Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions

José L. Hernández-Ramos | European Commission, Joint Research Centre
Juan A. Martínez | Odin Solutions S.L.
Vincenzo Savarino, Marco Angelini, Vincenzo Napolitano | Engineering Ingegneria Informatica SpA
Antonio F. Skarmeta | University of Murcia
Gianmarco Baldini | European Commission, Joint Research Centre

The digitalization of current urban spaces is realizing the vision of so-called smart cities, where security and privacy concerns could affect citizens' safety. This work discusses potential solutions derived from European Union research efforts to be considered in the coming years.

According to the United Nations (UN), the increase in population and current migratory phenomena will cause two thirds of the world's population to live in cities by 2050.[1] To cope with this global demographic trend, current urban spaces need to be efficiently managed to guarantee a sustainable environment for citizens. For this reason, the concept of a *smart city* emerged a few years ago in response to the need to transform these spaces through an increase of digitalization for the benefit of our societies. In fact, the UN's 2030 Agenda for Sustainable Development explicitly considers Sustainable Cities and Communities (Goal 11) to address this social challenge on a global scale. Because of this trend, cities are becoming the main social and economic hubs of countries around the world.

ISO 37122 (*Sustainable Cities and Communities—Indicators for Smart Cities*) defines a smart city as a "city that increases the pace at which it provides social, economic, and environmental sustainability outcomes and responds to challenges such as climate change, rapid population growth, and political and economic . . . and uses data information and modern technologies to deliver better services and quality of life to those in the city. . . ." Indeed, current technological developments led by the Internet of Things (IoT) are transforming various sectors of today's cities, including energy efficiency and health care, and fostering innovation through inclusive industrialization. These advances are integrated through a heterogeneous infrastructure composed by end devices (e.g., sensors and wearables), and powerful computer systems to monitor the state of a city and

Digital Object Identifier 10.1109/MSEC.2020.3012353
Date of current version: 12 August 2020

make automated decisions accordingly. The resulting ecosystem is realizing the vision of a data-driven society[2] to meet some of the main goals of the UN's 2030 Agenda for Sustainable Development, such as Industry, Innovation, and Infrastructure (Goal 9) or Climate Action (Objective 13).

To encourage the development of smart cities, different initiatives have emerged in recent years, such as the global program United Smart Cities and the European Innovation Partnership on Smart Cities and Communities (EIP-SCC) in the European Union (EU). These efforts consider recent advances in the IoT as key elements to transform current urban spaces. Nevertheless, the interconnection of physical and everyday devices also means an increase in the attack surface as well as a more significant impact on privacy, which can ultimately affect citizens' safety. Indeed, the use of pervasive devices (e.g., smartphones or wearables) generates a huge amount of data; this fact is already exploited by sophisticated artificial intelligence (AI) algorithms, increasing privacy concerns.

Additional aspects include the need to provide interoperable and lightweight mechanisms (including protocols and cryptographic algorithms) to be used even in devices with resource constraints throughout their lifecycles. These mechanisms must offer a high degree of flexibility due to the heterogeneity of current and future communication technologies (e.g., 5G). In addition, these techniques must be complemented with a continuous and automated security evaluation methodology to assess the security level of a certain IoT device or system and automatically react against potential attacks or threats. These aspects are aligned with the current EU initiative for the creation of a cybersecurity certification framework proposed by the recent EU Cybersecurity Act 2019/881. Additional legal restrictions are determined by compliance with the General Data Protection Regulation (GDPR) 2016/679 and other legal instruments that must be addressed to create a secure data-sharing ecosystem for future smart cities.

To cope with these challenges, holistic approaches are needed to address the technical, social, and legal requirements of a smart city. In this direction, we describe the main security and privacy challenges to realizing the notion of an IoT-enabled smart city. The set of challenges has been created based on the previous literature (e.g., Zhang et al.[3]) as well as the authors' experiences in different EU research projects. Based on this expertise, we discuss potential approaches and solutions derived from these initiatives. In particular, we consider the reference architecture developed in the scope of the EU H2020 SynchroniCity project as the baseline. SynchroniCity was a large-scale pilot with the aim of creating a single digital-city market for Europe.

Additionally, we describe the instantiation of the main components of the SynchroniCity architecture that have been developed within the scope of other EU research projects in recent years. Furthermore, as an example of the deployment of these components, we provide an overview of the ongoing ambitious initiative MiMurcia, which is being developed in the Spanish city of Murcia, where some of the components described are being considered to improve security and privacy.

Security and Privacy Requirements in IoT-Enabled Smart Cities

In this section, we describe the top 10 security and privacy requirements to be considered in IoT-enabled smart cities. As already mentioned, this set of requirements is based on previous literature, including the previous work of initiatives (e.g., the Open Web Application Security Project IoT) and institutions [e.g., the EU Agency for Cybersecurity (ENISA)] as well as the authors' experiences in this area.

Secure Communications for Resource-Constrained Devices and Networks

IoT devices (e.g., sensors or video surveillance systems) will be deployed throughout the smart city to sense their surrounding environment and generate data on traffic management, lighting, or pollution. In this context, one of the main challenges is to guarantee the security of the data generated by such devices, especially due to potential resource constraints, such as computing power and memory. Indeed, security protocols and cryptographic algorithms need to be adapted to these devices so that real-time data processing is securely performed.

