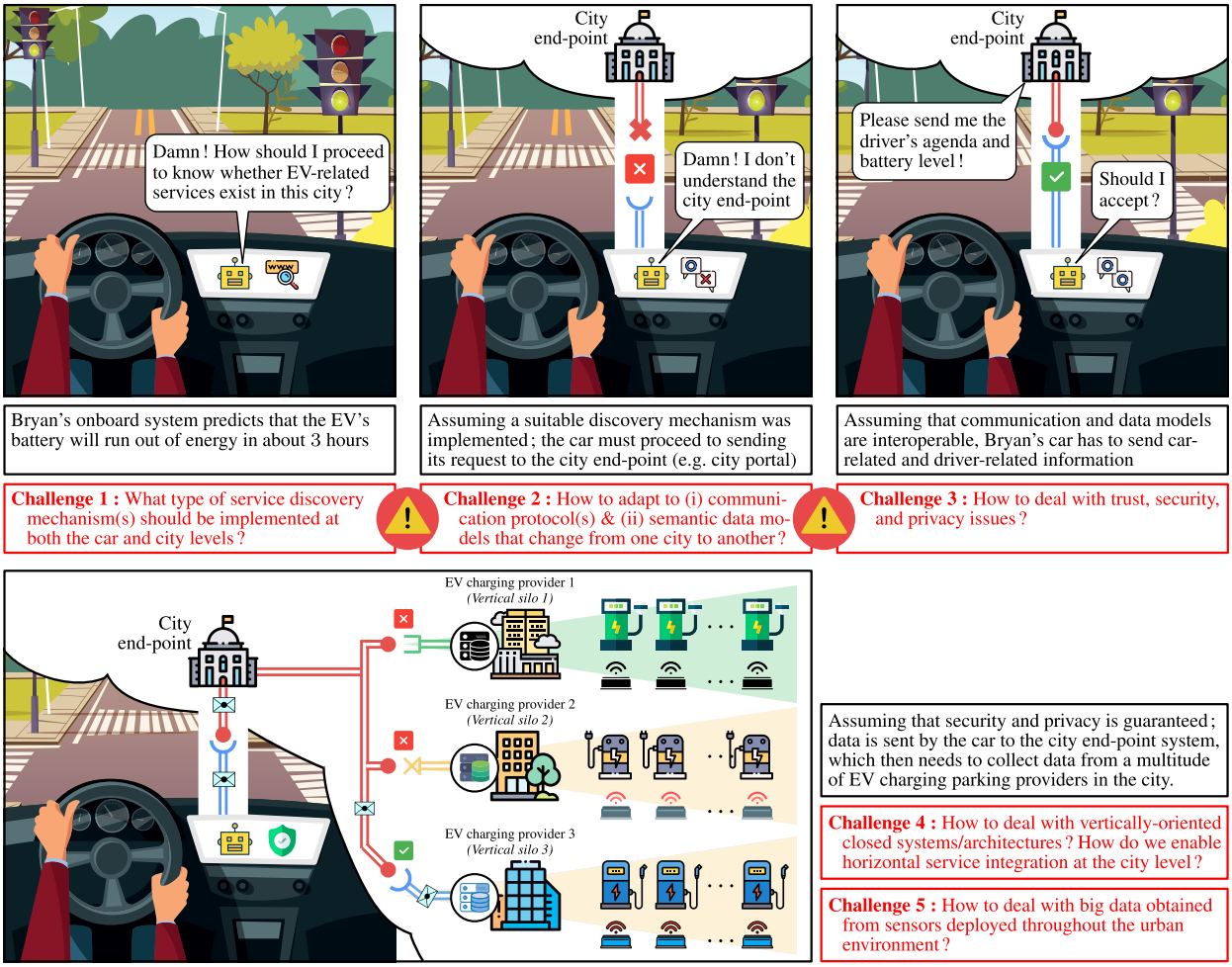


FIGURE 2. **Current situation: Achieving efficient smart city service integration, discovery and composition is far from being an easy task, which stresses five major challenges in smart cities.**

and security and cybersecurity [14], [15]. In this regard, cities currently face a number of barriers to configure the right ICT infrastructure for efficient service integration, discovery and composition. In a comic-style drawing in FIGURE 2, we depict the current state of affairs that features five major challenges for smart cities:

1) Implementing appropriate service discovery mechanism(s) at the car and city levels;
2) Implementing interoperable services by using standardized communication protocols and semantic data models;
3) Implementing appropriate trust, security and privacy mechanism(s) between the interacting systems;
4) Achieving horizontal interoperability between vendor lock-in and vertically-oriented closed systems;
5) Managing data lakes generated by sensors and smart city web applications.

While looking at existing smart city surveys, most of them focus only on one challenge or the other but rarely on the five challenges altogether, as depicted in TABLE 1. In fact, they seldom discuss technical details of smart city solution developments. As a result, in the following, we propose to review state-of-the-art technologies, protocols and standards that potentially address the above-mentioned challenges. Sections II-A and II-B, respectively, focus on communication protocols and data models designed for IoT (w.r.t. Challenge 2). Section II-C discusses current discovery mechanisms (w.r.t. Challenge 1). Section II-D investigates

TABLE 1. **Comparison of existing smart city surveys based on five Challenges: C1 refers to the service discovery challenge, C2 & C4 to the Interoperability challenge, C3 to the Security challenge, and C5 to the Big Data challange.**

Ref.	C1	C2 & C4	C3	C5	Focus
[16]				✓	Data fusion in smart cities
[1]			✓	✓	Smart city definitions
[15]		✓	✓		Cyber-security and policy
[17]				✓	Data monitoring and analytic
[18]	✓	✓			IoT and Cloud of Things
[19]	✓		✓	✓	Fog computing and applications
[20]		✓	✓	✓	Data management techniques

security and privacy-preserving solutions commonly adopted today (w.r.t. Challenge 3). Section II-E analyzes the types of integration models that shape existing smart city frameworks (w.r.t. Challenge 4). Sections II-F and II-G, respectively, examine the types of data sources that need to be tackled in urban environments, along with the data management solutions (w.r.t. Challenge 5). Based on all the state-of-the-art solutions discussed, existing smart city programs are reviewed to analyze the extent to which they address (or do not) the five aforementioned challenges.

A. (APPLICATION-LEVEL) COMMUNICATION PROTOCOLS

Secure and reliable communication is key to next generation sustainable and diversified networks in smart cities [21]. In the IoT, communication between connected systems can be divided into four models according to the RFC 7452 [22]: D2D (Device-to-Device), D2G (Device-to-Gateway), D2C (Device-to-Cloud) and BDS (Backend Data Sharing). Within this context, two main communication patterns govern these models[2]:

- *(a) Publish/Subscribe (Pub/Sub):* asynchronous, point-to-multipoint and loosely coupled messaging model allowing messages to be broadcast to systems having subscribed to a given ''topic''. The most common Pub/Sub protocols are MQTT (Message Queuing Telemetry Transport) [23], AMQP (Advanced Message Queuing Protocol) [24] and WAMP (Web Application Messaging Protocol) [25].
- *(b) Client/Server:* synchronous, point-to-point and tightly coupled messaging model allowing clients to request a data or service item from an identified server [26]. The most widely-adopted client/server protocols are HTTP [27], XMPP [28], SOAP [29] or CoAP [30].

Some communication protocols have been designed in order to support both communication patterns, as they appear to be appropriate alternatives to BDS communications. CoAP protocol has also been used for mobility management in smart cities [31]. Other protocols would include OneM2M [32], OPC-UA [33], O-MI (Open Messaging Interface) [34], [35], or even CoAP extensions, such as the Observing Resources in the CoAP [36] or the Pub/Sub Broker for the CoAP (draft-ietf-core-coap-pubsub-09).

B. DATA MODEL

Making Things accessible through a single universal application protocol does not ensure that applications can really *understand* what Things are about (i.e., the meaning and description of data and services they offer). This is where data models are relevant, defining the format, structure and semantics of a given data or service. Therefore, it is essential to ensure the interoperability of data models in the IoT to foster automatic search, indexing and integration of IoT data/services [56], [57].

[2]The numbering system (a), (b), (c), *etc.* is introduced in Sections II-A to II-G for use in Section III (when analyzing state-of-the-art smart city frameworks).

In the IoT, research on interoperability mostly examines *(c) Syntactic* interpretation, which includes data interchange and language-independent formats, such as O-DF (Open Data Format) [58], JSON(-LD), XML or RDF; and the *(d) Semantic* level, which includes investigations of ontology- and vocabulary-based approaches (e.g., SSN, schema.org, SensorML). A recent survey [59] summarizes ongoing research and challenges for the future.

C. DEVICE AND SERVICE DISCOVERY

Discovery mechanisms in IoT cover naming and addressing schemes, which help in identifying and/or locating available devices, understanding what they offer (or consume) as services and how to access them [60], [61]. In complex, heterogeneous and constantly changing environments, such as smart cities, it is crucial to implement efficient discovery mechanisms. Although the line between device and service discovery is very thin in the literature, mechanisms can be defined accordingly [61], [62]:

- *(e) Device discovery:* allows a machine (or user) to retrieve a list of IoT devices available in the residing network;
- *(f) (Web) Service discovery:* allows a machine (or user) to retrieve and understand services provided by the previously identified IoT devices or other systems.

TABLE 2 summarizes protocols, standards and technologies within the scope of each category, and being commonly used as part of smart city initiatives. Some technologies covering both device and web service discovery can also be referenced, such as IoTBnB (IoT service puBlication and Billing) [56], [63], AllJoyn [40] and DPWS (Devices Profile for Web Services) [64].

D. SECURITY AND PRIVACY

Security and privacy are key concerns for IoT applications, still posing some enormous challenges. These concerns arise in smart city development programs, since smart city applications not only collect a wide range of privacy-sensitive information from users but also control city facilities and influence people's lives [65]. Based on the taxonomies introduced in [66]–[68], TABLE 3 summarizes the key dimensions that systems should fulfil to meet both *(g) Security* and *(h) Privacy* requirements in IoT.

In smart city solution developments, the most common web security protocols for authentication and authorization are OAuth 2.0 [69], OpenID Connect [70], SAML (Security Assertion Markup Language) [71] and LDAP (Lightweight Directory Access Protocol) [72]. Furthermore, JWT (JSON Web Token) standard is also used for securely transmitting information and representing claims between two parties [73]. For data integrity and confidentiality, cryptographic approaches are mainly adopted to handle secure communication in the presence of third parties, in which HMAC [74] is the notable hash-based authentication code.

TABLE 2. Protocols, standards and technologies for device/service naming and discovery.

	Protocols/Techno.	Description
(e) Device discovery	mDNS	Multicast DNS (mDNS) protocol is used to discover devices or IoT nodes on the network [37]. This protocol is usually used in conjunction with DNS-Service Discovery (DNS-SD) to browse the network [38].
	UPnP	Universal Plug and Play (UPnP) [39] is a set of protocols, presented by Open Connectivity Foundation (OCF). It uses Simple Service Discovery Protocol (SSDP) for discovery mechanisms [40].
	IoTivity	An open-source framework for constraint IoT devices (i.e., device-to-device applications). IoTivity messaging is based on resource-based RESTful architecture model [41] and uses the CoAP service discovery feature.
	Multicast CoAP	This discovery mechanism is an extension to CoAP, with the introduction of a centralized server searchable by CoAP clients [38].
	Bonjour	Protocol implemented by Apple combining mDNS with DNS-SD, leveraging existing Internet protocols.
	DLNA	Digital Living Network Alliance (DLNA) relies on UPnP for sharing digital media over a network [42].
(f) Service discovery	UDDI	A Universal Description, Discovery, and Integration (UDDI) service registry is a syntactic text-based web service discovery mechanism (XML-based) [43]. UDDI uses WSDL (Web Services Description Language) to describe programmatic interfaces, and SAWSDL (Semantic Annotations for WSDL) for semantic annotations.
	OWL-S	Semantic-based web services ontology in the framework of the Web Ontology Language (OWL). It facilitates users and software agents to discover, invoke, compose, and monitor web services [44].
	WSMO	Web Service Modeling Ontology (WSMO) is a semantic-based web service discovery framework using a specified language called WSML for describing formal syntax and semantics [45].
	OGC OWS	The Open Geospatial Consortium (OGC) proposes an Open Web Services (OWS) standard for service discovery and bindings, which defines a software component called integrated clients [46].
	OGC CSW	OGC Catalogue Service for the Web (CSW) standard defines common interfaces to discover, browse, and query relevant scientific data and services from heterogeneous repositories [47].
	Apache River	Apache River, originally "Jini", is a network architecture in the form of modular co-operating services [48]. In the discovery process, clients uses the lookup service to search for specific services based on type, name, description, *etc.*
	OWL/RDF search engine	Several semantic-based search engines have been proposed in the literature [49]–[51], the two most common engines being: (i) *SPARQL* [52] and (ii) *SWSE* [53], both manipulating RDF data.
	WSDL-based search engine	A number of search engines compliant with WSDL and UDDI registries have been introduced [51], [54], the two most common being: (i) *Woogle* [54] and (ii) *seekda* [55] (Heritrix Web Crawler is used for annotating web pages).

TABLE 3. Security and privacy mechanism taxonomy for fulfilling IoT requirements.

	Mechanisms		Description
(g) Security	AC	Access Control	Combines identification, authentication, and authorization.
	DC	Data Confidentiality	Protect data (stored/processed) from unauthorized access.
	DI	Data Integrity	Ensure data accuracy and completeness curing communications.
	AA	Availability	Ensure Thing-related data and services are available at all times and to authorized parties.
	NR	Non-Repudiation	Refer to a situation where both sender and receiver nodes cannot deny the action.
(h) Privacy	IC	Information Collection	Addresses how and what information is collected.
	IProc	Information Processing	Deal with the causes of harmful activities (result of searching and accessing data).
	IDis	Information Dissemination	Deal with information releasing of personal information to third party systems.
	DE	Data Encryption	Conversion of data into encrypted code that can be securely shared with authorized entities.
	DA	Data Anonymity	Process in which private or sensitive data is being protected by erasing/encrypting identifiers.

