IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 October 2023, accepted 6 November 2023, date of publication 9 November 2023,
date of current version 21 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3331820

RESEARCH ARTICLE

Privacy and Security Best Practices for IoT Solutions

MATTEO ANEDDA[1], (Senior Member, IEEE), ALESSANDRO FLORIS[1], (Member, IEEE), ROBERTO GIRAU[2], (Member, IEEE), MAURO FADDA[3], (Senior Member, IEEE), PIETRO RUIU[3], MASSIMO FARINA[1], ALESSANDRO BONU[1], AND DANIELE D. GIUSTO[1], (Senior Member, IEEE)

[1]Department of Electrical and Electronic Engineering (UdR CNIT of Cagliari), University of Cagliari, 09123 Cagliari, Italy
[2]Department of Computer Science and Engineering (DISI), University of Bologna, 40126 Bologna, Italy
[3]Department of Biomedical Science, University of Sassari, 07100 Sassari, Italy

Corresponding author: Matteo Anedda (matteo.anedda@unica.it)

This work was supported in part by the Research and Development Project Piano Nazionale di Ripresa e Resilienza (PNRR)-Partenariato Esteso-RETURN "Multi Risk Science for Resilient Communities Under a Changing Climate" Ministry of Education and Merit (M.I.U.R) under Grant PE00000005, in part by the "Bando Fondazione di Sardegna 2022–2023," and in part by the Piano Operativo Nazionale (PON) "Ricerca e Innovazione" 2014–2020 (PON R&I) "Azione IV.4 Dottorati e contratti di ricerca su tematiche dell'innovazione."

ABSTRACT The rapid increase in Internet of Things (IoT) applications has raised security and privacy issues due to the huge amount of data acquired by IoT devices and transmitted through the Internet. Therefore, there is a need to understand what strategies should be applied to make IoT systems robust to security flaws and privacy weaknesses. In this paper, we first identify and discuss the best practices for IoT privacy and security, which include a set of procedures that can be taken as the guidelines to determine and solve privacy and security issues of IoT systems. Then, we follow and apply the identified best practices to two real IoT-based use cases: a crowding monitoring system and a vehicular mobility system. Finally, we computed the risk assessment score to evaluate the impact of the application of the identified best practices on the implemented IoT systems. We observe that following the proposed best practices the implemented IoT systems achieve an overall risk score of 1.3, which is from 215% to 361% lower than that achieved by comparable IoT systems proposed in the literature studies.

INDEX TERMS Internet of Things, IoT security, best practices, non-personal data, privacy by design, risk assessment.

I. INTRODUCTION

Telecommunications technologies and services have rapidly evolved in the last decades, causing the need for new regulations concerning the treatment of personal and non-personal data. Nowadays, the Internet of Things (IoT) technology allows heterogeneous objects (e.g., traffic lights, cars, watches, surveillance cameras, etc.) to communicate with each other through the Internet. It appears evident that with the evolution of telecommunications services, there is an exponential increase in the number of data producers and data consumers [1]. Accordingly, there is an increase in the types of data exchanged, which involve non-personal as well as personal data. Moreover, with the IoT revolution, the subjects involved in the data communication process are not only humans but also objects and machines. According to Paloalto's report released in 2020, 98% of the overall IoT traffic is unencrypted, exposing personal and confidential data on the Internet [2]. Moreover, 57% of IoT devices in the world are vulnerable to attacks whose severity was ranked medium to high. Thus, it is essential to understand how data exchange of IoT applications must be treated to protect the privacy and security of the users.

The interplay between things, objects, and people allows the datafication process, which transforms people's actions into data. Indeed, as there is a strict conjunction between

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

things and human beings, daily actions and behaviors of people (e.g., sleeping, working, playing sports) can be datified. This is possible, for example, by acquiring, tracing, and mapping people's positions and movements through smartphones, smartwatches, social networks, and other smart devices [3]. In this context, it is important to distinguish between personal and non-personal data, which can be predicted from the data producer. Indeed, the source of data production constitutes a useful guideline to discover the personal or non-personal nature of the data collected. In the IoT world, data sources can be both the user and the connected object. In the first case, data are definitely personal data belonging to the owner of the object. In the second case, data produced by the object can be personal data (if data related to the owner of the object is collected) or non-personal data, such as simple technical data (e.g., the level of oil in the engine of a vehicle or the power consumed by a household appliance) [4].