Additionally, the interconnection of these devices is being materialized by heterogeneous network technologies, including recent low-power WAN technologies (e.g., LoRaWAN). This heterogeneity requires security solutions independent of the underlying technologies to foster interoperable deployments. For this purpose, different standards-developing organizations (SDOs) have proposed different approaches to address security in constrained IoT devices. Specifically, the Internet Engineering Task Force (IETF) has established different working groups to deal with these aspects.[4] However, most of these solutions are not yet widely deployed in today's smart cities.

Automated and Secure Deployment of IoT Devices

The deployment of IoT devices with default insecure configurations can lead to security attacks, such as the well-known Mirai botnet, which took advantage

of default credentials to infect IoT devices. To address this issue, device manufacturers must provide the tools required to facilitate a secure and automated deployment of their devices. Furthermore, users should be able to configure their IoT devices when they are deployed, just as they can configure the security of their laptops or smartphones. Additionally, these devices receive updates and security patches during their lifecycles to cope with new attacks or vulnerabilities. However, many of them lack a user interface, making it difficult to configure their deployment and updating processes. Therefore, there is a need to design automated approaches that ensure a secure deployment of devices in IoT-enabled smart cities. For this purpose, a promising recent approach is the manufacturer usage description (MUD) [IETF request for comments (RFC) 8520], which defines network access control profiles to restrict the communications from/to a certain device.

Continuous Security Assessment

The security levels of IoT devices and infrastructure components will change throughout their lifecycles due to the emergence of new attacks and vulnerabilities. Therefore, the use of automated monitoring, testing, and mitigation tools is essential to address the risks arising from such threats or potential manufacturing or configuration failures. Although the use of intrusion-detection system tools has been widely considered, the security assessment process in IoT-enabled smart cities requires additional measures due to the potential impact of threats.

Indeed, the increasing interconnectivity among devices and systems means that a compromised device can be used to attack other systems in the city, provoking a cascade effect. This could be aggravated due to the involvement of (nonexpert) citizens managing their devices, as previously described. These aspects have received significant interest at the EU level through the Cybersecurity Act initiative, which aims to develop a cybersecurity certification framework to reflect the security level of an information and communications technology (ICT) product, service, or process throughout its lifecycle.

Transparent and Decentralized Data Sharing

The smart city ecosystem requires a reliable and transparent data-sharing platform to enable data-driven services for the benefit of society. Such a platform could be used to share the data detected by IoT devices but also to pool the information of threats and attacks associated with such devices. This way, smart city stakeholders can use this information to identify potential threats to their services and applications. In this context, a potential approach is represented by the use of distributed ledger technologies, such as blockchain,[5] which has attracted huge interest due to its well-known properties of decentralization and immutability. However, the advantages of blockchain could also represent security and privacy concerns, due to the lack of a centralized trust model, that can encourage potential attackers to exploit this feature for malicious purposes. Furthermore, data immutability could represent a conflicting aspect with GDPR principles (Articles 16 and 17), especially if the ledger stores personal data.

Access Control Management and Informed Consent

The need for a transparent data-sharing platform in a smart city requires the development of empowerment tools for citizens to manage their security and privacy. However, as already mentioned, the number of devices to be managed as well as their inherent features (e.g., lack of a user interface) require automated mechanisms to be considered. Indeed, the lack of these mechanisms can make it difficult for users to specify the *consent* and *purpose* of data processing. In this context, traditional access control approaches should evolve toward the definition of usage control policies to define how the information generated by a data provider will be used by data consumers.[6]

An additional challenge is the need to integrate usage control preferences over data that, in many cases, will be combined with data from other sources. In this situation, the use of a standardized mechanism is essential to avoid potential conflicts among restrictions. These mechanisms should be flexible to react upon configuration changes, taking into account the legal principles of current data protection regulations, such as GDPR.

Anonymization of Personal Data

In addition to the different elements deployed in a smart city, a current trend for data collection is to develop *mobile crowdsensing* mechanisms based on the infrastructure created by the devices that are transported by citizens (for example, wearables and smartphones) as well as vehicles and other mobile objects.[7] This trend allows cost savings in terms of infrastructure deployment as well as an increase in the accuracy of the data generated.

However, it can also harm the privacy of citizens, who (in many cases) are not aware of the information being shared by their devices. Therefore, the use of privacy-enhancing techniques, such as anonymous credential systems, can help reconcile massive data collection with privacy requirements. An additional aspect is the need to complement these techniques with tools that foster compliance with current legal instruments. These tools should help to enforce users' consent while a high degree of usability is still provided.

Privacy-Preserving Data Analytics

The data generated in an IoT-enabled smart city are sent to cloud servers for further processing. This way, high-level services are provided by identifying patterns in large amounts of data to design automated decision-making processes. However, with the use of machine learning techniques, such systems become attractive targets through the use of adversarial machine learning, which may lead AI-based systems to false and potentially damaging outcomes. Additionally, the use of these techniques raises privacy concerns, since new information is obtained without the explicit consent of citizens. In this context, the use of differential privacy techniques must be complemented by cryptographic mechanisms, such as secure multiparty computation and homomorphic encryption, to reconcile citizens' privacy needs.

However, the computational requirements of these techniques can represent an obstacle to deal with huge amounts of data. Moreover, data analytics techniques can have social, legal, and ethical implications, as companies can monetize citizens' data by allowing third parties to manage this information. These implications require a tradeoff between existing regulations (e.g., GDPR) and initiatives to support a sustainable business model for smart cities.

Interoperable and Secure Data Formats

The data obtained in the previous process are then shared through the smart city infrastructure to a platform for the realization of high-level services. The concept of an IoT platform is usually considered to designate a set of infrastructure components to share the information generated by IoT devices and systems. In this context, a key aspect is to ensure interoperability regarding the representation of raw data and information coming from different sources while properly protecting them.