E. TYPE OF INTEGRATION

A key problem at the Application layer of the OSI model is that no *lingua franca* unites all the objects but rather they speak literally hundreds of languages [75]. At the time of writing this paper, many initiatives pursued by distinct standardization fora are currently underway, which inevitably slow down the convergence and adoption of a *de facto* application protocol for IoT [35], [59], [76]. Amongst these initiatives, two schools of thought dominate: (i) the creation of new protocols that bypass traditional web protocols such as HTTP (e.g., MQTT, CoAP); (ii) the reuse and leveraging of widely popular Web protocols such as HTTP (e.g., OneM2M, O-MI, Webhook). These two schools of thought address different requirements at the application layer; while the former specify D2D, D2G and D2C communications, the latter are more suited to BDS communications. This situation, unfortunately, leads to the emergence of two integration models [77], [78]:

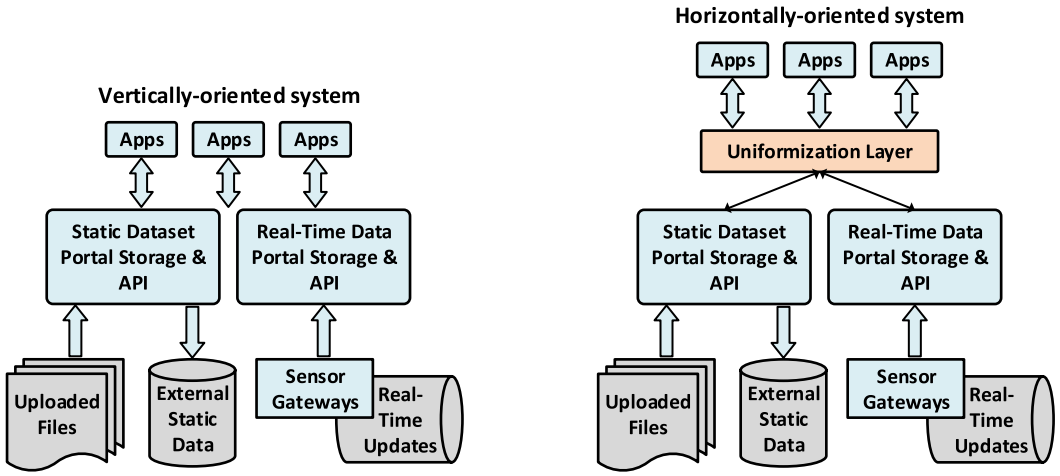
(i) Vertical integration: IoT platforms form no collaborative IoT ecosystem but rather vertical silos (data being siloed in a unique system and staying there [79]). This model poses interoperability and openness issues, as depicted in FIGURE 3(i);

(j) Horizontal integration: It offers a way to break down existing vertical silos, therefore enabling cross-platform and cross-domain IoT applications and services [80]. Horizontally-oriented platforms, also referred to as innovation ecosystems, require a uniformization layer that provides unified interfaces based on open communication standards, as described in FIGURE 3(j).

A smart city is one of the most striking examples of vertically-oriented closed systems, as it consists of a wide range of stakeholders and IT technologies. This results in vertical silos due to the use of different communication protocols and business models. Hence, the integration phase becomes very tedious and time consuming in smart city development programs [81].

F. OPEN DATA AND SERVICE STREAMS

Providing open data and service streams in smart city applications are essential [82], [83]. However, it is important to differentiate between *Open Data* and *Open ecosystem*. The former refers to the publication of governmental- and city-related datasets, while the latter refers to the



(i) Vertical integration

(j) Horizontal integration

FIGURE 3. Type of integration for smart city ecosystem.

consideration of open and standardized communication interfaces to allow real-time data exchanges across platforms and systems. In the majority of cases, and as emphasized in FIGURE 3, open data platforms, such as CKAN, Socrata and Opendatasoft, make *(k) static urban datasets* available (e.g., list of parking spaces/places in the city), while open IoT ecosystems, such as the ones developed as part of the IoT-EPI initiative[3] (bIoTope, Big-IoT, Agile, Inter-IoT...), relate more to *(l) real-time urban data streams*, such as sensor/actuator data and REST-based web services [84].

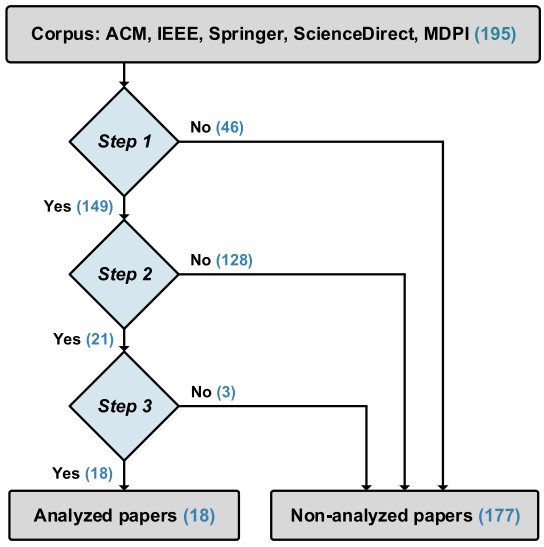
G. DATA MANAGEMENT

Due to the exponential growth of IoT devices and sensors, the volume of real-time urban data is exponentially growing. Large collections of data are sometimes referred to as data lakes in the big data era. Given the large variety of data sources in smart cities, two types of storage systems are typically considered depending on the application needs and constraints, namely: *(m) SQL storage systems* and *(n) NoSQL storage systems*. Unlike RDBMS, NoSQL technologies (e.g., MongoDB, Apache Cassandra, HBase) can support document-based, key-value store or graph-based data storage [85].

III. CURRENT STATE OF AFFAIRS OF SMART CITY FRAMEWORKS

All the mechanisms, protocols and technologies introduced in Sections II-A to II-G are summarized in the form of a taxonomy in TABLE 4. Based on this taxonomy, smart city-related papers have been selected and reviewed to analyze the extent to which they support taxonomy-related mechanisms, which are essential for addressing the challenges discussed in FIGURE 2. We targeted five main library databases for collecting smart city-related papers: ScienceDirect, ACM, IEEE Xplore, Springer and MDPI. Sources such as doctoral dissertations, master's theses, textbooks, conference proceedings and unpublished papers were ignored. In total, 195 scientific papers were collected. In order to exclude papers irrelevant to our study, a three-step methodology was defined and applied, as summarized in FIGURE 4. As a result, 18 selected articles were analyzed and compared with the proposed IoT ecosystem in TABLE 5 based on the criteria taxonomy introduced in TABLE 4.

[3][Online]. http://iot-epi.eu, last accessed June, 2020



Step 1: *papers published after year 2009*
Step 2: *papers dealing with the OSI Application layer protocols*
Step 3: *papers addressing more than 50% of the 14 taxonomy criteria (cf., (a) to (n) in Table 3)*

FIGURE 4. Smart city literature review methodology.

A. APPLICATION-LEVEL COMMUNICATION PROTOCOLS

It can be observed that all smart city frameworks support the Client/Server communication pattern, using REST API based

TABLE 4. Criteria taxonomy for systematic literature review.

Taxonomy *(numbering used in Table 5)*			**Frameworks**
Application-level comm. protocols	(a)	Pub/Sub	MQTT, AMQP, ...
	(b)	Client/Server	HTTP/HTTPs, SOAP, XMPP, ...
		Both	CoAP, O-MI/O-DF, oneM2M, OPC-UA
Data model	(c)	Syntactic	XML/RDF, JSON, HTML, gbXML, IFC, Turtle
	(d)	Semantic	SSN, SAREF, DUL, OGC SensorML & ContextML, schema.org, DateTime, WGS8pos, Km4City, Apache Jena, SAO, PROV, CES, OM, MORElab City4Age
Discovery capability	(e)	Device	mDNS, DNS-SD, UPnP, IoTivity, Multicast CoAP, Snoogle, Bonjour, DLNA
	(f)	Web Serv.	UDDI, OWL-S, WSMO, OGC OWS & CSW, Apache River, SPARQL, SWSE, Woogle, seekda
		Both	AllJoyn, DPWS, IoTBnB
Security & privacy	(g)	Security	Access Control (AC) - Identification (Iden), authentication (AuthN), authorization (AuthZ) -, Data Confidentiality (DC), Data Integrity (DI), Availability (AA), Non-repudiation (NR)
	(h)	Privacy	Information Collection (IC), Information Processing (IProc),Information Dissemination (IDis), Data Encryption (DE), Data Anonymity (DA)
Type of integration	(i)	Vertical	Vertically-oriented closed system
	(j)	Horizontal	Horizontally-oriented system
Open data & service streams	(k)	Static	Static urban data through CKAN, SOCRATA, OpenDataSoft, or FTP
	(l)	Real-time	Near/Soft real-time urban data streams through MQTT, WebSocket, etc.
Data management	(m)	SQL	H2, MySQL, MS SQL, PostgreSQL, NuoDB, Oracle, Google Spanner, ClustrixDB, Sedna
	(n)	NoSQL	MongoDB, Apache Cassandra, SimpleDB, DynamoDB, CouchDB, HBase, Redis, Warp10

on HTTP requests for the majority of the reviewed papers (14 out of the 18). Regarding the support of Pub/Sub communications, 11 of the papers (i.e., 60%) integrate such mechanisms with MQTT being the most widespread protocol.

B. DEVICE AND SERVICE DISCOVERY

7 articles (i.e., 39%) support device discovery mechanisms, which is significantly less than the number of papers supporting web service discovery (67% - 12 papers). Among these 12 papers, half rely on the OWL framework. It should nonetheless be noted that OWL-based search engines, such as SPARQL, still have limitations to be addressed. Among others, SPARQL endpoints have the disadvantage of being complex and thus less efficient than other query languages [106]. This is the main reason why semantic Web standards are not (and not likely to be) largely adopted by Web developers, as compared to RESTful APIs [107], [108].

C. DATA MODEL

Three main data formats are commonly used at the syntactic level namely XML, JSON and RDF. XML or JSON are adopted in 9 articles, while the remaining 9 papers consider RDF format. On the other hand, 13 out of the 18 papers (72%) deal with ontology- and vocabulary-based semantics. It can be observed that SSN and SensorML are the commonly applied vocabularies, which are being considered in 17% of the reviewed articles.

D. SECURITY AND PRIVACY

Most of the papers (12 out of the 18) integrate security and/or privacy mechanisms, the other 6 ignoring the topics. The security features implemented in smart city programs mainly cover AC, DC and DI for security purposes, and DE for privacy. This reveals that the existing smart city frameworks mostly cover 3 out of the 5 security dimensions listed in TABLE 3, and only 1 out of the 5 privacy dimensions. Although this finding should be put into perspective given the methodology applied in our study for selecting papers (*cf.*, FIGURE 4), this finding/trend in the context of smart city is pointed out in various studies such as [24], [87], [88], [98], [102]–[104].

E. TYPE OF INTEGRATION

The reviewed papers confirm the trend that most of the existing smart city applications are vertically integrated within separate silos without horizontal communications. As seen in Table 5, 83% of the smart city frameworks are designed in a vertical integration manner, whereas only 2 papers out of the 18 propose a horizontally-oriented strategy.

F. OPEN DATA AND SERVICE STREAMS

Most of the smart city frameworks (14 out of the 18 papers) deal with real-time urban data streams, while static urban data are mentioned (using CKAN) in only 4 papers. Again, this finding should be put into the perspective of this study, which does not directly address open data portal-related aspects but rather smart city infrastructures that are commonly used for real-time sensor data streams. However, this confirms that in most cases smart city-related papers typically address either open data-related research or IoT application-related research, which does not help move towards horizontal integration.

G. DATA MANAGEMENT

Data storage is equally performed with either SQL or NoSQL databases in the reviewed papers. This choice is not objectionable; however, one may wonder whether the proposed studies provide a possibility to add, wherever and whenever needed, a new storage system that can be seamlessly integrated to the smart city environment? When looking at the reviewed papers, only 3 papers out of the 18 (17%) provide or at least discuss such possibilities. All the other papers describe

TABLE 5. Classification of the scientific articles reviewed. ✓ means supported, ✗ means not supported, 'n/s' means not specified, and 'n/a' means not applicable.

Ref.	Year	Application-level comm. prot.		Discovery capability		Data model		Security & Privacy		Type of Integration		Open data & streams		Data management	
		a) Pub/Sub	b) Cli/Ser	e) Device	f) Web Ser.	c) Syntactic	d) Semantic	g) Secu.	h) Privacy	i) Vertical	j) Horiz.	k) Static	l) Real-t.	m) SQL	n) NoSQL
[86]	2017	✓(n/s)	✓(n/s)	✗	OWL/RDF search engine	XML/RDFs	SAREF, DUL, SSN	✓(n/s)	IC, IProc, IDis	✓	✗	✗	✓	✗	✓(n/s)
[87]	2014	✗	HTTP	✗	UDDI, OGC OWS, CSW	XML/RDF	OGC SensorML, ContextML	AC, DC, DI	IC, IProc, DE	✓	✗	CKAN	✓	MS SQL, PostgreSQL ...	MongoDB, SimpleDB, DynamoDB ...
[88]	2015	✗	SOAP	✗	UDDI	XML	✗	DC, DI, NR	DE, DA	✓	✗	✗	✓	Google Spanner, NuoDB, ClustrixDB	✗
[24]	2018	MQTT, AMQP	CoAP, XMPP	✗	✗	XML stanza	✗	AC, DC, DI	DE	✓	✗	✗	✓	n/a	n/a
[89]	2019	WAMP	HTTP	AllJoyn [90]	AllJoyn	JSON, XML	SSN, DateTime, WGS8pos	AuthN, DI	DE	✗	✓	CKAN	✗	✗	MongoDB
[91]	2017	✗	HTTP (Km4City API)	✗	OWL-S, OWL/RDF (SPARQL)	XML/RDF	Km4City LD [92]	✗	✗	✓	✗	✗	✓	✗	HBase, MongoDB
[93]	2012	✓(n/s)	HTTP, XMPP	✗	✓(n/s)	XML	OGC SensorML	✓(n/a)	DE	✓	✗	✗	✓	Oracle, Sedna PostgreSQL	Apache Cassandra
[94]	2019	AMQP	HTTP	✗	✓(n/s)	XML	✗	✗	✗	✓	✗	✗	✓	PostgreSQL	MongoDB, Redis
[95]	2018	MQTT	SOAP	Snoogle [96]	UDDI	XML	✗	✗	✗	✓	✗	✗	✓	✗	Apache Cassandra
[97]	2017	MQTT	HTTP	✓(n/s)	OWL-S	XML/RDF, JSON, gbXML, IFC	SenML, Apache Jena	✗	✗	✓	✗	✗	✓	✓(n/s)	✗
[98]	2014	✗	HTTP	✗	OWL-S, OWL/RDF (SPARQL)	XML/RDF, Turtle	SAO, PROV, CES, SSN	AC, DC, DI	DE	✓	✗	CKAN	✓	✗	✗
[99], [100]	2019	MQTT	HTTP	AllJoyn	OWL/RDF (SPARQL)	XML/RDF, Turtle	oneM2M Base, Fiesta-iot, OWL	✗	✗	✓	✗	✗	✓	✗	✓(n/s)
[101]	2019	✓(n/s)	SOAP, HTTP	✗	✗	JSON, XML	OM, PROV	AuthN	✗	✗	✓	✗	✓	n/a	n/a
[102], [103]	2018	✗	HTTP	✗	✗	RDF, JSON	MORElab City4Age, schema.org	AC, DC, DI, AA	DE	✓	✗	CKAN	✗	PostgreSQL	✗
[104]	2019	✗	HTTP, SOAP	UPnP	✗	XML	✗	AC, DC, DI, AA	IC, IProc, IDis, DE	✗	✗	✗	✓	n/a	n/a
[105]	2013	✓(n/s)	HTTP	✓(n/s)	✗	JSON, XML	OGC SensorML	✓(n/s)	✗	✓	✗	✗	✓	MySQL	✗
Proposed (bIoTope project)	2016 – 2019	O-MI	O-MI	IoTBnB	IoTBnB	O-DF	schema.org, MobiVoc ...	AC, DC, DI	IC, IProc, IDis, DE	✗	✓	✓	✓	✓	✓

smart city architectures that are application-driven and not appropriate for efficient service integration, discovery and composition.