The technological evolution of telecommunications, in terms of the capillarity of the network, type, and amount of data to be transmitted and stored, has brought the need for an evolution even from a legal and regulatory point of view. Indeed, an identifiable and localizable IoT raises issues related to the processing of personal data and the protection of data subjects to which the information refers. From the common use objects (i.e., smartphone, tablet, own vehicle, connected IoT objects in smart house environment), it is possible to trace people, their position, habits, and behavior. Today, security is seen in scenarios such as roads, cars, and homes, as well as the ever-increasing production and consumption of products. In this context, IoT solutions provide valuable data and insights that improve the way people work and live. IoT security is the practice of keeping IoT systems safe [5], i.e., protecting the IoT system from IoT security threats, such as authentication, confidentiality, integrity, and availability [6], [7].

The design and development of security and privacy management schemes for IoT devices are guided by factors like good performance, low power consumption, robustness to attacks, tampering of the data, and end-to-end security. Security schemes in IoT provide unauthorized access to information or other objects by protecting against alterations or destruction. Privacy schemes maintain the right to control the collected information for its usage and purpose.

To the best of the author's knowledge, current literature studies provide discussion and analysis of major IoT security- and privacy-related issues and threats [6], [7], [8]. However, these studies do not provide general indications to protect an IoT system from the surveyed threats. Also, they do not provide risk evaluation based on real systems physically installed in the smart city environment. Therefore, the main goal of this work is focused on best practices for privacy in IoT with the adoption of privacy-protecting solutions, and best practices for risk and security in IoT, both according to recent guidelines of the National Institute of Standards and Technology (NIST) [9] and to the European GDPR privacy regulation.

The purpose of this paper is to interpret, develop, and apply some essential best practices solutions on critical key aspects:

- data encryption to translate data from plaintext (unencrypted) to ciphertext (encrypted) by providing data integrity, authentication, and non-repudiation;
- data pseudonymization for removing identifying information from snippets data;
- to assess and to understand the security risk in the most modern and complex IoT ecosystems;
- the diversity of the data considered, the computational capacity of the devices and the cybersecurity solutions that unfortunately are not unique and do not offer similar protection for all possible variants of IoT implementations;
- each hardware and software element need to be evaluated in order to assess the overall risk and the risk of the individual elements that make up the chain of the entire system.

The main contributions of this paper are as follows. We have identified and discussed the best practices for IoT privacy and security, which include a set of procedures in accordance with the NIST guidelines and the European GDPR regulation. These best practices can be taken as guidelines to prevent and solve privacy and security issues when designing IoT-based systems. We have implemented two real IoT-based use cases (a crowding monitoring system and a vehicular mobility system) by following and applying the identified best practices to minimize security and privacy issues for these systems. Finally, we have conducted a risk analysis assessment to evaluate the impact of the application of the identified best practices on the implemented IoT systems and to compare the achieved risk overall score with that achieved by state-of-the-art studies.

The rest of the paper is structured as follows. Section II outlines related work on IoT security and privacy. Section III identifies and discusses the best practices for IoT privacy and security. Section IV introduces two real IoT-based use cases (concerning crowding and mobility monitoring applications) to which we applied the identified best practices. Best practices evaluation is presented in Section V, where we computed the overall risk score of the two IoT systems comparing the proposed methodology with state-of-the-art solutions. Finally, the conclusions are drawn in Section VI.

II. BACKGROUND

Recently, the European Commission (EC) published a report [10] focused on the features and benefits offered by the IoT. The first part of the report analyses EU legislation on the safety of products placed on the European market. It should be noted that regulatory product safety contains a number of gaps that need to be filled with new legislative interventions by the EU and the Member States. Similar regulations are adopted around the world. The framework on this issue was drawn up before the birth of digital technologies such as

artificial intelligence (AI), IoT, or robotics and, consequently, the rules are not always able to regulate the risks related to these emerging technologies. In particular, the characteristics of emerging technologies may make it difficult to determine liability for any damages and it is therefore important that victims of accidents arising from products and services, including emerging digital products, do not undergo a level of protection lower than that of traditional technologies. The diversity of applications and heterogeneity of devices in IoT systems implicate that security and privacy properties need to be more robust and versatile.