Interoperability challenges can be exacerbated by the need to interconnect different data platforms with different representation formats and implementations. In a large-scale smart city deployment, different platforms need to be interconnected to foster the sharing of information among different systems, areas, or contexts. In fact, this interconnection or federation of platforms allows the data obtained by different sensors in a local environment (for example, a certain street) to be used to predict or explain phenomena on a global scale with respect to energy efficiency or climate change.

Enforcement of Current Security and Privacy Regulations

A strongly digitalized smart city needs to be adequately regulated. At the EU level, GDPR was adopted in 2016 and has been applicable since 2018. GDPR proposes a framework for data protection through a set of principles regarding the processing of personal data (Article 5). In addition, it describes the rights of a data subject (i.e., the individual associated with certain personal data) as well as the obligations of a data controller, that is, the entity that determines the purpose of the processing of personal data (Chapter 4).

Furthermore, GDPR advocates data protection by design and by default (Article 25). In particular, it determines the need for technical and organizational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed. For this purpose, the use of techniques such as pseudonymization, encryption, aggregation, or data usage control needs to be considered to guarantee the compliance of GDPR and other legal instruments in IoT-enabled smart cities.

Cybersecurity Awareness

According to the literature analysis and our own experience in EU initiatives, we often perceive a lack of user awareness campaigns on cybersecurity risks related to the IoT. In this direction, the recent EU Cybersecurity Act advocates the need to promote concrete actions through good practices for citizens, organizations, and businesses in awareness, education, and cyberhygiene (Article 10). Additionally, a recent ENISA report[8] emphasizes the need for awareness initiatives to encourage the deployment of trustworthy IoT scenarios.

It should be noted that an increase in awareness initiatives will be crucial for a secure deployment of IoT-enabled smart cities. Indeed, citizens play an active role in the provision of data through their devices. As demonstrated by well-known attacks (e.g., the Mirai botnet), compromised IoT devices can be used to launch attacks against ICT systems and critical infrastructures. Therefore, the lack of awareness of a single citizen could represent security and privacy risks affecting other systems and citizens in a smart city.

A Reference Architecture for Secure and Privacy-Aware IoT-Enabled Smart Cities

Based on the 10 requirements for security and privacy in IoT-enabled smart cities, this section describes the results from different EU research projects addressing such needs.

The SynchroniCity Approach

In recent years, different reference architectures have been proposed for addressing security and privacy in IoT scenarios, such as the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) IoT reference model (recommendation

ITU-T Y.20604) and IEEE *Standard for an Architectural Framework for the Internet of Things (IoT)*. Based on these efforts, a recent approach has been carried out in the scope of the H2020 SynchroniCity project (grant agreement ID 732240) funded under the European IoT Large-Scale Pilots Program. SynchroniCity was intended to develop a single digital-city market for Europe by piloting its foundations in 11 cities. Unlike previous initiatives, the SynchroniCity architecture is focused on addressing security and privacy aspects in IoT-enabled smart cities.

Figure 1 shows the SynchroniCity reference architecture that includes different high-level logical components and their functionalities. For the realization of such a framework, the analysis focused on the relevant standards and technologies of SDO initiatives, EU partnership programs, and EU research projects. The SynchroniCity framework is built around the Open & Agile Smart Cities initiative's "minimal interoperability mechanisms" (MIMs), which provide the technical foundation for the procurement and deployment of IoT-enabled services for cities and communities. The MIMs are vendor neutral and technology agnostic, and they can be integrated with existing systems. The implementation of the MIMs can vary, but every technical architecture must use the same interoperability mechanisms.

The architecture embraces different modules, including

- *Context Data Management*, which manages the context information coming from different sources.
- *IoT Management* to deal with the heterogeneity of IoT devices.
- *Data Storage Management*, which addresses the data storage and access of devices and the city platform.
- *IoT Data Marketplace*, which supports business interactions between data providers and consumers.
- *Monitoring and Platform Management*, which provides the functionality required to manage and monitor the activities provided by different services.
- *Security, Privacy, and Governance*, which is intended to provide basic security and privacy properties for IoT data, infrastructure, and platform services.

It should be noted that, while different aspects of the framework have been addressed in SynchroniCity and other EU research projects, we focus on the *Security, Privacy, and Governance* module. In particular, this module contains a set of submodules aimed to ensure data protection and privacy, identity management, and authentication and authorization for citizens and devices accessing information. The *Data Protection and Privacy* submodule is intended to ensure flexible security and privacy capabilities for different smart city use cases. It provides support for confidentiality, integrity, authentication, immutability, and nonrepudiation as well as cryptographic mechanisms to authenticate and secure the communication and storage of data. These aspects are aligned with the enforcement of privacy-by-design principles, and compliance with GDPR requirements by empowering citizens to control their personal data.

Furthermore, the *Identity Management* submodule is focused on identification aspects of users and services, such as identity federation and single sign-on (SSO) features. Then, the *Authentication, Authorization, and Accounting* (*AAA*) submodule provides AAA capabilities. It is aimed to enforce conditions defining whether users have access to specific resources while also storing access information for audit purposes. Moreover, the *Policy Management* submodule provides a unified policy management regarding the access, privacy, and governance of the SynchroniCity framework. This component is intended to define security and privacy policies independently of underlying technologies.