H. TOWARDS OPEN IoT ECOSYSTEMS

As revealed in TABLE 5, existing smart city frameworks are often designed on a mixture of proprietary technologies, platforms and protocols that hamper the efficient integration of such platforms. This poses various functional integration problems including: (i) the lack of standardized protocols at the communication and technical, syntactic as well as semantic levels; and (ii) the lack of open service discovery (and publication) platforms/catalogs to ease and incentivized the search and composition of IoT data sources and services. The lack of standardized protocol adoption might be the biggest problem today, as also stated by Espinha *et al.* [109] that ''IoT integrator companies estimate that support for every new service API requires a few days to months of software development effort, not to mention the effort to maintain these APIs''. More concretely, the cost/effort for interconnecting n distinct platforms (with n distinct proprietary APIs) would result in developing $\frac{n\times(n-1)}{2}$ wrappers that follow a quadratic function. While adopting an open IoT ecosystem approach such as bIoTope, which consists of a common standardized communication layer, the cost would result in the development of n wrappers, thus following a linear function. As an example, a single business has to develop $(n-1)$ wrappers if standardized APIs are not considered, while it only develop 1 wrapper when joining an open ecosystem. These cost/effort functions for integrating platform APIs with a traditional approach vs. bIoTope approach are further discussed and illustrated in Appendix B (and associated FIGURE 14).

To address these two major problems, the European Initiative for IoT platforms (IoT-EPI)[4] was formed under the EU's H2020 research and innovation programme. The aim was to investigate and build a vibrant and sustainable IoT ecosystem in Europe in order to maximise the opportunities for platform development, interoperability and information sharing. As part of this initiative, seven projects funded under the same program investigated different aspects of such open innovation ecosystems, with a particular focus on smart city pilots. In Section IV, the key building blocks of one of the seven projects, called bIoTope (Building an IoT Open Ecosystem for Connected Smart Objects), are introduced. These building blocks aim at fulfilling, to the best possible and synergistic extent, the seven dimensions introduced in the taxonomy in TABLE 4. The proposed ecosystem relies on numerous open standards for communication and data, where the ones published by the Open Group form the common denominator that allows integration over application domains, protocol stack levels, and between vertical silos. In contrast to bIoTope, the functional integration in most of the business-driven API systems is based on proprietary APIs, especially from a syntactic and semantic viewpoints. Further, open service discovery (and publication) platforms are often missing, or are limited to a specific domain (e.g., mobility, energy). It should be noted that our proposed ecosystem does not expect businesses to drop their commercially-driven APIs, but rather, if they are willing to join and benefit from our ecosystem, they just need to develop a wrapper (using O-MI/O-DF).

[4][Online]. http://iot-epi.eu, last accessed June, 2020

IV. bIoTope ECOSYSTEM

One of the main contributions of this paper is the development of an open IoT ecosystem that allows for the integration of a wide range of IT platforms/systems, web services and other functional APIs. This integration to the ecosystem is: (i) based on open and complementary IoT standards (O-MI and O-DF standards in this research); (ii) simplified by including a service publication and discovery platform, referred to a IoTBnB marketplace, along with incentives for developers/businesses to join and make use of that platform. Such complementary building blocks differ from state-of-the-art frameworks, as they are often based on a mixture of non-complementary (or non-standardized) technologies, frameworks and protocols.

An overview of the bIoTope ecosystem is provided in FIGURE 5, including the seven functional building blocks (center of the figure), along with potential ecosystem stakeholders and external IoT systems (e.g., smart connected objects). As will be discussed in this section, and particularly in Sections IV-A and IV-B, horizontal integration of external/new IoT systems and platforms in the bIoTope ecosystem is achieved using standardized communication interfaces and data models, which necessitates the development of external software agents called ''wrapper agents'' in FIGURE 5. Sections IV-A to IV-F present the architectural design choices underlying each of the seven functional building blocks of the bIoTope ecosystem. Section IV-G discusses the incentives that motivate businesses to join the open IoT ecosystem.

A. (APPLICATION-LEVEL) COMMUNICATION PROTOCOL

In bIoTope, O-MI is adopted as the application communication protocol, which provides standardized communication interfaces fulfilling both Client/Server and Pub/Sub models. TABLE 6 lists the six interfaces (operations) provided by O-MI, which are required to support both models, as well as the CRUD (Create, Read, Update, Delete) model, which is the key in any given IoT application, as discussed in earlier research papers [35], [110], [111]. One of the fundamental properties of O-MI is that it is ''protocol agnostic'', meaning that it can be implemented over HTTP, WebSocket, SOAP, TCP-IP or similar protocols.

An open-source reference implementation for O-MI standard has been released,[5] which consists of three core components: (i) *API endpoint:* It manages user requests, and currently supports both HTTP and WebSocket protocols;

[5]O-MI reference implementation by Aalto University. https://github.com/AaltoAsia/O-MI, last accessed June, 2020

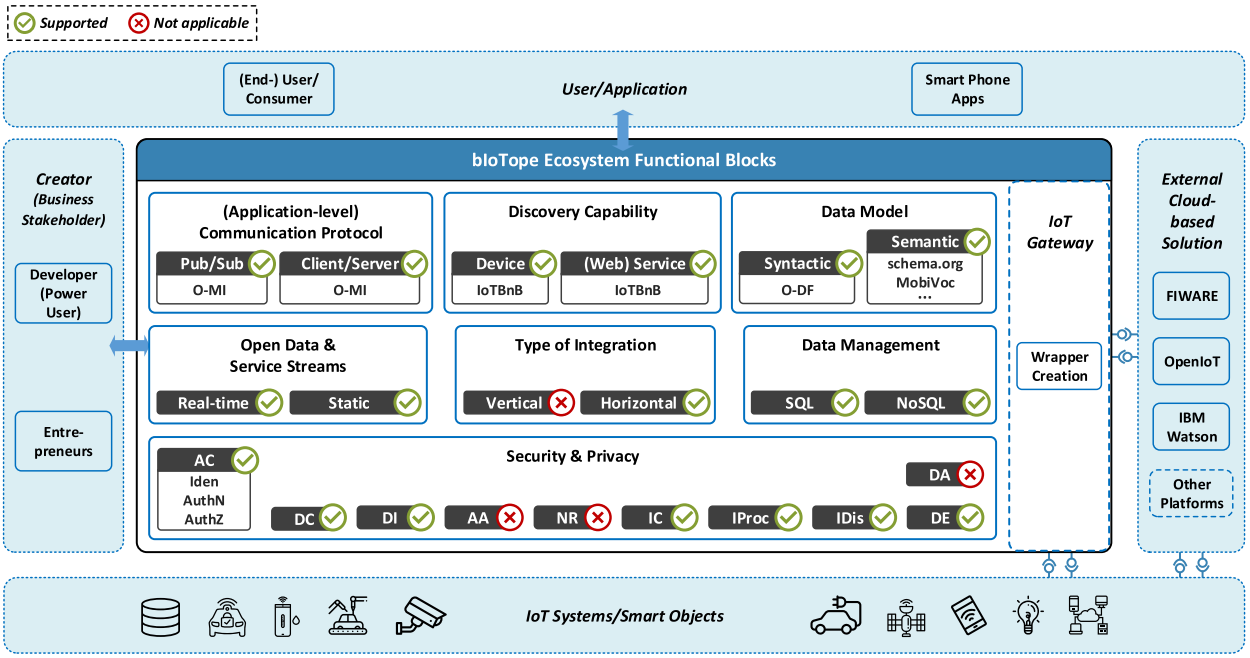


FIGURE 5. bIoTope reference architecture containing seven functional building blocks; where *O-MI* is Open Messaging Interface, *O-DF* is Open Data Format, *AC* is Access Control, *Iden* is Identification, *AuthN* is Authentication, *AuthZ* is Authorization, *DC* is Data Confidentiality, *DI* is Data Integrity, *AA* is Availability, *NR* is Non-repudiation, *IC* is Information Collection, *IProc* is Information Processing, *IDis* is Information Dissemination, *DE* is Data Encryption, and *DA* is Data Anonymity.

TABLE 6. O-MI communication interfaces (supported operations).

Operation	Description
1- Write	Used to write information updates from sensors, events, or other devices to O-MI nodes.
2- One-Time Read	Used to retrieve immediate or old information from the O-MI nodes.
3- Read (Subscription)	A specific read operation for retrieving information at regular intervals. Two types of subscription can be performed: • *Subscription with callback address:* The requested data are sent to the callback address with a specified interval (interval-based and event-based are supported). • *Subscription without callback address:* The data are stored on the subscribed node until the subscription is valid. The data can then be retrieved (polled) by issuing a new read request.
4- Method Call	Used to call functional parts of O-DF structures with given parameters.
5- Cancel	Used to cancel subscription before it expires.
6- Delete	Used to delete parts of O-DF hierarchy.

(ii) *Agent system:* It contains multiple software agents, which are integrated with the API endpoint to pull/push data (e.g., sensor data values) from and to the internal database; and (iii) *User/Web interface:* This service is used for executing O-MI operations, listed in Table 6. Furthermore, FIGURE 6 provides an example of the O-MI message which uses the method call operation (see line 2) for *discovery* request. The requested services are described along with the payload format discussed in Section IV-B, which uses a standard complementary to O-MI named O-DF (Open Data Format) [58], as highlighted in FIGURE 6. Note that just as the HTTP can embed other format than HTML, O-MI is designed to be independent of O-DF and can embed any other formats.

B. DATA MODEL

The syntactical data model in bIoTope is based on the O-DF standard specified using XML and defined as a generic ontology to represent any IoT object. It is intentionally presented in an analogous way as data structures in object-oriented programming. The hierarchical tree structure is organized as follows (refer to FIGURE 6 for a more detailed understanding of the following explanation): it starts with an `Objects` element as its top element, which can contain any number of `Object` sub-elements. The `Object` elements can have any number of properties, referred to as `InfoItems`, as well as `Object` sub-elements. The resulting `Object` tree can contain any number of levels. Every `Object` has a compulsory sub-element called `id` that identifies the `Object`, which should preferably be unique for a specific application or residing network.

Looking further at the O-MI/O-DF message given in FIGURE 6, it shows a discovery request (as previously discussed) to an IoT (O-MI) endpoint for the surrounding EV charging station addresses by passing, as input parameters, the car's geo-coordinate (lines 21 and 24), maximal distance (line 13), and a plug type (line 16). From a semantic

```
1  <omiEnvelope xmlns="http://www.opengroup.org/xsd/omi/1.0/" version="1.0" ttl="30">
2    <call msgformat="odf">
3      <msg>
4        <Objects xmlns="http://www.opengroup.org/xsd/odf/1.0/"
5                 prefix="schema: http://www.schema.org/ mv: http://www.schema.mobivoc.org/">
6          <Object>
7            <id>ChargingService</id>
8            <InfoItem name="getAddress">
9              <value type="odf">
10               <Objects>
11                 <Object>
12                   <id>Parameters</id>
13                   <InfoItem type="schema:Distance" name="maxDistance" required="true">
14                     <value>100</value>
15                   </InfoItem>
16                   <InfoItem type="mv:plugType" name="plugType" required="false">
17                     <value>mv:CHAdeMO</value>
18                   </InfoItem>
19                   <Object type="schema:GeoCoordinates">
20                     <id>Coordinates</id>
21                     <InfoItem type="schema:longitude" name="longitude" required="true">
22                       <value>60.187640</value>
23                     </InfoItem>
24                     <InfoItem type="schema:latitude" name="latitude" required="true">
25                       <value>24.828300</value>
26                     </InfoItem>
27                   </Object>
28                 </Object>
29               </Objects>
30             </value>
31           </InfoItem>
32         </Object>
33       </Objects>
34     </msg>
35   </call>
36 </omiEnvelope>
```

O-MI

O-DF

O-MI

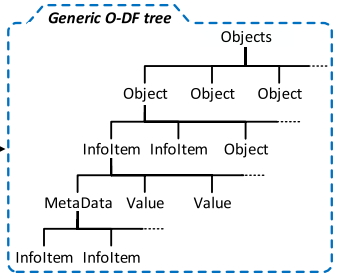


FIGURE 6. O-MI/O-DF call message requesting for surrounding EV charging stations.

viewpoint, it is crucial to support flexible and complex semantic structures. In this respect, we adopt the O-DF standard at the data format-level, which provides us with the flexibility to extent the data description (payload) with domain-dependent and/or domain-independent semantic vocabularies, such as SSN, schema.org, and MobiVoc [59], [112]. In the message given in FIGURE 6, O-DF has been enriched with schema.org tags in lines 13, 19, 21, 24 and MobiVoc[6] tag in line 16 (using ''type'' parameters). In this example, we make use of the MobiVoc vocabulary to describe parking- and electrical vehicle-related data/services, as SSN does not provide any parking- and charging-related semantics. Furthermore, it is appropriate to enrich new and more complex semantics to the O-DF payload, once developers are aware of what models and related vocabularies they want to include to the O-DF structure. Within this context, several relevant papers have been published as part of the bIoTope project [59], [112]–[114].

C. DEVICE AND SERVICE DISCOVERY

For device and service discovery, bIoTope uses both:

- *O-MI/O-DF standard capabilities:* Although not discussed in previous sections, O-MI/O-DF standards allow for calling `MetaData` of O-DF elements, which return information about what the InfoItem (i.e., data/service) is about, and what the response will consist of. An exemplary response when calling the `MetaData` of `getAddress` method is given in Appendix A. In this response, two different vocabularies are shown in line 8 (using ''prefix'' parameter) that are used to describe the same *address* object in lines 42 and 44;
- *an online digital marketplace:* The bIoTope digital marketplace is called IoTBnB[7] (IoT service puBlication and Billing). It provides (i) IoT data/service producers with the possibility to register their own O-MI node on IoTBnB to make one or more data/service items visible and accessible (either free of charge or in return for payment) to third-party developers and systems; (ii) IoT data/service consumers (i.e., third-party developers) with the possibility to search for IoT data streams or services that are relevant for their own applications/business.

From a functioning viewpoint, IoTBnB only collects the description of data/service items that the O-MI node owner decides to expose to the marketplace. In other words, only *MetaData* of O-DF elements describing what the data stream or service is about and how to call it, is collected and indexed by IoTBnB's search engine. This logic is aligned with other similar platforms such as Thingful or ThingSeek [115].

IoTBnB consists of a number of components, as detailed in FIGURE 7. The ''IoTBnB UI'' component enables IoT publishers and consumers to interact with the digital marketplace. The ''O-MI node registration'' module allows the owner of an O-MI node/endpoint to register his/her node (providing e.g. the node URL, name, or authentication parameters). Once completed, IoTBnB begins the process of collecting, indexing and storing O-DF InfoItem-related metadata of the exposed data/service items. The indexed data/service items

[6][Online]. http://schema.mobivoc.org/, last accessed Oct, 2020

[7][Online]. http://iotbnb.jeremy-robert.fr, last accessed May, 2020

TABLE 7. IoTBnB APIs to enable search & discovery of IoT data/services in the bIoTope ecosystem: http://iotbnb-api.jeremy-robert.fr.

API	Input	Output	Description
`getAllServices()`	N/A	List of services	Return all services available in the service catalog/registry.
`searchServices('input')`	keyword, type, price, reputation, coordinates	List of services	Search for existing IoT data/services depending on specific needs (e.g., location-based, price-based...)
`getServiceAccessInformation('input')`	serviceID (returned by searchServices)	InfoItem_url, OMI_node_url	Retrieve service-related access information (access key being provided when a service is not for free).