Related work in this area focused on challenges such as detection and recovery from malicious or malfunctioning nodes, safety against attacks, prevention of malicious threats, and dynamic mutual authentication. In [11], the authors explored the most relevant limitations of IoT devices and their solutions, by classifying IoT attacks and analyzing mechanisms and architectures for authentication, access control, and security issues in different IoT layers. In [12], the authors presented an IoT security roadmap overview based on a novel cognitive and systemic approach describing the role of each component, interactions with the other main components, and their impact on the overall. A case study is presented to highlight the components and interactions of the systemic and cognitive approach. Moreover, security questions were discussed considering novel taxonomy of the IoT framework and standardization activities, to propose research directions. In [13], Tawalbeh et al. address IoT privacy and solutions with a focus on challenges and solutions. Specifically, the background of IoT systems and security measures is analyzed, defining privacy policies but offering no real solution in terms of people's privacy. Moreover, in addition to the legal aspects related to IoT data, there are technical aspects and no less important than the legal ones: intrusion prevention and detection in the IoT environment are generating increasing attention in the research community [14]. The primary goal of the research conducted by Rizvi et al. [15], is to advance the current state of the art in IoT research by identifying the critical domains where IoT is heavily used, the security requirements and challenges that IoT is currently facing, and the existing security solutions that have been proposed or implemented with their limitations. The protection of data and privacy of things is one of the key challenges in the IoT. In [16], the authors addressed the topic from the perspective of authentication, authorization, identification, and localization of IoT objects, providing further discussion in terms of software vulnerabilities and backdoor analysis in IoT and Android. However, privacy in the IoT is only marginally addressed and no solutions regarding data collection and data anonymization are proposed. The surveys in [6], [7], and [8] provide discussion and analysis of major IoT security- and privacy-related issues and threats. However, all these studies lack indications and guidelines to protect a general IoT system from the identified threats. Also, the application of discussed solutions on real IoT-based systems was not proven, and risk assessment methodologies have not been investigated.

Other studies focused on specific security and privacy issues. In [17], a scheme for Industrial IoT (IIoT) was proposed to overcome risks by individuating compromised nodes and applying a desired policy enforcement to isolate them. In [18], an anomaly detection method is described based on an architecture that uses device proxies to control access to devices and collect the relevant data, also presenting an experimental case study using data generated from a typical IoT subnetwork environment with no specific controls on the environments except for the locations of the sensors. In [19], a blockchain-based privacy-aware data access control (BPADAC) scheme for distributed and secure Unmanned Aerial Vehicles (UAV) data sharing in cloud-based Internet of Drones (IoD) is presented. Moreover, a formal security analysis is presented. However, these studies did not consider risk evaluation based on real systems physically installed in the smart city environment.

In this work we aim to make a step forward with respect to the state of the art. First, we identify and discuss the best practices for IoT privacy and security, which include a set of procedures that can be taken as the guidelines to determine and solve privacy and security issues of IoT systems. Second, we follow and apply the identified best practices to two real IoT-based use cases. Third, we compare the overall risk score of these IoT systems achieved with the proposed methodology with that achieved with state-of-the-art approaches.

III. BEST PRACTICES OVERVIEW

The concept of *best practices* implies a set of well-organized practices, procedures, and behaviors that can be universally taken as a reference. In particular, security best practice guidelines (SBPG) can be defined as the best procedure that has the best operational characteristics and the best quality indicators [20]. The application of SBPG in the systems proposed in this work, aims to define the best procedures to ensure high levels of privacy and simultaneously reduced risks in terms of information security. Therefore, it is clear that both in the area of privacy and in that of the risks inherent in the security of the proposed systems, best practices are needed to ensure a high level of protection of personal data and a high level of IoT security. In the following, we discuss best practices for both privacy and information security, SBPG accordingly.

Best practices involving privacy follow regulations that are becoming increasingly insistent across the planet. For example, Europe is addressing privacy with the General Data Protection Regulation (GDPR) [21]. Simultaneously, in the United States, the state of California was the first to enact the California Consumer Privacy Act (CCPA) [22], while other states such as Maryland, Oklahoma, Ohio, New Jersey, Florida, and Alaska are working on a Private Right of Action (PRA). In Asia, there is also a positive regulatory trend, as far as personal data protection is concerned. China's Personal

Information Protection Law (PIPL) [23] officially went into effect on November 1, 2021. Finally, In India, the new Privacy Bill was introduced in late 2021. Among the most notable changes in the submitted bill is the introduction of a set of non-personal data protection obligations, passed in 2022. Instead, best practices on cyber risks follow worldwide guidelines. For example, the breach of a gateway, the criticality of an IT process, and the vulnerability of certain login credentials are identical worldwide.