Instantiating SynchroniCity Components

The different security and privacy aspects highlighted by SynchroniCity have been considered by different EU research projects in recent years. To realize the functionality of the *Data Protection and Privacy* submodule, IoTCrawler (grant agreement ID 779852) is an ongoing project to develop an innovative, secure, and privacy-aware search engine for the IoT. The project considers the use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE)[9] to define encryption policies based on a combination of identity attributes. This way, only entities with cryptographic keys satisfying that policy will access the encrypted data. While CP-ABE was already considered in the scope of the EU projects SOCIOTAL (grant agreement ID 609112) and SMARTIE (grant agreement ID 609062), the use of CP-ABE in an IoT-enabled smart city copes with the requirements about access control (see the "Access Control Management and Informed Consent" section) and supports the enforcement of data protection regulations (see the "Enforcement of Current Security and Privacy Regulations" section).

In addition, the EU project CPaaS.io (grant agreement ID 723076) was also focused on security and privacy aspects in smart cities. As part of the project activities, the *personal data store* component was proposed to specify which services can have access to specific attributes of users' sensitive data as well as to revoke such decisions at any time. Additional privacy-preserving techniques are being considered in the H2020 Fed4IoT project (grant agreement ID

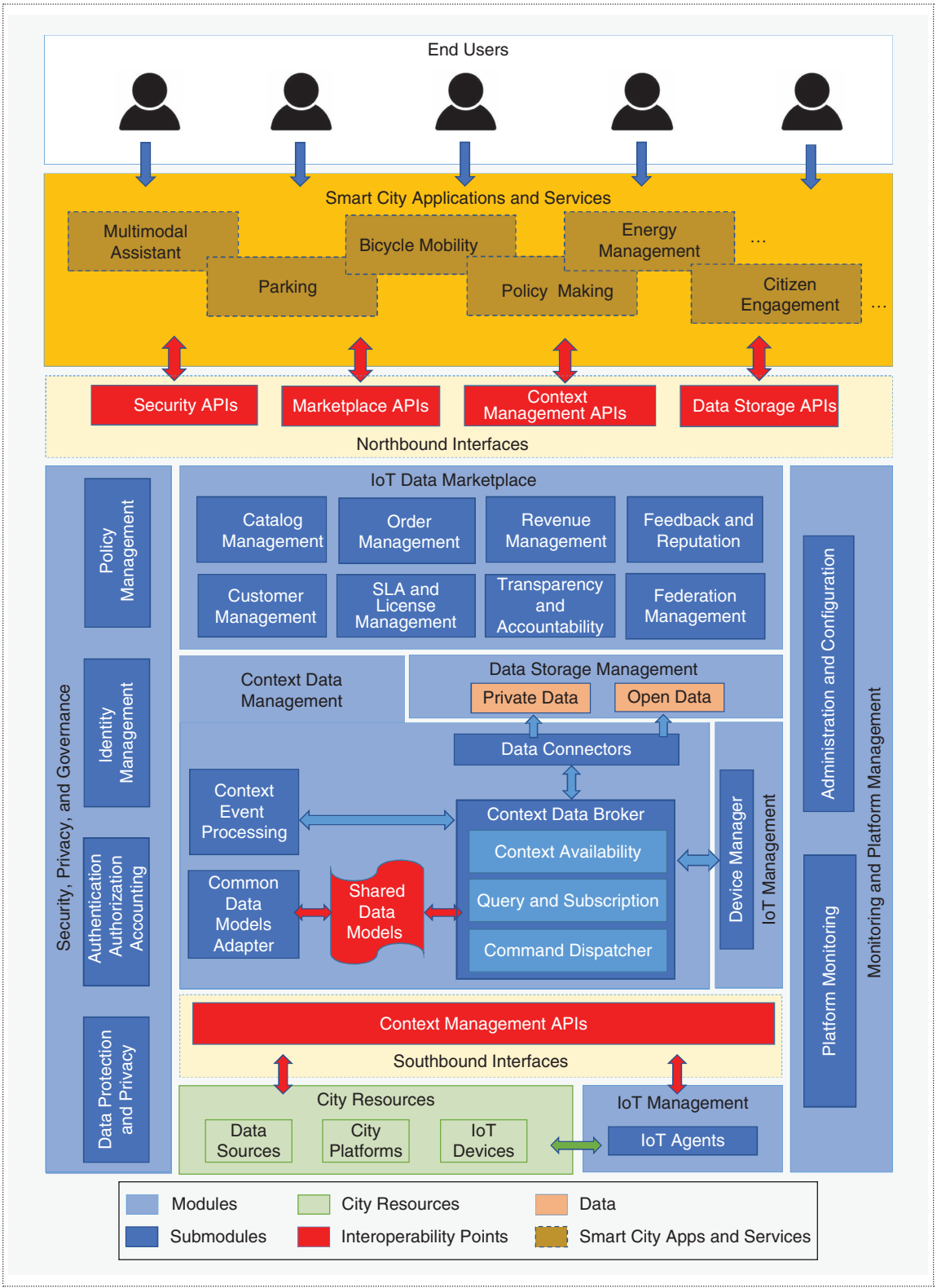

Figure 1. The SynchroniCity reference architecture. API: application programming interface; SLA: service level agreement. (Source: Synchronicity Project; used with permission.)

814918), such as the use of homomorphic encryption to operate with encrypted data coming from IoT devices (see the "Privacy-Preserving Data Analytics" section).