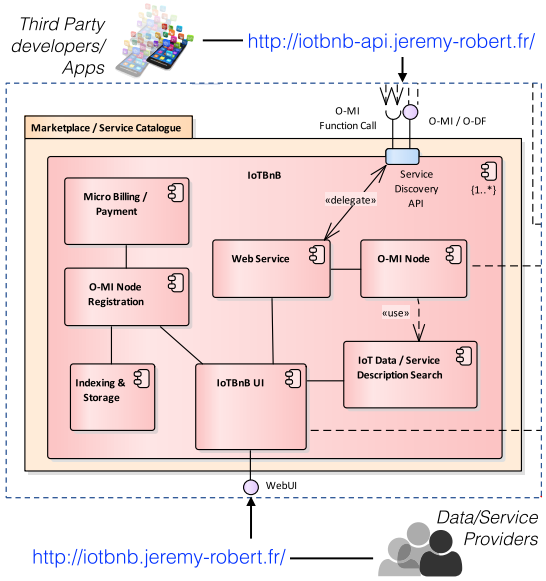


FIGURE 7. IoTBnB internal components.

are searchable using either the WebUI or API calls, as given in TABLE 7.

D. SECURITY AND PRIVACY

A security module pluggable with O-MI nodes has been designed[8] to ensure access control, data confidentiality, integrity, and data encryption. From a technical viewpoint, this module consists of two sub-modules:

- *Authentication:* accountable for handling new user registrations and managing sessions. This module currently supports three methods [116], [117]: (i) password-based authentication; (ii) OAuth 2.0-based registration using Facebook as its service provider; and (iii) LDAP-based authentication.
- *Authorization:* accountable for providing O-MI node owners with fine-grained control over the data/service items they would like to share/sell. This module further consists of two components: (i) access control to process O-MI requests to verify whether the requester is (or not) allowed to access the requested data/service items; (ii) administrator console to provide O-MI node owners with the possibility to manage access policies [118].

[8]Authentication module: https://github.com/AaltoAsia/O-MI-Authentication, Authorization module: https://github.com/AaltoAsia/O-MI-Authorization, last accessed June, 2020

A sequence diagram showing data exchanges between the authentication and authorization modules based upon client request is detailed in FIGURE 8, which result in either access permission or denial. Note that, in this sequence diagram, only the password-based authentication is depicted.

E. TYPE OF INTEGRATION AND OPEN DATA/SERVICE STREAMS

As discussed in sections IV-A, IV-B and IV-C, the adoption of open and standardized APIs such as O-MI, along with generic data models for IoT data representation such as O-DF, contributes to make the bIoTope ecosystem able to achieve horizontal integration. This provides innovative cross-platform and cross-domain IoT applications with the integration of both static datasets (e.g., from city open data portals) and real-time urban data streams (e.g., from connected smart Objects). Such cross-platform and cross-domain applications in different smart city scenarios will be presented in Section V.

F. DATA MANAGEMENT

It is important to distinguish two data storage aspects in the bIoTope ecosystem, namely data storage system(s) that are used as part of (i) the core bIoTope ecosystem functional blocks (*cf.*, FIGURE 5) and (ii) systems/platforms external to the core functional blocks. In the latter case, the number of data storage system possibilities are infinite, as long as O-MI/O-DF wrappers are developed for each considered storage system (examples will be detailed in the smart city pilots presented in Section V). Given this, we only discuss the former case in this section, i.e. data storage systems that have been considered as part of the seven functional building blocks underlying the bIoTope ecosystem. In this respect, three functional blocks have been designed by integrating data storage solutions: (i) *IoTBnB (device & service discovery):* Elasticsearch database is used for data/service description indexation; (ii) *IoT gateway:* either H2 or Warp10[9] database can be selected when setting up the O-MI node; and (iii) *O-MI security module (security & privacy):* H2 database has been used for access control storage.

G. INCENTIVES FOR BUSINESS INVOLVEMENT

To motivate businesses to join an open IoT ecosystem such as bIoTope, the incentive lies in the opportunities of engaging

[9][Online]. https://www.warp10.io/, last accessed June, 2020

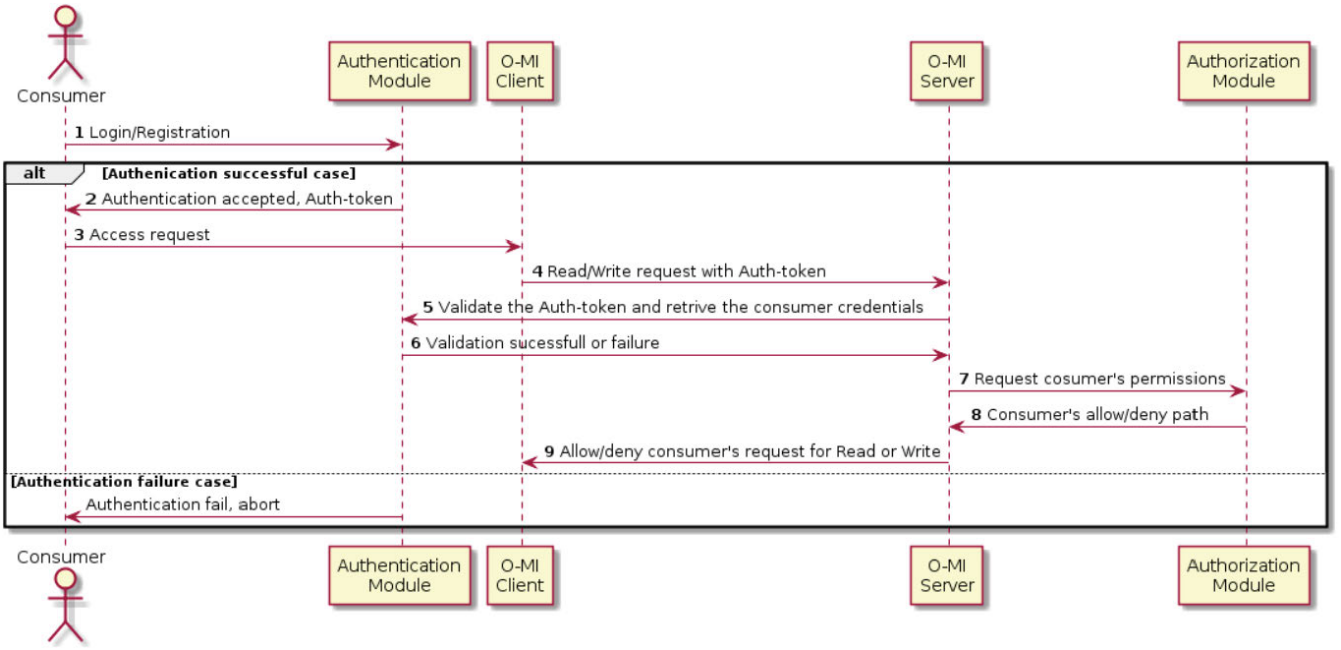


FIGURE 8. Sequence diagram for authentication and authorization module [116].

with new market segments, and this in two respects: (i) it provides businesses with the possibility to access new (semantically annotated) data sets, which could serve for developing new digital services; (ii) it provides businesses with the possibility to publish and sell their own company-related data (e.g., BMW, in the bIoTope project, considers the possible sale of car-related statistics). To connect with an open IoT ecosystem, innovative technology is the first step as it provides new ways for businesses to create customer experiences, connect with them, and understand customer behavior. It is crucial to adopt new technology as other incompatible approaches in the market can scale down the growth of the technology [119]. This leads to the following driving factors which are both economically and technically feasible measures: (i) interoperability to connect various data providers and consumers; (ii) promoting innovation and creating new possibilities for businesses; (iii) shifting towards an open and standardized platform to promote flexibility, the rapid development of new products, and numerous ways to meet individual customer needs.

Furthermore, as stated earlier in this paper, let us remind ourselves that in open innovation ecosystems such as the ones proposed in bIoTope, symbIoTe,[10] BIG-IoT,[11] INTER-IoT,[12] and other projects involved in the European Initiative for IoT platform development (IoT-EPI), businesses are not expected to drop their own APIs. If they are willing to join the ecosystem, they need to develop a wrapper based on standardized communication interfaces to be part of that ecosystem and benefit from it, as discussed in the previous sections.

V. bIoTope REAL-LIFE CASE STUDIES

In the bIoTope project, executed from year 2016 to 2019, one of the goals was to lay the foundation for open innovation ecosystems in which companies and cities can innovate by creating both new software components for the IoT ecosystem, and create new platforms for connected smart objects with minimal investment. Several smart city pilots were developed and deployed in three European cities: Helsinki, Grand Lyon and Brussels [35], [56], [78], [120], [121]. They were implemented to validate the social, technical and business facets of the proposed open IoT ecosystem.

TABLE 8 provides insight into the main Proofs-of-Concept (PoCs) developed in each city, highlighting the smart connected objects (i.e., sensors and/or platforms) and data providers that have been integrated into the bIoTope ecosystem, along with targeted business stakeholders. For conciseness purposes, only one pilot per city is detailed in this paper, namely EV charging-related PoC in Helsinki (Section V-A), smart watering-related PoC in Lyon (Section V-B), and safety of pupils-related PoC in Brussels (Section V-C). They were selected to demonstrate the feasibility of the approach in fostering greener and safer cities as collaboration between companies and cities. These distinct real-life smart city pilots in Lyon, Helsinki and Brussels also prove that the implied open IoT ecosystem is sufficiently flexible for the integration of other IoT systems. Again, for conciseness purposes, more details are presented in the first pilot (i.e., Helsinki) than the others, as the key point in presenting these PoCs is to

[10] [Online]. https://www.symbiote-h2020.eu/, last accessed Oct, 2020
[11] [Online]. http://big-iot.eu/, last accessed Oct, 2020
[12] [Online]. https://inter-iot.eu/, last accessed Oct, 2020

TABLE 8. Case study pilots overview for three European cities; Helsinki - 1 pilot, Lyon - 2 pilots, and Brussels - 3 pilots.

	Helsinki (Sec. V-A)	**Lyon** (Sec. V-B)	**Lyon**	**Brussels** (Sec. V-C)	**Brussels**	**Brussels**
Pilot (PoC)	Vendor independent EV charging station service	Smart watering that self-adapts to climate change	Enhanced bottle bank collection in the city	Safety of pupils around schools	Enhanced quality of public transportation	Vendor independent parking location service
Implementation	*Client:* App *Server:* O-MI node (set up in Amazon Cloud)	*Client:* Dashboard *Server:* O-MI node (in municipality facilities)	*Client:* App (Toodego) *Server:* O-MI node (in municipality facilities)	*Client:* App *Server:* O-MI node (in municipality facilities)	*Client:* App (Waterbus) *Server:* O-MI node (in municipality facilities)	*Client:* App (On Wheels) *Server:* O-MI node (CIRB)
Smart connected objects	*Platforms:* - Park & Ride - Parkkihubi - BMW connected drive - EV charger box	*Sensors:* - Soil humidity; - Temperature; - Tank Level; - Tree activity; - Rain gauge	*Platforms:* - LoRaWAN - SigrenEa - MINERIS - Truck navigation system	*Platforms:* - Orange - Waze - OpenStreet Map	*Platforms:* - Google maps	*Sensors/Platforms:* - In-ground & surface-mounted sensors - BMW connected drive
Data providers	- Parking Energy - City of Helsinki - BMW	- InfoClimat	- Grand Lyon - Bottle bank sensor providers	- Firebase - Orange - Waze - Warp10	- Brussels harbor	- BMW
Business stakeholders	- Aalto University - Parking Energy - City of Helsinki	- Hydrasol - Grand Lyon - UrbaSense - Sigfox - Objenious	- Bottle bank companies - MINERIS - Grand Lyon - SigrenEa	- Holonix - CIRB brussels - Brussels mobility - Cropland	- Brussels harbor	- CommuniThings - On Wheels - Parking Brussels

show how the ''generic'' bIoTope ecosystem (introduced in FIGURE 5) can – *and has been* – instantiated/adapted to each city infrastructure. Furthermore, technical details about some of these pilots have been published in earlier research papers [35], [56], [78], [121].

The real-life case studies presented in our article are based on the bIoTope ecosystem which has also been compared with state-of-the-art research innovations in Sections II and III. The strategy of commercial vendors is often about binding city organizations to their proprietary API solutions, locking them in vertical silos. One of the major challenges targeted in this paper is achieving horizontal interoperability between vendor lock-in and vertically-oriented closed systems. Moreover, the commercially-driven API is often non-standardized and there is no support for open service discovery. Hence, we focus on the creation of an open IoT innovation ecosystem to address part of this challenge.

A. HELSINKI PILOT: EV CHARGING STATION SERVICE

The EV Charging Station-related PoC was conceptualized with the aim to create a vendor-independent EV charging station ecosystem in Helsinki city and surrounding areas. In other words, it should help the city to easily integrate any EV charging technological solutions provided by private companies and other non-specialized IT solution providers (e.g., households and private parking places) into that ecosystem. This PoC is developed around the scenario that has been described in the comics introduced in Figures 1 and 2 (i.e., an EV arriving in a new location and searching for the best option for parking and charging). As highlighted in TABLE 8, several external data sources and platforms were integrated, including:

- *Database of Parking Energy Ltd. (PE):* an O-MI node/server has been installed at their premises, enabling the control of the company charging boxes using O-MI/O-DF messages;
- *Databases of Helsinki municipality:* an O-MI server has been installed on Amazon Lambda, enabling to access two distinct databases of Helsinki municipality: (i) one storing near real-time street side parking data, and (ii) another storing Park & Ride (P&R) data of regional transport;
- *The connected private parking system at Aalto University:* a prototype of a charging box developed in-house was also integrated to the same O-MI node.

FIGURE 9 provides insight into the overall PoC implementation and how it connects with the bIoTope ecosystem. The in-house EV charger box and EV used for this PoC are depicted, along with the App named *Parking and charging App* that has been developed by Gruppo Sigla srl. to enable end-users (i.e., citizens) to interact with the bIoTope ecosystem, and more specifically with the EV Charging Station Service. BMW EV, as shown in FIGURE 9, was used for demonstrating the feasibility of this PoC. A video about this PoC was published on the bIoTope project website (see URL given as footnote[13]).

FIGURE 10 provides a more in-depth view in the form of a sequence diagram of how horizontal integration for the above-introduced platforms (databases, systems) was achieved. Before interacting with an end user (via App/EV), several data exchanges have to be performed for being prepared to any subsequent – *EV charging station*

[13]https://biotope-project.eu/news/new-video-describing-biotope-innovations-for-smart-equipment-and-, last accessed June, 2020

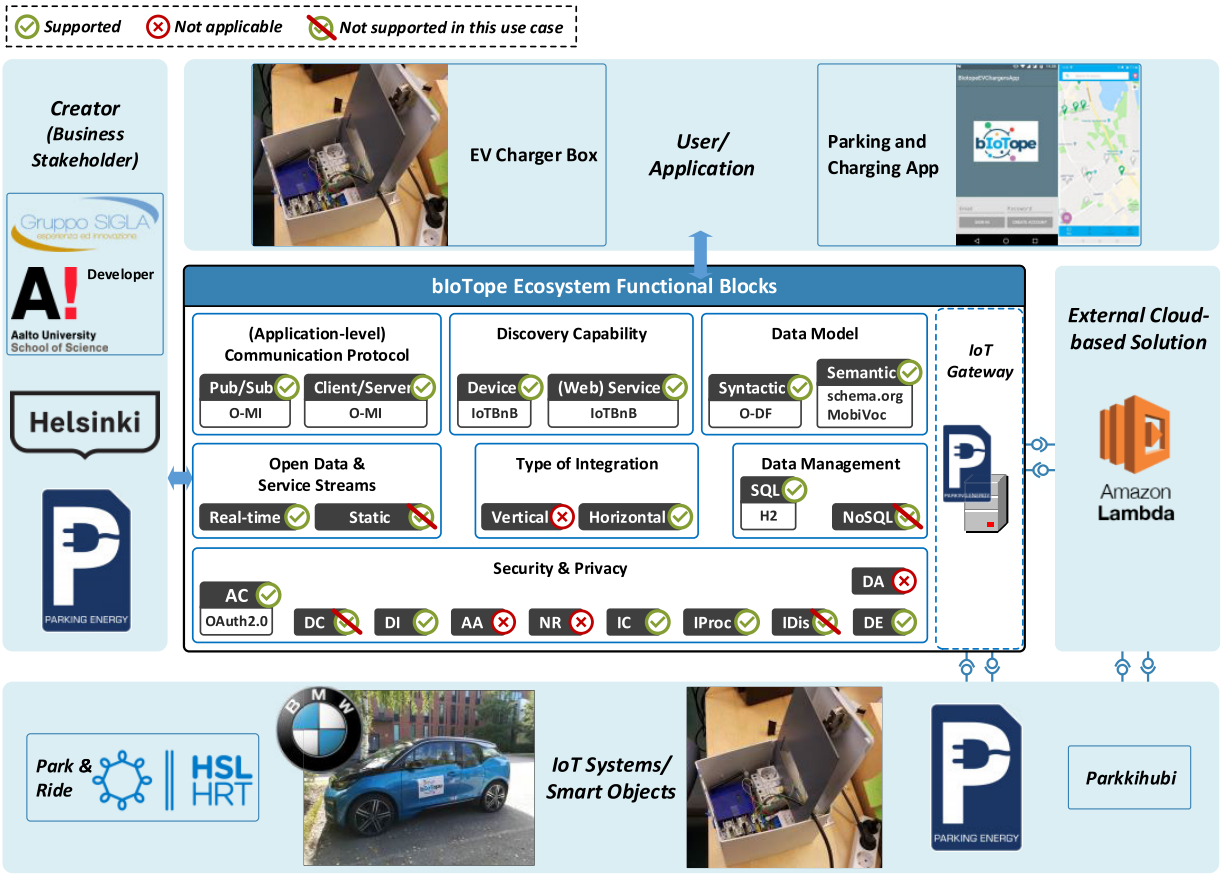


FIGURE 9. EV parking and charging use case; where *O-MI* is Open Messaging Interface, *O-DF* is Open Data Format, *AC* is Access Control, *DC* is Data Confidentiality, *DI* is Data Integrity, *AA* is Availability, *NR* is Non-repudiation, *IC* is Information Collection, *IProc* is Information Processing, *IDis* is Information Dissemination, *DE* is Data Encryption, and *DA* is Data Anonymity.

service – request. First, software agents (O-MI updaters) running on Amazon Web Services (AWS) poll parking data interfaces provided by Parkkihubi and HSL's Park&Ride (see steps denoted by *1a* and *1b* in FIGURE 10), thus updating parking states on an O-MI node residing at AWS. A third software agent subscribes to residential parking boxes using O-MI subscription mechanisms (see *1c*). The Parking Energy, hosting their own O-MI node, maintain their node with their internal update routines (see *1d*). The two O-MI nodes are then registered *via* IoTBnB to make their services discoverable/visible on the data/service catalog (see *2a-2b*). In this respect, upon registration, the O-MI node behind the marketplace IoTBnB performs an O-MI "read all" request to the registered services (see *3a-3b*) in order to index the exposed data/services. Now that parking and charging data consolidation processes have been set up, the end user can perform searches. At step *4* in FIGURE 10, interaction between the App/EV and the ecosystem begins. The App/EV discovers available parking and charging services using IoTBnB APIs (IoTBnB returns the AWS and Parking Energy O-MI web end points). The App/EV then requests parking and charging availability from these O-MI nodes (see *5a* and *5b*). These requests include the profile and any contextual information that is currently available (e.g., target location, estimated time of arrival, current battery level). The O-MI nodes (or software agents) then determine the optimal available locations for parking and charging and return them to the App/EV.

To evaluate the parking and charging system, we perform a load test on two O-MI nodes (IoTBnB and Parking Energy nodes) and observe the throughput that these O-MI nodes can manage. FIGURE 11 shows the results, providing throughput in Mb/s over the increasing number of users. We evaluate the maximum (measured) throughput by creating 1000 concurrent users through the Apache JMeter software that sent only once, respectively, (i) the search request depicted in Figure 11(a) for the IoTBnB O-MI node, and (ii) a method call request for the Parking Energy O-MI node. The theoretical throughput is computed by considering that the server handles only one frame per user at a time, i.e. a traffic load (request + response) equals to 1924 bytes at 100 Mb/s. Indeed, each user generated a single request for a specific query in such experiments. Based on the subsequent throughput evaluation, the measured throughput does not increase as sharply as theoretical throughput in FIGURE 11(a). Similarly, in FIGURE 11(b), the measured throughput becomes almost consistent after only 10 concurrent users in contrast to

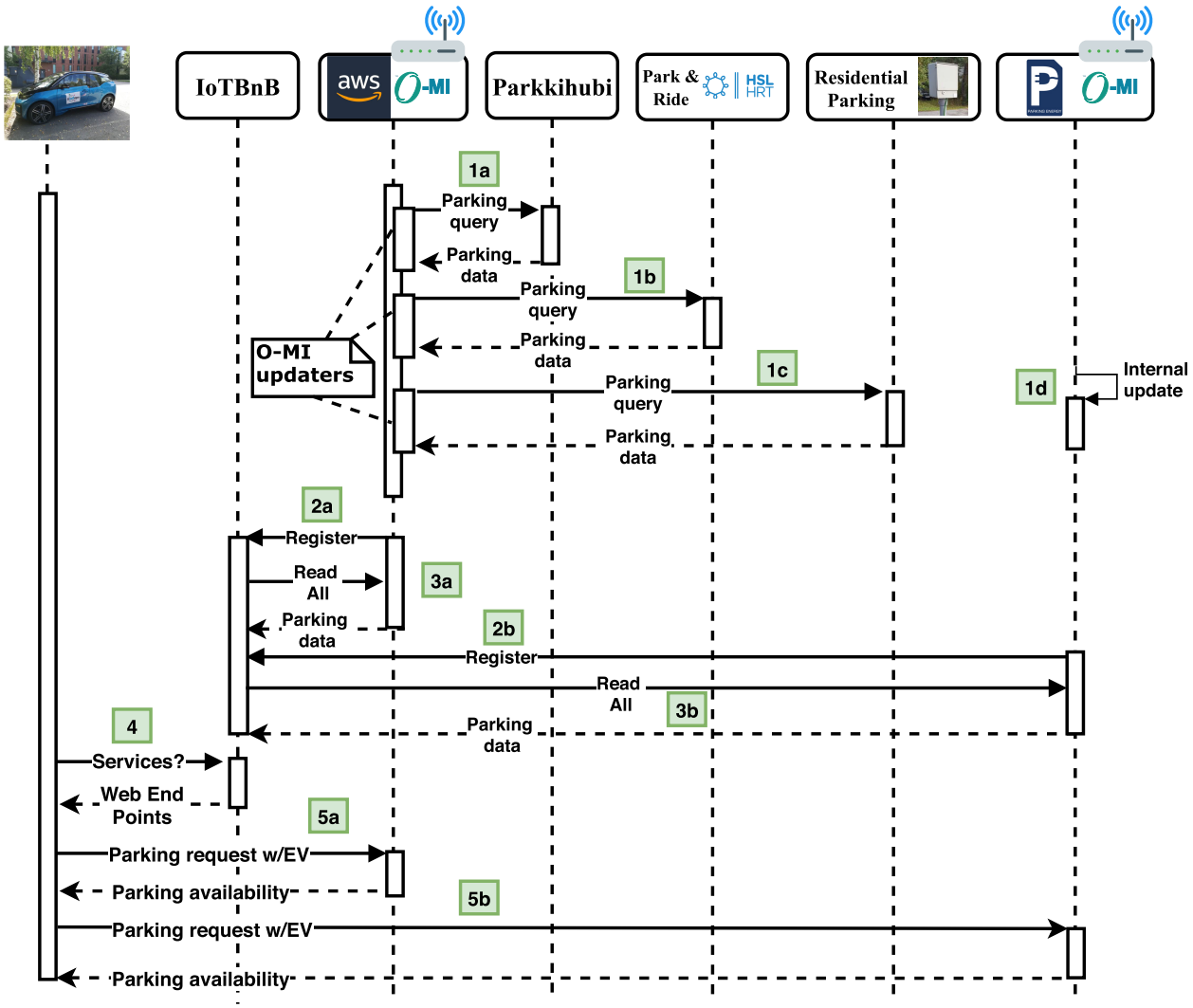
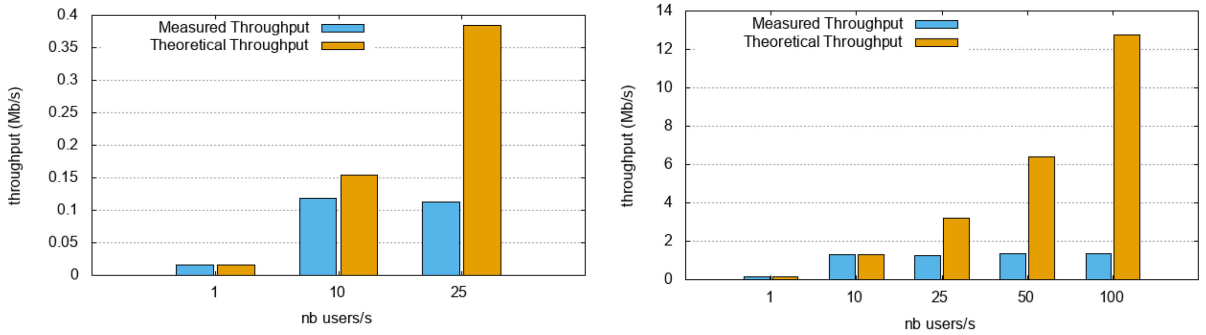


FIGURE 10. Sequence diagram for EV charging and parking availability which shows O-MI/O-DF communications among seven entities involved in the pilot.



(a) Throughput evaluation for IoTBnB O-MI node

(b) Throughput evaluation for Parking Energy O-MI node

FIGURE 11. Throughput measurements w.r.t. the increasing number of users for EV charging and parking system.

theoretical throughput. Overall, it can be concluded that the use case scenario is scalable and efficient with the increase in load (user requests) when thousands of users access the EV charging system in a short period of time.

B. LYON PILOT: HEAT WAVE MITIGATION

Métropole de Lyon has been conducting heat wave measurement campaigns using temporary or mobile sensors. However, partners of the territory, and in particular researchers

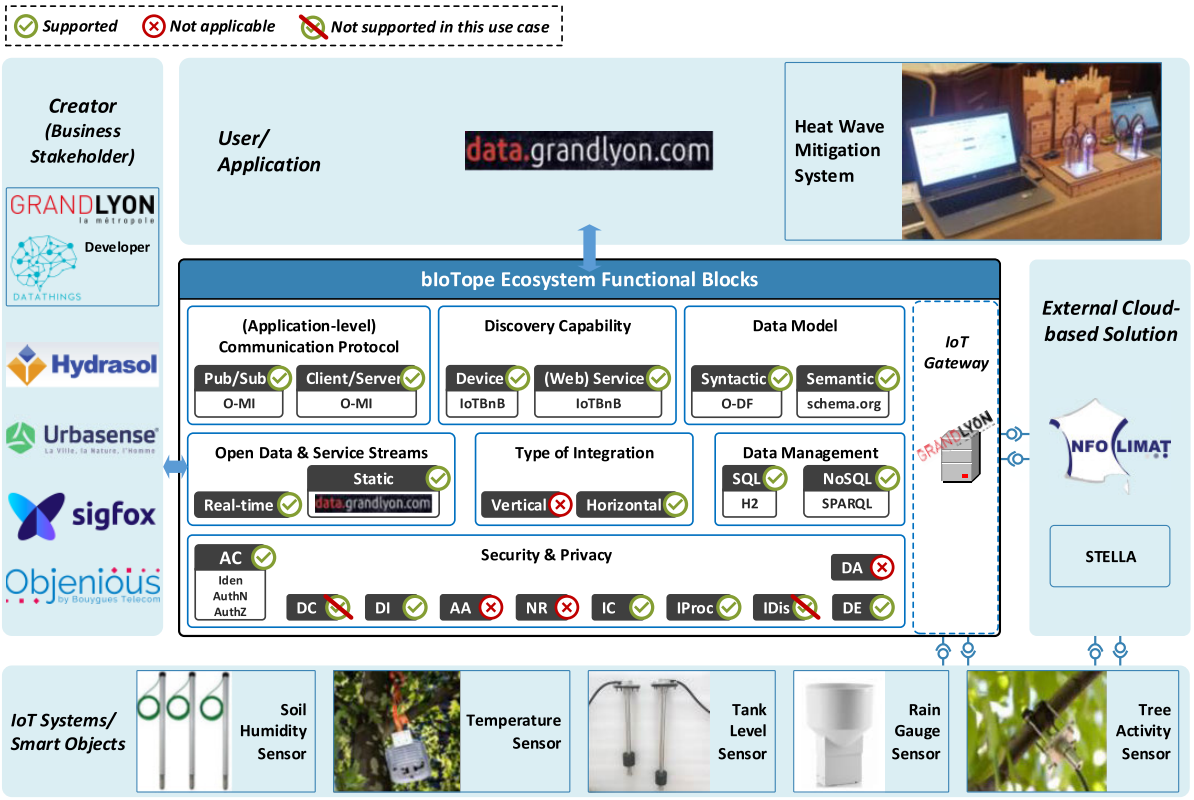


FIGURE 12. Heat wave mitigation use case; where *O-MI* is Open Messaging Interface, *O-DF* is Open Data Format, *AC* is Access Control, *Iden* is Identification, *AuthN* is Authentication, *AuthZ* is Authorization, *DC* is Data Confidentiality, *DI* is Data Integrity, *AA* is Availability, *NR* is Non-repudiation, *IC* is Information Collection, *IProc* is Information Processing, *IDis* is Information Dissemination, *DE* is Data Encryption, and *DA* is Data Anonymity.

modelling heat wave phenomena and their impact on citizens, would prefer a true IoT network that allows horizontal communications between distinct storage and processing platforms. Within this context, the Garibaldi street, which is subject to a large-scale urban renewal project, has undergone a fundamental transformation/renovation in 2014 in order to support IoT experiments. An interesting feature of this street is that an underground vault of 1200m^3 has been re-purposed to store rainwater e.g. for street cleaning and street sweeper refilling. Four green areas were equipped with various kinds of sensors, in particular, air temperature sensors, soil moisture and tree activity/health sensors to monitor the watering needs of trees. Remote controllable pumps and valves (for irrigation control management) were installed.