In the case of the *Identity Management* submodule, the most widely considered implementation is represented by the use of the FIWARE initiative, which provides an EU platform providing different middleware implementations. In particular, the Keyrock identity management system is based on standard protocols to manage users' access to services and applications. This system is also in charge of users' profile management, and more advanced features, such as SSO and identity federation. In addition to this implementation, privacy-preserving aspects were considered in the SOCIOTAL project by using anonymous credential systems, such as Idemix,[10] which aims to minimize the disclosure of personal data. Idemix is based on zero-knowledge proofs for privacy-preserving identity management. The use of this approach is intended to cope with the challenges described in the "Anonymization of Personal Data" and "Enforcement of Current Security and Privacy Regulations" sections.

Furthermore, the functionality provided by the *AAA* submodule has also been considered in different projects. For example, the use of the Constrained Application Protocol (CoAP) (IETF RFC 7252) was considered in the scope of the SMARTIE and IoTCrawler projects to transport Extensible Authentication Protocol (EAP) (IETF RFC 3748) messages. The approach was also integrated with an AAA infrastructure for a secure deployment of IoT devices (see the "Automated and Secure Deployment of IoT Devices" section).

Furthermore, other technologies have been proposed for authentication and authorization purposes in IoT-related EU projects. In particular, the Datagram Transport Layer Security protocol (IETF RFC 6347) was deployed in the same project and CPaas.io to ensure channel protection in the communications between devices and systems II-A. More focused on authorization aspects, projects such as SMARTIE and IoTCrawler analyzed the use of lightweight access control tokens by using a capability-based access control model.[11] This mechanism follows a similar approach to the use of JavaScript Object Notation Web Tokens (IETF RFC 7519), in which access privileges are included in the token to be validated by resource-constrained IoT devices (see the "Secure Communications for Resource-Constrained Devices and Networks" and "Access Control Management and Informed Consent" sections).

For the Policy Management submodule, the use of the eXtensible Access Control Markup Language (XACML) [Organization for the Advancement of Structured Information Standards (OASIS)] has been proposed in different projects, including SOCIOTAL and IoTCrawler. XACML defines access control policies based on the triple subject/resource/action, in which components can be defined based on the combination of attributes defined in the *Identity Management* submodule. In the case of IoTCrawler, this policy-based approach is combined with the mentioned capability-based authorization tokens. The resulting approach has been combined with the use of blockchain by using smart contracts (see the "Transparent and Decentralized Data Sharing" section). This way, IoTCrawler covers authorization aspects for a distributed scenario where different IoT platforms agree for specific authorization policies that must be employed in the whole IoTCrawler framework.

In addition to the *Security, Privacy, and Governance* module, other aspects of the SynchroniCity framework have been addressed by EU research initiatives. In the case of the *Context Data Management* module, several projects consider the use of the Orion Context Broker, which is provided by FIWARE to serve as a central component for sharing devices' data. This component uses the Open Mobile Alliance (OMA) Next Generation Services Interface (OMA-NGSI) to represent such information.

For example, IoTCrawler defines mechanisms based on NGSI linked data (NGSI-LD) to foster the interoperability among different IoT platforms (see the "Interoperable and Secure Data Formats" section). Furthermore, Fed4IoT is focused on the federation of heterogeneous IoT platforms that could use different technologies for accessing the information. The approach is based on the concepts of *Virtual Thing* and NGSI-LD to create a common representation framework independent of the underlying technology. This approach also integrates XACML and CP-ABE techniques.

Moreover, the *Monitoring and Platform Management* submodule has been addressed in other initiatives, such as the H2020 EU COMPACT project (grant agreement ID 740712), which was focused on empowering local public administrations to deal with cyber resilience aspects. The approach is based on a specialization of the Plan–Do–Check–Act strategy to monitor the security level of different systems in a smart city (see the "Continuous Security Assessment" section). In particular, the toolset provided by COMPACT includes techniques for risk assessment, awareness and training, security monitoring, and information-sharing tools.

In the "Plan phase," the information provided by a security operation center is used to estimate a risk profile. Then, in the "Do phase," the risk profile is

treated using security guidelines, best practices, training, and gamification (see the "Cybersecurity Awareness" section). Furthermore, in the "Check phase," the effectiveness of the risk treatment is monitored to detect weaknesses in the adopted risk treatment strategies. Finally, in the "Act phase," countermeasures and risk treatment strategies are implemented. In addition to COMPACT, the H2020 EU ARMOUR project (grant agreement ID 688237) proposed the use of security assessment techniques based on the European Telecommunications Standards Institute (ETSI) "Risk-Based Security Assessment and Testing Methodologies" (ETSI EG 203 251 V1.1.1).

Deploying Security and Privacy in Smart Cities: The Case of MiMurcia

This section uses the smart city project of the city of Murcia to show an example of a real scenario in which some of the components described are being considered to enhance security and privacy aspects in an IoT-enabled smart city. Murcia is a city located in the southeast of Spain; it has a population of approximately 650,000 and is currently implementing different actions according to the smart city project called MiMurcia. This project was selected from the Second Call for Intelligent Cities of the Digital Agenda for Spain by the Spanish Ministry of Energy, Tourism, and Digital Agenda with a total budget of about 8 million euros.

This ambitious project is focused on the integration and coordination of different areas and sectors in the city, including public street lighting, parks and gardens management, public transport (bus, tram, and bicycles), traffic management, tourism, and e-administration, among other services. As an illustration of such integration, Figure 2 shows a map-based webpage including information about different resources and entities in the city, such as buses, trams, or bicycle parking lots, which are geolocalized in Murcia. Additional information can be obtained by clicking over each entity, such as the bus identifier, the bus line to which it belongs, or the availability of a bicycle parking lot.

It should be noted that the different services provided in the city could potentially include sensitive information. Therefore, the use of suitable security and privacy techniques is essential to ensure the trustworthy development of such smart city services. For example, the management of water resources is crucial in Murcia. Because of its location and topology, the city has approximately 330 sunny days per year and, consequently, very scarce water resources compared to other regions in Spain. Another aspect is the air quality management due to the increase in the levels of carbon monoxide and CO_2 as well as the presence of other substances as a consequence of the high number of vehicles and growing factory activity. In both cases, there is a need to ensure that the information generated by sensors in the city is coming from legitimate and authorized entities so that the information is completely reliable.

The information generated by the different devices is sent to the smart city platform through different IoT gateways, which are used to check the authentication and authorization aspects of such devices. For this purpose, devices and gateways make use of CoAP–EAP to enable a secure deployment of IoT devices in the city. The platform integrates an AAA infrastructure to increase the scalability level of the solution by authenticating the devices. Furthermore, the use of EAP fosters a flexible approach in which different authentication methods can be used to cope with the heterogeneity of current IoT devices and systems.

After being securely deployed, access to the platform to provide/obtain the information is managed by the combination of XACML (for policy management purposes) and the use of capability tokens,[11] which are generated according to the authorization decision based on the XACML policy evaluation. The main goal of this integration is to foster a simple access control management, while at the same time, authorization credentials can be used by end devices. This way, only authenticated devices with the corresponding token will be able to access the smart city platform. A similar approach is also applied to citizens for access to such information.

Other services, such as e-administration procedures and the geolocalization information of resources, could give rise to privacy concerns. For this reason, the use of these services requires additional techniques to ensure only certain city stakeholders are able to access the information. For example, the information related to the location of bicycles could be available only to the company providing the service to ensure a responsible use of the bicycles.

However, disclosing the geolocalization data of this resource could harm citizens' privacy if this information is accessible to other users or services. In this case, the use of CP-ABE is considered to provide a high level of flexibility in terms of policy definition by using different identity attributes. This way, only the users or services (e.g., the bicycle rental service) with identity attributes satisfying such a policy will be able to decrypt the information, thus preserving the privacy of data in the smart city platform. This encryption technique is integrated with the access control technologies previously discussed. Communication with the smart city platform is based on the approach employed in the mentioned EU research projects by using FIWARE components (i.e., based on NGSI).

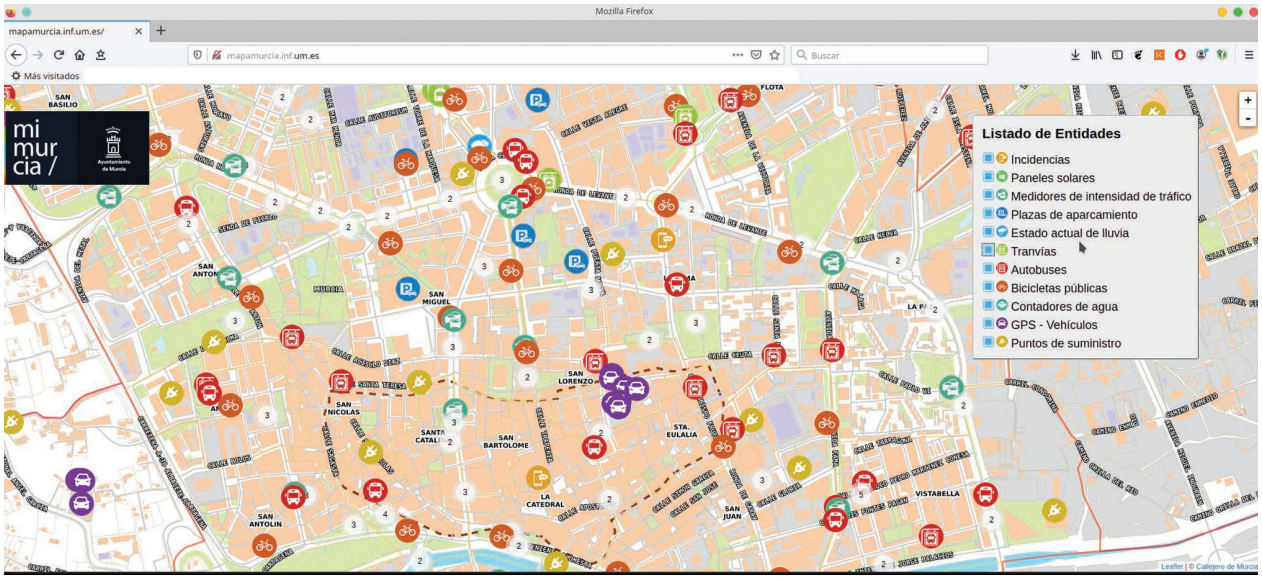

Figure 2. A screenshot of the MiMurcia web-based application presenting the integration of heterogeneous information.

These examples provide an overview of the different approaches that are being currently considered in the MiMurcia project to deal with some of the main requirements discussed in the "Security and Privacy Requirements in IoT-Enabled Smart Cities" section. The current implementation will evolve during the implementation of the MiMurcia project by extending such developments, which will be integrated with additional techniques to ensure security and privacy for the services provided in the city.

Analysis and Future Research Directions

The realization of secure and privacy-aware IoT-enabled smart cities requires coordinated efforts addressing technical, social, and legal challenges. The concept of the smart city has attracted a strong interest worldwide. In addition to the United Smart Cities global program and the EIP-SCC initiative at the EU level, other efforts have been recently created, such as the Digital Transition Partnership of the Urban Agenda for the EU and the Digital Cities initiative, which has recently evolved into the 100 Intelligent Cities Challenge program.