All these technologies were integrated to the bIoTope ecosystem, as detailed in FIGURE 12. It can be observed that all bIoTope ecosystem functional blocks are used, except the data confidentiality and information dissemination modules. In this PoC, Datathings (a Luxembourgish company), Hydrasol, Urbasense, and Objenious (french companies) as well as Grand-Lyon Metropolis developed together this pilot, which means that all back-end systems of these private and public organization were integrated by setting a number of O-MI nodes in different premises. Furthermore, external cloud-based solutions, namely Infoclimat and Stella, were integrated to respectively access weather-related data and control the water supervision system of Grand-Lyon Metropolis. From an end-user viewpoint, outcomes of this PoC are made available/accessible via the Grand Lyon metropolis's open data portal.[14]

C. BRUSSELS PILOT: SAFETY AROUND SCHOOL

Safety around school is one of the pilots that addresses a safer mobility of children travelling to/from school in the Brussels-Capital region. Since most of the accidents in the Brussels region are caused by dangerous overruns, excessive speed and pedestrian crossing, the municipality aims to develop appropriate safety measures. These measures include reducing the number of vehicles, informing children and parents about potential dangers around the school, or advising them to select a specific and safer itinerary [121].

FIGURE 13 provides insight into the architecture set up for this PoC. Brussels Mobility (see Business stakeholders) is the administration of the Brussels-Capital region responsible for the definition of mobility strategies, projects to develop, renew and maintain public spaces and roads, as well as public transport infrastructure and taxis of the region. For the foreseen PoC, the following platforms were integrated to

[14]https://data.grandlyon.com/accueil, last accessed June, 2020

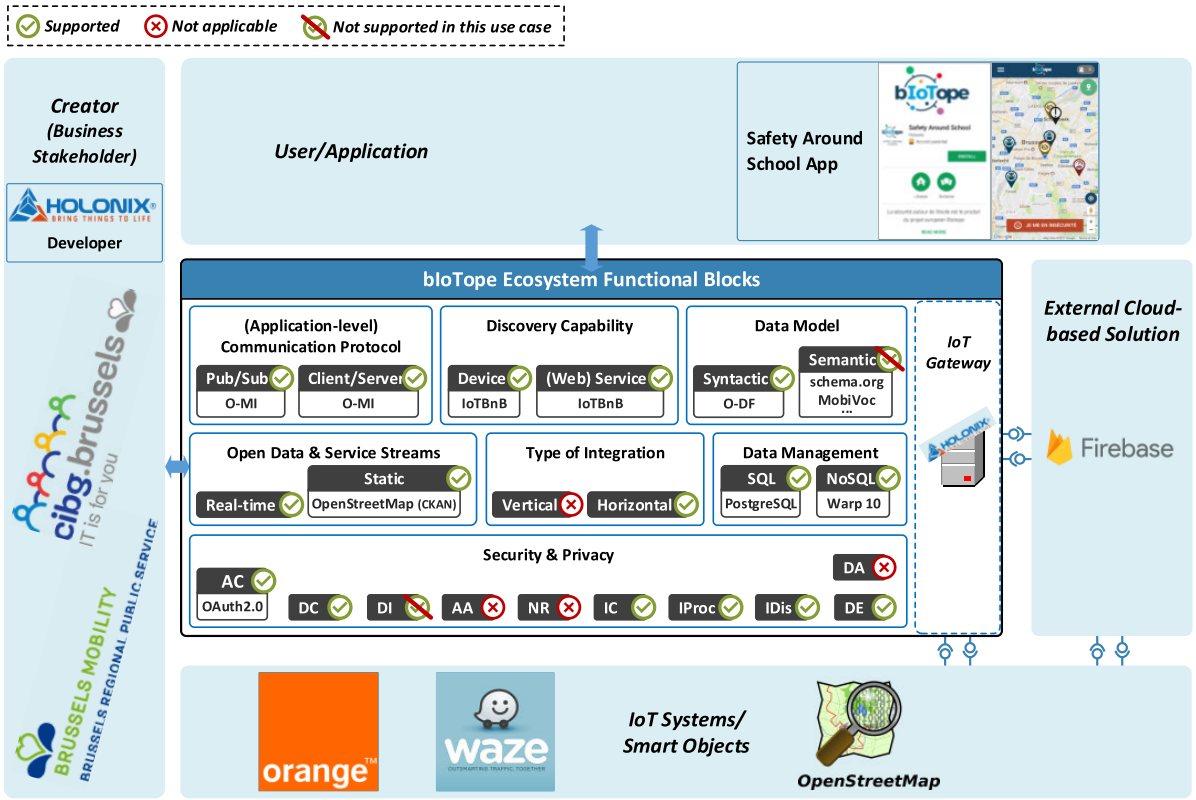


FIGURE 13. Safety around school use case; where *O-MI* is Open Messaging Interface, *O-DF* is Open Data Format, *AC* is Access Control, *DC* is Data Confidentiality, *DI* is Data Integrity, *AA* is Availability, *NR* is Non-repudiation, *IC* is Information Collection, *IProc* is Information Processing, *IDis* is Information Dissemination, *DE* is Data Encryption, and *DA* is Data Anonymity.

the bIoTope ecosystem: (i) *Orange (owned by CIRB Brussels):* giving access to mobility-related data; (ii) *Waze:* giving access to community-based traffic and navigation events; (iii) *OpenStreetMap:* giving access to roads, trails and much more, around the region which is free to use for any purpose. The collected data are stored as aggregated data per segment in the database of the Holonix company, which integrated into a Big Data container. Holonix is the main developer of the pilot with the end-user application provided in the form of *Safety Around School* mobile App. Note that Firebase (Google's mobile platform) has been integrated into this PoC in order to develop the end-user app.

VI. bIoTope ECOSYSTEM EVALUATION

In our bIoTope project, the consortium defines the following three Key Performance Indicators (KPIs) to assess the achievements and the project impact: (i) New applications developed, (ii) Number of services developed, and (iii) Number of startups stepping into bIoTope every year. With respect to this, the bIoTope project achievements are listed in TABLE 9. In addition to these measures, the European commission has developed an Innovation Radar platform to identify high potential innovations and innovators in EU-funded research programmes based on their market readiness. The Innovation Radar results of bIoTope are provided on the EU Horizon 2020 webpage for the O-MI/O-DF connectivity framework[15] and IoTBnB marketplace innovations.[16]

TABLE 9. bIoTope project achievements.

KPI	Measure	Outcome	Comments
New applications	12	18	bIoTope engaged 11 new SMEs through open calls, each having developed 1-2 new applications
Number of services	3	3	The proposed services were developed as a part of the Helsinki pilot
Number of startups	10	20	11 new startups were engaged through open calls. Additional startups were working as sub-contractors and partners to these startups

Several KPI frameworks measure the outcome of smart city programs. We consider Innovation metrics from the Prosperity-related KPIs of CITYKeys framework [10] to evaluate the contribution of our bIoTope ecosystem and compare it with the current state-of-the-art smart city infrastructures. These metrics are: (i) Improved interoperability: It is measured by assigning numbers from 1 (lowest) to 6 (highest) based on six taxonomy criteria a) to f) defined in Section II and the associated TABLE 4; (ii) New startups: The number

[15]https://www.innoradar.eu/innovation/34055, last accessed Oct, 2020
[16]https://www.innoradar.eu/innovation/22481, last accessed Oct, 2020

TABLE 10. Comparative analysis based on Innovation-related metrics. ✓means supported, 'n/s' means not specified, and 'n/a' means not applicable.

Ref.	Interoperability	Innovative environment	Open data quality
Proposed (bIoTope project)	6	3 (Helsinki, Brussels, Lyon)	⋆⋆⋆⋆
[86]	5	1 (Murcia)	n/s
[87]	4	1 (Bristol)	⋆⋆⋆⋆
[88]	3	✓(n/s)	n/s
[24]	3	n/s	n/s
[89]	6	1 (Messina)	⋆⋆⋆
[91]	4	1 (Tuscany)	⋆⋆⋆⋆
[93]	5	n/s	n/s
[94]	4	1 (São Paulo)	⋆⋆⋆
[95]	5	1 (Khulna)	✓(n/s)
[97]	6	2 (Turin, Manchester)	n/s
[98]	4	1 (Aarhus)	⋆⋆⋆⋆
[99], [100]	6	1 (Santander)	n/s
[101]	4	✓(n/s)	n/s
[102], [103]	3	6 (Athens, Birminghan, Lecce, Madrid, Singapore and Montpellier)	⋆⋆⋆⋆⋆
[104]	3	n/s	n/a
[105]	5	1 (Santander)	n/s

of startups stepping into the project; (iii) Stimulating an innovative environment: It is measured based on the smart city pilots set up in distinct countries and the numbers are assigned from 1 to 6; and (iv) Quality of open data: we adopt Tim's 5-star open data plan[17] to measure the data quality. TABLE 10 shows the comparison of our proposed ecosystem with the existing literature (namely articles initially reviewed in TABLE 5) based on three metrics, since no information can be found in the papers regrading the fourth metric, that is, number of startups. Nevertheless, the resultant startups are 20 in the bIoTope project.

VII. CONCLUSION, IMPLICATIONS AND LIMITATIONS

A. CONCLUSION

The Internet of Things (IoT) is revolutionizing smart cities, making it possible for billions of devices to discover, communicate and seamlessly interact with each other. However, all these Things are today feeding vertically-oriented closed systems (commonly referred to as vertical silos), proprietary platforms and application areas, which prevent the development of viable IoT infrastructure, both technologically and business-wise. This is valid in the context of smart cities, which comprises many sub-systems, tons of heterogeneous sensor data, and a wide range of interacting and cooperating city stakeholders such as citizens, governments, companies, logistic centers and other legal entities. To this end, smart city infrastructures must provide means to create, when and as needed, ad hoc and loosely coupled information flows between any kinds of smart connected objects, databases and users. In this paper: (i) we discuss a state-of-the-art literature review of smart city infrastructures by analyzing the current state of affairs; (ii) we introduce seven functional building blocks underlying the open IoT ecosystem developed as part of the EU's Horizon 2020 bIoTope project; (iii) we present the smart city proofs-of-concept of the implementation, or instantiation to be precise, of the bIoTope ecosystem in three distinct cities: Helsinki, Lyon and Brussels; and (iv) we evaluate and compare our bIoTope ecosystem by considering Prosperity-related metrics of the CITYKeys framework.

These pilots demonstrate the extent to which the bIoTope ecosystem is able to achieve horizontal integration between proprietary and vertically-oriented closed systems, which is the major obstacle of cross-domain and cross-application services. The bIoTope ecosystem was not evaluated in detail in this paper, as such evaluation studies were reviewed in previous research papers focusing on specific use cases [35], [56], [78], [121].

B. IMPLICATIONS

The bIoTope ecosystem could contribute to improve existing smart city KPI frameworks. For example, considering the CITYKeys framework [10], bIoTope could contribute to:

- *Planet-related KPIs (e.g., Pollution & waste, Climate Resilience and Energy & mitigation):* bIoTope can help to more easily integrate (over time) new sensor technologies and innovative web services that could contribute to KPI-related computation;
- *Prosperity-related KPIs (e.g., Innovation):* bIoTope can contribute to improve accessibility of open data based on open and standardized APIs;
- *Governance-related KPIs (e.g., Organisation):* bIoTope is primarily designed to support horizontal integration of systems, thus fostering open innovation across all smart city sectors, spanning from energy, water, building and mobility to industry.

C. LIMITATIONS

Despite commendable improvements in the IoT technology for smart cities, few limitations still remain to be addressed in the proposed bIoTope ecosystem:

1) The digital marketplace (IoTBnB) provides the necessary APIs to discover and access relevant IoT data/services in cities, under the condition that the system looking for a data/service is aware of the IoTBnB endpoint. This is still a limitation in the exploitation of the ecosystem;
2) The owner of an O-MI node has to manually register his/her node on IoTBnB, which poses some limitations, as thus far, no module has been designed to automate this registration process;
3) Although O-DF is flexible enough to embed semantic annotations, there is no module to help O-MI node owners to select appropriate semantic vocabularies (knowing that tens of different ontologies could exist to describe the same domain/entity).

[17] [Online]. https://5stardata.info/en/, last accessed Oct, 2020

```
<omiEnvelope ttl="10" version="1.0" xmlns="http://www.opengroup.org/xsd/omi/1.0/">
  <response>
    <result msgformat="odf">
      <return returnCode="200">
      </return>
      <msg>
     <Objects xmlns="http://www.opengroup.org/xsd/odf/1.0/">
       <Object type="ChargingService" prefix="schema: http://www.schema.org/ mv: http://www.schema.mobivoc.org/">
            <id>ChargingService</id>
            <InfoItem name="getAddress" method="odf" >
              <MetaData>
                <InfoItem name="InfoItemType">
                  <value>odf:Method</value>
                </InfoItem>
                <InfoItem name="odf:Parameter">
                  <value type="odf:Objects">
                    <Objects>
                      <Object>
                        <id>Parameters</id>
                        <InfoItem type="schema:Distance" name="maxDistance" required="true">
                          <value>100</value>
                        </InfoItem>
                        <InfoItem name="plugType" type="mv:plugType" required="false">
                          <value>mv:CHAdeMO</value>
                        </InfoItem>
                        <Object type="schema:GeoCoordinates">
                          <id>Coordinates</id>
                          <InfoItem type="schema:longitude" name="longitude" required="true">
                            <value>60.187640</value>
                          </InfoItem>
                          <InfoItem type="schema:latitude" name="latitude" required="true">
                            <value>24.828300</value>
                          </InfoItem>
                        </Object>
                      </Object>
                    </Objects>
                  </value>
                </InfoItem>
                <InfoItem name="odf:ReturnType">
                  <value type="odf:Objects">
                    <Objects xmlns="http://www.opengroup.org/xsd/odf/1.0/" xmlns:xs="http://www.w3.org/2001/
                         XMLSchema" xmlns:odf="http://www.opengroup.org/xsd/odf/1.0/">
                      <Object type="mv:ParkingFacility">
                        <id>ParkingFacilities</id>
                        <Object type="schema:PostalAddress">
                          <id>address</id>
                          <InfoItem name="addressCountry">
                            <value>Finland</value>
                          </InfoItem>
                          <InfoItem name="addressLocality">
                            <value>Otaniemi</value>
                          </InfoItem>
                          <InfoItem name="addressRegion">
                            <value>Espoo</value>
                          </InfoItem>
                          <InfoItem name="streetAddress">
                            <value>Konemiehentie 4</value>
                          </InfoItem>
                        </Object>
                      </Object>
                    </Objects>
                  </value>
                </InfoItem>
              </MetaData>
              <value>odf:Method</value>
            </InfoItem>
          </Object>
        </Objects>
      </msg>
    </result>
  </response>
</omiEnvelope>
```

Listing. 1. Response after reading Metadata for method call.

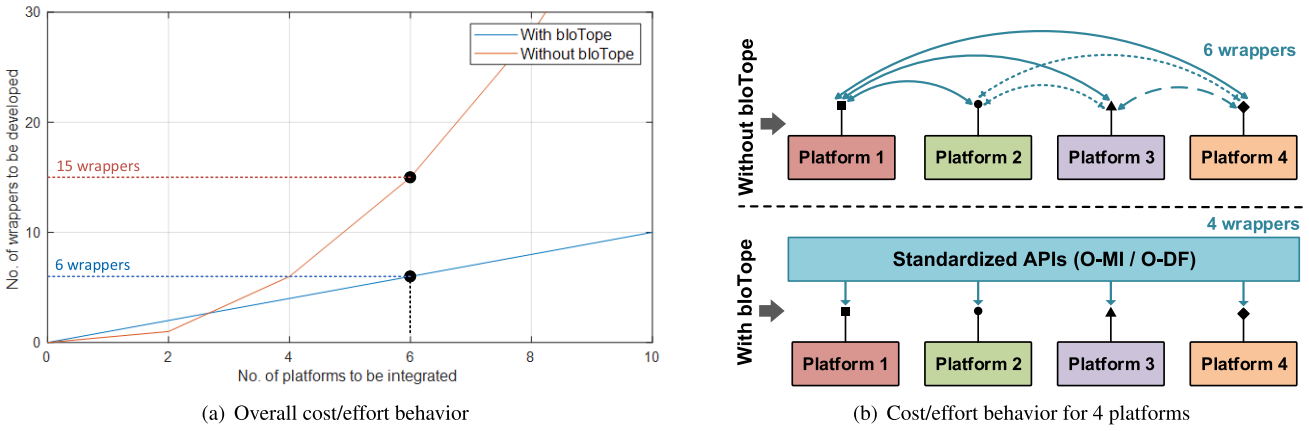
D. FUTURE RESEARCH DIRECTIONS

In future work, the above limitations should be addressed, although some preliminary work has been conducted and recently published regarding the third limitation [59], [113], in which linked vocabulary recommendation strategies have been investigated. Further, the related future research avenues could include:

- The scalability of the proposed framework for the incorporation of more efficient alignment with governmental objectives and strategies. This can provide line-of-sight

```
<omiEnvelope xmlns="http://www.opengroup.org/xsd/omi/1.0/" version="1.0" ttl="0">
  <read msgformat="odf">
    <msg>
      <Objects xmlns="http://www.opengroup.org/xsd/odf/1.0/">
        <Object>
          <id>ChargingService</id>
          <InfoItem name="getAddress">
            <MetaData/>
          </InfoItem>
        </Object>
      </Objects>
    </msg>
  </read>
</omiEnvelope>
```

Listing. 2. **Read metadata of the method call.**



(a) Overall cost/effort behavior

(b) Cost/effort behavior for 4 platforms

FIGURE 14. **Example of cost/effort with and without bIoTope ecosystem.**

to citizen requirements and the performance of smart city services.

- The commercial business requirements and insights into the relation between business and citizen needs through infrastructure assets.
- Data security and digital citizens' privacy issues at both hardware and system levels. This requires a more robust and resilient ecosystem for prevention against cyber threats.
- Controlling personal data about the IoT marketplace by end-users. Such data will assist them in (i) deciding what personal data are shared together with the actual content and (ii) auditing the access of their personal data.

APPENDIX A
O-MI/O-DF MESSAGES FOR READING THE MetaData OF METHOD NAMED "getAddress"

See Listing 1 and 2.

APPENDIX B
COMPARISON OF COST/EFFORT BETWEEN TRADITIONAL APPROACH VS. bIoTope APPROACH

Figure 14(a) shows the cost/effort behavior for integrating platform APIs with a traditional approach vs. bIoTope approach. This graph is drawn from the fact that for interconnecting n distinct platforms, it is required to develop $\frac{n\times(n-1)}{2}$ wrappers. While adopting an open IoT ecosystem approach such as bIoTope, only n wrappers need to be developed. Figure 14(b) shows an interconnection between four platforms in which 6 wrappers are required with traditional approach, whereas 4 wrappers are required with bIoTope approach.

REFERENCES

[1] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, "Future trends and current state of smart city concepts: A survey," *IEEE Access*, vol. 8, pp. 86448–86467, 2020.

[2] F. Sivrikaya, N. Ben-Sassi, X.-T. Dang, O. C. Gorur, and C. Kuster, "Internet of smart city objects: A distributed framework for service discovery and composition," *IEEE Access*, vol. 7, pp. 14434–14454, 2019.

[3] S. N. Kinawy, T. E. El-Diraby, and H. Konomi, "Customizing information delivery to project stakeholders in the smart city," *Sustain. Cities Soc.*, vol. 38, pp. 286–300, Apr. 2018.

[4] A. Camero and E. Alba, "Smart city and information technology: A review," *Cities*, vol. 93, pp. 84–94, Oct. 2019.

[5] R. W. S. Ruhlandt, "The governance of smart cities: A systematic literature review," *Cities*, vol. 81, pp. 1–23, Nov. 2018.

[6] L. Anthopoulos, "Smart utopia VS smart reality: Learning by experience from 10 smart city cases," *Cities*, vol. 63, pp. 128–148, Mar. 2017.

[7] R. P. Dameri, "Smart city definition, goals and performance," in *Smart City Implementation*. Cham, Switzerland: Springer, 2017, pp. 1–22.

[8] V. Fernandez-Anez, "Stakeholders approach to smart cities: A survey on smart city definitions," in *Proc. Int. Conf. Smart Cities*. Cham, Switzerland: Springer, 2016, pp. 157–167.

[9] A. Huovila, P. Bosch, and M. Airaksinen, "Comparative analysis of standardized indicators for smart sustainable cities: What indicators and standards to use and when?" *Cities*, vol. 89, pp. 141–153, Jun. 2019.

[10] P. Bosch, S. Jongeneel, V. Rovers, H.-M. Neumann, M. Airaksinen, and A. Huovila, "Citykeys indicators for smart city projects and smart cities," Eur. Commission, CITYkeys Rep. D1-4, 2017.

[11] K. Främling, J. Holmström, T. Ala-Risku, and M. Kärkkäinen, "Product agents for handling information about physical objects," Rep. Lab. Inf. Process. Sci. Ser. B, TKO-B, Helsinki Univ. Technol., Espoo, Finland, Tech. Rep. B153, 2003, vol. 153, no. 2003.

[12] N. T. Nguyen and R. Matsuhashi, "An optimal design on sustainable energy systems for shrimp farms," *IEEE Access*, vol. 7, pp. 165543–165558, 2019.

[13] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT," *IEEE Access*, vol. 3, pp. 622–637, 2015.

[14] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[15] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, Oct. 2019, Art. no. 101660.

[16] B. P. L. Lau, S. H. Marakkalage, Y. Zhou, N. U. Hassan, C. Yuen, M. Zhang, and U.-X. Tan, "A survey of data fusion in smart city applications," *Inf. Fusion*, vol. 52, pp. 357–374, Dec. 2019.

[17] V. Moustaka, A. Vakali, and L. G. Anthopoulos, "A systematic review for smart city data analytics," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–41, Jan. 2019.

[18] R. Petrolo, V. Loscrì, and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, p. e2931, Jan. 2017.

[19] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Comput. Surv.*, vol. 50, no. 3, pp. 1–43, 2017.

[20] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[21] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102080.

[22] H. Tschofenig, J. Arkko, and D. McPherson, "Architectural considerations in smart object networking," Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. RFC-7452, Mar. 2015.

[23] P.-L. Benedick, J. Robert, Y. Le Traon, and S. Kubler, "O-MI/O-DF vs. MQTT: A performance analysis," in *Proc. IEEE Ind. Cyber-Phys. Syst. (ICPS)*, May 2018, pp. 153–158.

[24] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design," *Comput. Netw.*, vol. 144, pp. 163–200, Oct. 2018.

[25] T. G. Oberstein and A. Goedde. (2016). *The Web Application Messaging Protocol*. [Online]. Available: https://tools.ietf.org/html/draft-oberstet-hybi-tavendo-wamp-02

[26] H. S. Oluwatosin, "Client-server model," *IOSRJ Comput. Eng.*, vol. 16, no. 1, pp. 2278–8727, 2014.

[27] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, *Hypertext Transfer Protocol–HTTP/1.1*, document RFC 2616, 1999.

[28] P. Saint-Andre, *Extensible Messaging and Presence Protocol (XMPP): Core*, document RFC 6120, 2004.

[29] D. Box, D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. F. Nielsen, S. Thatte, and D. Winer, "Simple object access protocol (SOAP) 1.1," World Wide Web Consortium (W3C), Cambridge, MA, USA, Tech. Rep., 2000.

[30] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, *The Constrained Application Protocol (CoAP)*, document RFC 7252, Internet Eng. Task Force, 2014.

[31] S. Din, A. Paul, W.-H. Hong, and H. Seo, "Constrained application for mobility management using embedded devices in the Internet of Things based urban planning in smart cities," *Sustain. Cities Soc.*, vol. 44, pp. 144–151, Jan. 2019.

[32] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, and J. Song, "Toward a standardized common M2M service layer platform: Introduction to oneM2M," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 20–26, Jun. 2014.

[33] S.-H. Leitner and W. Mahnke, "OPC UA–service-oriented architecture for industrial applications," *ABB Corporate Res. Center*, vol. 48, pp. 61–66, 2006.

[34] K. Främling. (Dec. 2019). Open Messaging Interface (O-MI). The Open Group, Standard. [Online]. Available: https://www.opengroup.org/library/c19e

[35] S. Kubler, J. Robert, A. Hefnawy, K. Framling, C. Cherifi, and A. Bouras, "Open IoT ecosystem for sporting event management," *IEEE Access*, vol. 5, pp. 7064–7079, 2017.

[36] K. Hartke, *Observing Resources in the Constrained Application Protocol (CoAP)*, document IETF RFC 7641, 2015.

[37] S. Cheshire and M. Krochmal, *Multicast DNS*, document RFC 6762, IETF, 2013.

[38] C. Vandana and A. A. Chikkamannur, "Study of resource discovery trends in Internet of Things (IoT)," *Int. J. Adv. Netw. Appl.*, vol. 8, no. 3, p. 3084, 2016.

[39] M. Boucadair, R. Penno, and D. Wing, *Universal Plug and Play (UPnP) Internet Gateway Device-Port Control Protocol Interworking Function (IGD-PCP IWF)*, document RFC 6970, 2013.

[40] R. Khan and S. U. Khan, "Design and implementation of UPnP-based energy gateway for demand side management in smart grid," *J. Ind. Inf. Integr.*, vol. 8, pp. 8–21, Dec. 2017.

[41] J.-C. Lee, J.-H. Jeon, and S.-H. Kim, "Design and implementation of healthcare resource model on IoTivity platform," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2016, pp. 887–891.

[42] J.-T. Kim, Y.-J. Oh, H.-K. Lee, E.-H. Paik, and K.-R. Park, "Implementation of the DLNA proxy system for sharing home media contents," *IEEE Trans. Consum. Electron.*, vol. 53, no. 1, pp. 139–144, Feb. 2007.

[43] D. Kourtesis and I. Paraskakis, "Combining SAWSDL, OWL-DL and UDDI for semantically enhanced Web service discovery," in *Proc. Eur. Semantic Web Conf.* Cham, Switzerland: Springer, 2008, pp. 614–628.

[44] D. Martin, M. Burstein, J. Hobbs, O. Lassila, D. McDermott, S. McIlraith, S. Narayanan, M. Paolucci, B. Parsia, T. Payne, E. Sirin, N. Srinivasan, and K. Sycara. (2004). *OWL-S: Semantic Markup for Web Services*. [Online]. Available: https://www.w3.org/Submission/OWL-S/

[45] J. Sangers, F. Frasincar, F. Hogenboom, and V. Chepegin, "Semantic Web service discovery using natural language processing techniques," *Expert Syst. Appl.*, vol. 40, no. 11, pp. 4660–4671, Sep. 2013.

[46] *OWS Integrated Client: Architecture, Design, and Experience*, I. Open Geospatial Consortium (OGC), Wayland, MA, USA, 2006.

[47] W. Li, C. Yang, D. Nebert, R. Raskin, P. Houser, H. Wu, and Z. Li, "Semantic-based Web service discovery and chaining for building an arctic spatial data infrastructure," *Comput. Geosci.*, vol. 37, no. 11, pp. 1752–1762, Nov. 2011.

[48] M. Lackovic and P. Trunfio, "A service-oriented discovery framework for cooperating smart objects," in *Internet of Things Based on Smart Objects*. Cham, Switzerland: Springer, 2014, pp. 85–105.

[49] F. Shaikh, U. A. Siddiqui, I. Shahzadi, S. I. Jami, and Z. A. Shaikh, "SWISE: Semantic Web based intelligent search engine," in *Proc. Int. Conf. Inf. Emerg. Technol.*, Jun. 2010, pp. 1–5.

[50] O. Verhodubs, "Towards the ontology Web search engine," *CoRR*, vol. abs/1505.00755, pp. 1–8, May 2015.

[51] M. d'Aquin and E. Motta, "Watson, more than a semantic Web search engine," *Semantic Web*, vol. 2, no. 1, pp. 55–63, 2011.

[52] E. Prud'hommeaux and A. Seaborne. (Jan. 2008). *SPARQL Query Language for RDF, W3C Recommendation*. [Online]. Available: https://www.w3.org/TR/rdf-sparql-query/

[53] A. Hogan, A. Harth, J. Umbrich, S. Kinsella, A. Polleres, and S. Decker, "Searching and browsing linked data with SWSE: The semantic Web search engine," *J. Web Semantics*, vol. 9, no. 4, pp. 365–401, Dec. 2011.

[54] O. Hatzi, G. Batistatos, M. Nikolaidou, and D. Anagnostopoulos, "A specialized search engine for Web service discovery," in *Proc. IEEE 19th Int. Conf. Web Services*, Jun. 2012, pp. 448–455.

[55] *Seekda-Web Services Search Engine*. Accessed: Feb. 2020. [Online]. Available: http://sumedha.blogspot.com/2008/10/wso2-wsas-try-it-powerful-simple.html

[56] A. Karpenko, T. Kinnunen, M. Madhikermi, J. Robert, K. Främling, B. Dave, and A. Nurminen, "Data exchange interoperability in IoT ecosystem for smart parking and EV charging," *Sensors*, vol. 18, no. 12, p. 4404, Dec. 2018.

[57] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 796–809, Jun. 2019.