In the United States, the SmartAmerica program was established by the White House to create an innovation ecosystem with about 100 stakeholders. Then, the Global City Teams Challenge initiative was launched by the National Institute of Standards and Technology (NIST) as a collaboration platform between different stakeholders for the development of emerging technologies in smart cities. In this context, there is a need to promote cooperation and dialogue among these initiatives as well as the use of standard technologies to encourage the creation of a common framework addressing security and privacy in smart cities.

Based on these initiatives, one of the main concepts associated with the development of smart cities is *hyperconnectivity*, which is promoting the development of a data-driven society. With the adoption of new communication technologies and protocols, devices and systems can be ubiquitously accessed. A smart city can be considered a data-driven ecosystem that makes use of the data generated by different sources to provide services that improve citizens' lives. In this context, in addition to the IoT, different technological advances are being considered, especially around 5G technologies, blockchain, and AI,[2] that increase security and privacy concerns. In particular, the development of 5G technologies enables the communication of large amounts of data, raising security concerns.

Although there are initiatives for the deployment of 5G in several cities worldwide, the application of security mechanisms and cryptographic algorithms must meet scalability requirements and deal with the heterogeneity of the devices to be connected. Indeed, the security approaches previously described in current smart city initiatives might need to be adapted for a 5G-enabled smart city. Moreover, blockchain can enable a transparent and decentralized data-sharing ecosystem, which can be used to encourage the development of the recently announced European Data Strategy. However, despite its well-known advantages, the immutability of the data may be in conflict with the requirements established by GDPR.

An additional aspect is that different companies or institutions may need to interconnect their blockchain

implementations with different security and privacy requirements. In this context, it is essential to ensure compliance with these requirements while achieving a high degree of interoperability. For this purpose, recent *interledger* approaches[12] need to be further investigated for interconnecting ledgers of different smart cities. Regarding the use of AI algorithms, these techniques are a double-edged sword; while they can help to detect possible attacks or vulnerabilities in a system by analyzing data traffic, attackers can use such techniques to launch sophisticated attacks over devices and systems in a smart city. Furthermore, the use of personal data in automated decision-making systems enabled by AI can have severe consequences for citizens' rights. This is exacerbated by the lack of explainability of AI techniques that could be opaque to humans. For this purpose, transparency, reliability, and data protection should be encouraged to ensure that AI techniques adhere to current security and privacy regulations.

An additional aspect to be considered is the involvement of citizens for the deployment and management of their devices in a smart city. As mentioned, a single compromised IoT device could be used to launch security attacks against other devices, services, or infrastructure in a smart city. Therefore, it is necessary to ensure the secure deployment and management of IoT devices throughout their lifecycles. It is necessary for device manufacturers to be increasingly involved in the promotion of automated solutions that guarantee the intended operation of each device.

In this context, the use of recent approaches such as the IETF standard MUD (IETF RFC 8520) can foster an automated and secure deployment of IoT devices. MUD is used to describe the intended use of a device by restricting the communication from/to such device. This approach has attracted significant interest in recent years from different SDOs, especially the NIST,[13] which describes how MUD can reduce the vulnerability of IoT devices to botnets and other network-based threats. Indeed, the integration of the MUD standard with previous approaches for the secure deployment of IoT devices (e.g., based on CoAP) has been recently considered.[14] However, MUD is not yet widely used by manufacturers.

The use of automated security approaches can enhance the process of continuous security assessment of IoT devices. These aspects are considered in the recent Cybersecurity Act regulation, which is intended to create a cybersecurity certification framework for ICT products, services, and processes. The deployment of certified devices and systems could increase citizens' trust in using smart city services. In this context, the use of methodologies such as the "Risk-Based Security Assessment and Testing Methodologies" from the ETSI was considered in our previous work,[15] which represents a promising starting point for automated security assessment in the IoT. However, the certification of IoT devices and systems poses new challenges and requirements that need to be addressed in the coming years to realize secure and privacy-aware IoT-enabled smart cities.

The concept of the smart city represents one of the main pillars of the next digital era to improve citizens' lives. Current technological improvements are turning current urban spaces into digitized environments to provide data-driven services. In this context, we described the main security and privacy challenges in a smart city ecosystem as well as different EU efforts addressing such needs. Our work analyzed technical security and privacy solutions as well as social and regulatory aspects.

Based on this analysis, despite the current efforts and initiatives across the world, the current landscape of smart cities still poses technical, social, and legal challenges that must be addressed in the coming years. With the development of new emerging technologies, including 5G, blockchain, and AI techniques, these challenges will require an adaptation of current technical and regulatory solutions to ensure trustworthy smart cities for the benefit of society.

Acknowledgments

This work was partially funded by the European Commission through the projects H2020-830929 CyberSec4Europe, H2020-779852 IoTCrawler, and H2020-780139 SerIoT. ■

References

1. D. o. E. United Nations and P. D. Social Affairs, "World urbanization prospects: The 2018 revision," United Nations, New York, 2019. [Online]. Available: https://population.un.org/wup/Publications/Files/WUP2018-Report.pdf
2. J. L. H. Ramos, D. Geneiatakis, I. Kounelis, G. Steri, and I. N. Fovino, "Toward a data-driven society: A technological perspective on the development of cybersecurity and data-protection policies," *IEEE Security Privacy*, vol. 18, no. 1, pp. 28–38, 2020. doi: 10.1109/MSEC.2019.2939728.
3. 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, 2017. doi: 10.1109/MCOM.2017.1600267CM.
4. H. Tschofenig and E. Baccelli, "Cyberphysical security for the masses: A survey of the internet protocol suite for internet of things security," *IEEE Security Privacy*, vol. 17, no. 5, pp. 47–57, 2019. doi: 10.1109/MSEC.2019.2923973.

5. J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 2019. doi: 10.1109/COMST.2019.2899617.
6. R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, and A. R. Biswas, "An agent-based framework for informed consent in the internet of things," in *Proc. 2015 IEEE 2nd World Forum Internet of Things (WF-IoT)*, pp. 789–794. doi: 10.1109/WF-IoT.2015.7389154.
7. Y. Liu, L. Kong, and G. Chen, "Data-oriented mobile crowdsensing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2849–2885, 2019. doi: 10.1109/COMST.2019.2910855.
8. "Good practices for security of IoT: Secure software development lifecycle," European Union Agency for Cybersecurity, Heraklion, Greece, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
9. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. 2007 IEEE Symp. Security and Privacy (SP'07)*, pp. 321–334. doi: 10.1109/SP.2007.11.
10. J. B. Bernabé, J. L. H. Ramos, and A. F. Gómez-Skarmeta, "Holistic privacy-preserving identity management system for the internet of things," *Mobile Inf. Syst.*, vol. 2017, Aug. 2017, Art. no. 6384186. doi: 10.1155/2017/6384186.
11. J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta Gómez, "DCapBAC: Embedding authorization logic into smart things through ECC optimizations," *Int. J. Comput. Math.*, vol. 93, no. 2, pp. 345–366, 2016. doi: 10.1080/00207160.2014.915316.
12. V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger approaches," *IEEE Access*, vol. 7, pp. 89,948–89,966, July 2019. doi: 10.1109/ACCESS.2019.2926880.
13. "Securing small-business and home Internet of Things (IoT) devices," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 1800-15, 2019.
14. S. N. Matheu et al., "Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems," *Sensors*, vol. 20, no. 7, p. 1882, 2020. doi: 10.3390/s20071882.
15. S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a cybersecurity certification framework for the Internet of Things," *IEEE Security Privacy*, vol. 17, no. 3, pp. 66–76, 2019. doi: 10.1109/MSEC.2019.2904475.

José L. Hernández-Ramos is a scientific project officer at the Joint Research Centre of the European Commission. His research interests include the application of security and privacy mechanisms in the Internet of Things and transport systems scenarios. Hernández-Ramos received a Ph.D. in computer science from the University of Murcia, Spain. He has served as a technical program committee and chair member for different international conferences. Contact him at jose-luis.hernandez-ramos@ec.europa.eu.

Juan A. Martínez is a senior researcher and research project coordinator at Odin Solutions S.L. His research interests include the Internet of Things (IoT) domain, including security and access control, applied to the scope of agriculture and smart cities. Martínez received a Ph.D. in computer science from the University of Murcia in 2015. He has participated in different European and national research projects related to the IoT in different domains, such as SMARTIE, CPaaS.IO, ARMOUR, IoTCrawler, and Fed4IoT. Contact him at jamartinez@odins.es.

Vincenzo Savarino is a senior researcher at Engineering Ingegneria Informatica SpA. His research interests include privacy-enhancing technologies, blockchain, business and process modeling, and human–computer interaction. Savarino received a laurea in computer engineering from the Università degli Studi di Palermo. Since 2004, he has been involved in several research projects financed by both the Italian Ministry of University and Research and the European Community. He is the responsible for the smart cities pilot in the Cybersec4Europe project. Contact him at vincenzo.savarino@eng.it.

Marco Angelini has been with Engineering Ingegneria Informatica SpA R&D labs since 2014. Angelini received a laurea in computer engineering from the University of Rome II. He has been involved in national and H2020 European Union projects, such as HERMENEUT and COMPACT. He is now coordinating the engineering research team involved in the CyberSec4Europe project, with a focus on cybersecurity for smart cities. Contact him at marco.angelini@eng.it.

Vincenzo Napolitano is a cybersecurity researcher with Engineering Ingegneria Informatica SpA. His research interests include social engineering vulnerability assessment, gamification of the cyberawareness training programs, cyberthreat intelligence, cybervulnerability assessment, and risk modeling. Napolitano received a laurea in computer engineering from the University of Salerno. Since 2014, he has been involved in several H2020 research projects, such as Cybersec4Europe. Contact him at vincenzo.napolitano@eng.it.

Antonio F. Skarmeta is a full professor and has been the head of the Research Group ANTS at the University

of Murcia since its creation in 1995. His research interests include the integration of security services, identity, the Internet of Things (IoT), and smart cities. Skarmeta received a Ph.D. in computer science from the University of Murcia, Spain. Since 2014, he has been the Spanish National Representative for the Marie Skłodowska-Curie Actions within H2020. He has worked on and coordinated different European Union research projects in the IoT area, such as SMARTIE, SOCIOTAL, IoT6, and IoTCrawler. Contact him at skarmeta@um.es.

Gianmarco Baldini has worked as a scientific project manager at the Joint Research Centre of the European Commission since 2007. His research interests include wireless communications, security, positioning, and machine learning, and he contributed to the formulation of European policies in the areas of the radio-frequency spectrum, road transportation, and cybersecurity. Baldini received a laurea in electronic engineering from the University of Rome in 1993. Contact him at gianmarco.baldini@ec.europa.eu.