[58] K. Främling. (Dec. 2019). Open data format (O-DF). The Open Group, Standard. [Online]. Available: https://www.opengroup.org/library/c19d

[59] N. Kolbe, S. Kubler, J. Robert, Y. Le Traon, and A. Zaslavsky, "Linked vocabulary recommendation tools for Internet of Things: A survey," *ACM Comput. Surv.*, vol. 51, no. 6, p. 127, 2019.
[60] C. Cabrera and S. Clarke, "A self-adaptive service discovery model for smart cities," *IEEE Trans. Services Comput.*, early access, Sep. 27, 2019, doi: 10.1109/TSC.2019.2944356.
[61] *Ac02–'Naming, Addressing, Search, Discovery'*, Eur. Res. Cluster Internet-of-Things, Oslo, Norway, 2014.
[62] K. Lee, S. Kim, J. Jeong, S. Lee, H. Kim, and J.-S. Park, "A framework for DNS naming services for Internet-of-Things devices," *Future Gener. Comput. Syst.*, vol. 92, pp. 617–627, Mar. 2019.
[63] J. Robert, S. Kubler, and Y. Le Traon, "Micro-billing framework for IoT: Research & technological foundations," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 301–308.
[64] H. Bohn, F. Golatowski, and D. Timmermann, "Dynamic device and service discovery extensions for WS-BPEL," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2008, pp. 1–6.
[65] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.
[66] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," in *Proc. Int. Conf. Netw. Secur. Appl.* Cham, Switzerland: Springer, 2010, pp. 420–429.
[67] B. Alsamani and H. Lahza, "A taxonomy of IoT: Security and privacy threats," in *Proc. Int. Conf. Inf. Comput. Technol. (ICICT)*, Mar. 2018, pp. 72–77.
[68] D. J. Solove, "A taxonomy of privacy," *Univ. PA Law Rev.*, vol. 154, no. 3, p. 477, Jan. 2006.
[69] D. Hardt, *The OAuth 2.0 Authorization Framework*, IETF, document RFC 6749, vol. 10, 2012, pp. 1721–2070.
[70] *Openid Connect Core 1.0*. Accessed: Jul. 2020. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0-final.html
[71] K. D. Lewis andjames E. Lewis,"Web single sign-on authentication using SAML," 2009, *arXiv:0909.2368*. [Online]. Available: http://arxiv.org/abs/0909.2368
[72] R. Harrison, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*, document RFC 4513, Jun. 2006.
[73] M. Jones, J. Bradley, and N. Sakimura, *Json Web Token (JWT)*, document RFC 7519, Date Retrieval, vol. 5, 2015.
[74] H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, document RFC 2104, Feb. 1997.
[75] D. Guinard and V. Trifa, *Building the Web of Things: With examples in Node.js and Raspberry Pi*. Shelter Island, NY, USA: Manning Publications, 2016.
[76] *Alliance for Internet of Things Innovation (AIOTI)*, European Commission, AIOTI, France, Italy, 2015.
[77] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, and M. Mohammadi, "Toward better horizontal integration among IoT services," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 72–79, Sep. 2015.
[78] J. Robert, S. Kubler, N. Kolbe, A. Cerioni, E. Gastaud, and K. Främling, "Open IoT ecosystem for enhanced interoperability in smart cities–example of Métropole de lyon," *Sensors*, vol. 17, no. 12, p. 2849, Dec. 2017.
[79] S. Kubler, J. Robert, A. Hefnawy, K. Framling, C. Cherifi, and A. Bouras, "Open IoT ecosystem for sporting event management," *IEEE Access*, vol. 5, pp. 7064–7079, 2017.
[80] A. Broring, S. Schmid, C.-K. Schindhelm, A. Khelil, S. Kabisch, D. Kramer, D. Le Phuoc, J. Mitic, D. Anicic, and E. Teniente, "Enabling IoT ecosystems through platform interoperability," *IEEE Softw.*, vol. 34, no. 1, pp. 54–61, Jan. 2017.
[81] P. Turkama and H. Schaffers, *Research and Innovation Programmes Shaping Ecosystems for Open Innovation–Some Lessons, European Commission*, DG Connect Open Innovation Yearbook, 2015.
[82] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, "Internet of Things for smart cities: Interoperability and open data," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 52–56, Nov. 2016.
[83] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.
[84] M. M. Rathore, A. Paul, W.-H. Hong, H. Seo, I. Awan, and S. Saeed, "Exploiting IoT and big data analytics: Defining smart digital city using real-time urban data," *Sustain. Cities Soc.*, vol. 40, pp. 600–610, Jul. 2018.
[85] V. N. Gudivada, D. Rao, and V. V. Raghavan, "NoSQL systems for big data management," in *Proc. IEEE World Congr. Services*, Jun. 2014, pp. 190–197.
[86] M. V. Moreno, F. Terroso-Saenz, A. Gonzalez-Vidal, M. Valdes-Vela, A. F. Skarmeta, M. A. Zamora, and V. Chang, "Applicability of big data techniques to smart cities deployments," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 800–809, Apr. 2017.
[87] Z. Khan, S. L. Kiani, and K. Soomro, "A framework for cloud-based context-aware information services for citizens in smart cities," *J. Cloud Comput.*, vol. 3, no. 1, p. 14, Dec. 2014.
[88] N. Zakaria and J. A. Shamsi, "Smart city architecture: Vision and challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 11, pp. 246–255, 2015.
[89] D. Bruneo, S. Distefano, M. Giacobbe, A. Longo Minnolo, F. Longo, G. Merlino, D. Mulfari, A. Panarello, G. Patanè, A. Puliafito, C. Puliafito, and N. Tapas, "An IoT service ecosystem for smart cities: The #SmartME project," *Internet Things*, vol. 5, pp. 12–33, Mar. 2019.
[90] D. Bruneo, F. Longo, G. Merlino, A. Puliafito, and S. Distefano, "Deploying advanced services in the #SmartME infrastructure," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Sep. 2016, pp. 1–5.
[91] C. Badii, P. Bellini, D. Cenni, A. Difino, P. Nesi, and M. Paolucci, "Analysis and assessment of a knowledge based smart city architecture providing service APIs," *Future Gener. Comput. Syst.*, vol. 75, pp. 14–29, Oct. 2017.
[92] P. Nesi, C. Badii, P. Bellini, D. Cenni, G. Martelli, and M. Paolucci, "Km4City smart city API: An integrated support for mobility services," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2016, pp. 1–8.
[93] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining cloud and sensors in a smart city environment," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, p. 247, Dec. 2012.
[94] A. de M. Del Esposte, E. F. Z. Santana, L. Kanashiro, F. M. Costa, K. R. Braghetto, N. Lago, and F. Kon, "Design and evaluation of a scalable smart city software platform with large-scale simulations," *Future Gener. Comput. Syst.*, vol. 93, pp. 427–441, Apr. 2019.
[95] S. Alamgir Hossain, M. Anisur Rahman, and M. A. Hossain, "Edge computing framework for enabling situation awareness in IoT based smart city," *J. Parallel Distrib. Comput.*, vol. 122, pp. 226–237, Dec. 2018.
[96] H. Wang, C. C. Tan, and Q. Li, "Snoogle: A search engine for pervasive environments," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 8, pp. 1188–1202, Aug. 2010.
[97] F. G. Brundu, L. Rietto, A. Acquaviva, E. Patti, A. Osello, M. D. Giudice, N. Rapetti, A. Krylovskiy, M. Jahn, V. Verda, and E. Guelpa, "IoT software infrastructure for energy management and simulation in smart cities," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 832–840, Apr. 2017.
[98] S. Kolozali, D. Kuemper, R. Tonjes, M. Bermudez-Edo, N. Farajidavar, P. Barnaghi, F. Gao, M. Intizar Ali, A. Mileo, M. Fischer, and T. Iggena, "Observing the pulse of a city: A smart city framework for real-time discovery, federation, and aggregation of data streams," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2651–2668, Apr. 2019.
[99] J. An, F. Le Gall, J. Kim, J. Yun, J. Hwang, M. Bauer, M. Zhao, and J. Song, "Toward global IoT-enabled smart cities interworking using adaptive semantic adapter," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5753–5765, Jun. 2019.
[100] J. Hwang, J. An, A. Aziz, J. Kim, S. Jeong, and J. Song, "Interworking models of smart city with heterogeneous Internet of Things standards," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 74–79, Jun. 2019.
[101] A. Brutti, P. De Sabbata, A. Frascella, N. Gessa, R. Ianniello, C. Novelli, S. Pizzuti, and G. Ponti, "Smart city platform specification: A modular approach to achieve interoperability in smart cities," in *The Internet Things for Smart Urban Ecosystems*. Cham, Switzerland: Springer, 2019, pp. 25–50.
[102] R. Mulero, V. Urosevic, A. Almeida, and C. Tatsiopoulos, "Towards ambient assisted cities using linked data and data analysis," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 5, pp. 1573–1591, Oct. 2018.
[103] R. Mulero, A. Almeida, G. Azkune, P. Abril-Jimenez, M. T. Arredondo Waldmeyer, M. Paramo Castrillo, L. Patrono, P. Rametta, and I. Sergi, "An IoT-aware approach for elderly-friendly cities," *IEEE Access*, vol. 6, pp. 7941–7957, 2018.
[104] D. Minoli, "Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach," *Internet Things*, vol. 10, Jun. 2020, Art. no. 100147.

[105] L. Sánchez, I. Elicegui, J. Cuesta, L. Muñoz, and J. Lanza, "Integration of utilities infrastructures in a future Internet enabled smart city framework," *Sensors*, vol. 13, no. 11, pp. 14438–14465, Oct. 2013.
[106] C. Zhang and J. Beetz, "Querying linked building data using SPARQL with functional extensions," in *Proc. 11th Eur. Conf. Product Process Modelling (ECPPM)*, Limassol, Cyprus, Sep. 2016. [Online]. Available: http://cyprusconferences.org/ecppm2016/
[107] M. Lanthaler and C. Gutl, "A semantic description language for RESTful data services to combat semaphobia," in *Proc. 5th IEEE Int. Conf. Digit. Ecosyst. Technol. (IEEE DEST)*, May 2011, pp. 47–53.
[108] F. Michel, C. Faron-Zucker, O. Corby, and F. Gandon, "Enabling automatic discovery and querying of Web APIs at Web scale using linked data standards," in *Proc. Companion World Wide Web Conf.*, May 2019, pp. 883–892.
[109] T. Espinha, A. Zaidman, and H.-G. Gross, "Web API growing pains: Loosely coupled yet strongly tied," *J. Syst. Softw.*, vol. 100, pp. 27–43, Feb. 2015.
[110] K. Framling, S. Kubler, and A. Buda, "Universal messaging standards for the IoT from a lifecycle management perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 319–327, Aug. 2014.
[111] B. Dave, S. Kubler, K. Främling, and L. Koskela, "Opportunities for enhanced lean construction management using Internet of Things standards," *Autom. Construct.*, vol. 61, pp. 86–97, Jan. 2016.
[112] N. Kolbe, J. Robert, S. Kubler, and Y. Le Traon, "Proficient: Productivity tool for semantic interoperability in an open IoT ecosystem," in *Proc. 14th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, 2018, pp. 116–125.
[113] N. Kolbe, S. Kubler, and Y. Le Traon, "Popularity-driven ontology ranking using qualitative features," in *Proc. Int. Semantic Web Conf.*, 2019, pp. 329–346.
[114] N. Kolbe, P.-Y. Vandenbussche, S. Kubler, and Y. Le Traon, "LOVBench: Ontology ranking benchmark," in *Proc. Web Conf.*, Apr. 2020, pp. 1750–1760.
[115] M. Liu, D. Li, C. Xu, J. Zhou, and W. Huang, "Discovery of multimodal sensor data through webpage exploration," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5232–5245, Jun. 2019.
[116] J. Robert, "D3.9 context-sensitive security, privacy management, adaptation framework v2," Univ. Luxembourg, Luxembourg City, Luxembourg, bIoTope deliverable, Tech. Rep. D3.9, Aug. 2018.
[117] H. Monga, T. Kinnunen, A. Malhi, A. Javed, and K. Främling, "An OAuth-based authentication mechanism for open messaging interface standard," in *Proc. 12th Int. Conf. Agents Artif. Intell.*, Valletta, Malta, 2020, pp. 1–10.
[118] N. Yousefnezhad, R. Filippov, A. Javed, A. Buda, M. Madhikermi, and K. Främling, "Authentication and access control for open messaging interface standard," in *Proc. 14th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, Nov. 2017, pp. 20–27.
[119] C. Shapiro and H. Varian, *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA, USA: Harvard Business Press, 1998.
[120] N. Kolbe, S. Kubler, J. Robert, Y. Le Traon, and A. Zaslavsky, "Towards semantic interoperability in an open IoT ecosystem for connected vehicle services," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–5.
[121] A. Javed, N. Yousefnezhad, J. Robert, K. Heljanko, and K. Framling, "Access time improvement framework for standardized IoT gateways," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 220–226.

ASAD JAVED (Member, IEEE) received the B.S. degree in computer engineering with COMSATS University Islamabad (CUI), Pakistan, in 2013, and the M.Sc. degree in Computer Science (Major: Embedded Systems) from the EIT Digital Master School in 2016, which is the leading open innovation European organization. It was a double degree program with first year of master studies conducted at KTH Royal Institute of Technology, Sweden and the exit year was at Aalto University, Finland. He is currently pursuing the Ph.D. degree in Internet of Things, edge computing, fault-tolerant distributed systems, and cloud technologies with the Department of Computer Science, Aalto University, Finland. His Ph.D. research aims to propose, implement, and evaluate microservices-based IoT applications that are scalable, fault-tolerant, and performance efficient.

SYLVAIN KUBLER (Member, IEEE) received the M.Sc. degree in network systems engineering and the Ph.D. degree in computer science and engineering from the University of Lorraine, France, in 2009 and 2012, respectively. He was a Research Associate with the Interdisciplinary Centre for Security, Reliability, and Trust, University of Luxembourg, from 2015 to 2017, and with Aalto University, from 2013 to 2015. He is currently an Associate Professor with the Research Center for Automatic Control of Nancy (UMR 7039), Université de Lorraine. He was awarded the best thesis in automatic control from the IFAC French Workgroup GdR MACS/Club EEA. He has a leading role in the bIoTope H2020 project (Building an IoT OPen innovation Ecosystem for connected smart objects), which is a 9.6M£ project involving 21 partners amongst which three smart cities (Brussels, Helsinki, and Greater Lyon). He has broad expertise in the IoT, Networking, Interoperability, Context-Awareness, Product Lifecycle Management, Multi-Criteria Decision Making, Fuzzy Logic, and Semantic Web.

AVLEEN MALHI received the Ph.D. and M.Sc. degrees in computer science engineering from Thapar University, India, in 2012 and 2016, respectively. She is currently working as a Postdoctoral Researcher with the Department of Computer Science, Aalto University. She is also employed as Assistant Professor at Thapar University, for four years. She worked on the security of Vehicular Ad-Hoc Networks on an Industry Sponsored project by TATA Consultancy Services India, for four years during her Ph.D. studies. Her research interests include the IoT, machine learning, and information security. She has 17 SCIE journal publications and 20 International conferences mainly in the area of machine learning, the IoT, and security. She also plays a leading role in Business Finland project, eParkly for smart parking management system.

ANTTI NURMINEN received the M.Sc. degree in material physics and the Ph.D. degree (Hons.) in computer science with the topic of Mobile 3D City Maps from the Helsinki University of Technology (TKK), in 1999 and 2009, respectively. In 2011, he was a Postdoctoral Researcher with the HITLab New Zealand. He was three years in the board of Intelligent Traffic Systems Finland, a high-level collaborative organization. He was a Research Fellow with Aalto University from 2015 to 2020. He has been the Project Manager for more than ten EU projects. He coordinated the EU FP7 project CultAR from 2013 to 2015, receiving the grade Excellent Progress from all its reviews. His research interests include mixed reality, computer graphics, real-time large scale IoT systems, and smart cities. He is currently positioned as the CIO of ePiece Ltd.

JÉRÉMY ROBERT received the M.Sc. and Ph.D. degrees in computer science and engineering from the University of Lorraine, France, in 2009 and 2012, respectively. He is currently a Research Associate with the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg. He has broad expertise in industrial and embedded networks since his Ph.D. research focused on the use of switched Ethernet embedded in the future space launchers. Since 2015, his work is more about heterogeneous data communication challenges in the Internet of Things and the implementation of messaging services and high-level data formats. As the major research work was conducted in collaboration with the industry, these skills could be therefore applied in the area of the smart factory (industry 4.0), smart cities.

KARY FRÄMLING (Member, IEEE) is currently working as Full Professor with Umeå University Sweden and as an Adjunct Professor with Aalto University Finland. He is one of the first movers in the space of the IoT and has worked on joint projects with tens of industrial partners, such as BMW and Nokia. He is also the Founder of a successful IoT startup, Control Things. He is also the Founder and the former Chairman of the IoT Work Group of The Open Group, which published the first IoT standards that address all IoT-connected systems on October 16th, 2014: the Open Messaging Interface (O-MI) and Open Data Format (O-DF). The standards were initially developed jointly with leading industrial partners but he is the main architect and author of these standards. The course will benefit from the insights and the network that he can provide and he is committed to this project beyond research and through commercialization.