A. IoT AND PRIVACY

This section aims to analyze privacy issues concerning IoT technologies with regard to privacy guidelines. As a matter of fact, the interplay between the huge amount of things, goods, and people allows the datafication process, which transforms people's actions into data. Indeed, as there is a strict conjunction between things and human beings, daily actions and behaviors of people lead to dangerous acquisitions, tracing, or mapping of people's positions and movements through smartphones, smartwatches, social networks, and other smart devices. For instance, there are many Bluetooth Low-Energy (BLE) based applications able to monitor and measure the quality of sleep; there are smart shoes that trace the run, monitor the time and the number of steps, and the route executed. Since these kinds of applications and services require an in-depth analysis of the social, ethical, and cultural effects of the IoT, legal concerns, with particular regard to the protection of the fundamental rights of the individual, play a crucial role. The IoT needs clear and precise rules that protect the human person from a variety of risks, such as health and privacy. Thus, it is necessary to trace the boundaries between the lawfulness and illegality of certain behaviors, with particular attention to the main following aspects:

- Physical aspects: presence of smart chips in a given product; environmental impact of chips and recycling; development of an additional network structure and infrastructure for IoT applications and hardware; impact of electromagnetic fields on animals.
- Privacy aspects: privacy and user confidence; silence on the chips right; guarantees for citizens regarding the protection during the collection and processing of personal data; ensuring the best possible protection of citizens and businesses from all types of online cyber-attacks.
- Standardization aspects: harmonization of regional standards; development of open technology standards; interoperability between different systems.

The *datafication* due to IoT resulting in the collection, processing, and transfer of data, requires the correct identification of the subjects involved, i.e., the data controller and data subject [24]. Their correct identification is necessary as the data controller is responsible for protecting personal data, subjected to all the obligations provided by the local regulations, and punished in cases of infringements. The data subject, besides, is the one to whom the personal data refers, so it is the subject that must be protected.

B. BEST PRACTICES FOR PRIVACY IN IOT

When personal data processing starts, regardless of the area of interest involved, the local Regulation requires the conduction of a preliminary analysis to assess the regulatory impact. This procedure is needed to verify how and if that treatment can be carried out in compliance with the own Regulations. This rule is called the principle of *"data protection by design and by default"*, a concept developed in the United States and Canada in 2010, and later adopted in Europe by the GDPR as well [21]. The cardinal foundations on which this principle is based are:

- Lawfulness, fairness, and transparency. Avoiding anything generally unlawful with personal data. Do not deceive or mislead people when collecting their personal data. Be open and honest, and comply with the transparency obligations of the right to be informed.
- Purpose limitation. If there is a plan to use personal data for a new purpose other than a legal obligation or function set out in the law, it is necessary to check that this is compatible with the original purpose or get specific consent for the new purpose.
- Data minimization. Collecting personal data we actually need for our specified purposes, and arranging sufficient personal data to properly fulfill those purposes. Periodically review the data hold, and delete anything not needed.
- Accuracy. Records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. Complying with the individual's right to rectification and carefully considering any challenges to the accuracy of the personal data.
- Storage limitation. Regularly review the information and erase or anonymize personal data when no longer needed. Clearly identify any personal data that is needed to keep for public interest archiving, scientific or historical research, or statistical purposes.
- Integrity and confidentiality. Must ensure that you have appropriate security measures in place to protect the personal data you hold. Understanding the requirements of confidentiality, integrity, and availability for the processed personal data, and using encryption and/or pseudonymization where it is appropriate to do so.

Once this first check has been carried out, aimed at ascertaining compliance with the aforementioned principles, the risks of the specific treatment are assessed, in order to apply the appropriate safety measures (i.e., appropriate technical measures) to limit them. The proposed study and procedures are based on the principles of "data protection by design end by default," with full respect for transparency, limiting data collection to the purposes of the project. Moreover, storage is limited to data needed for pedestrian and vehicular monitoring, ensuring integrity, functionality, and privacy through encryption and pseudonymization techniques.

C. IoT SECURITY AND RISK

Although the IoT offers clear benefits, cyber-attacks and uncertainty about the best security practices to be applied, together with the costs associated with these practices, are a disincentive to the adoption of this technology. Consideration should also be given to the mistrust in terms of perceived IoT security breaches by end users. A study conducted by Gemalto [25] indicates that 90% of consumers lack confidence in the security of IoT devices. According to the State of IoT Security report for the latest trends:

- 96% of businesses and 90% of consumers believe there should be IoT security regulations;
- 54% of consumers own an average of four IoT devices, but only 14% believe that they are knowledgeable on IoT device security;
- 65% of consumers are concerned about a hacker controlling their IoT device, while 60% are concerned about data being leaked.

In [26], a comparative study considering Australia, Canada, France, Japan, the UK and the US revealed that:

- 63% of people surveyed find connected devices 'creepy' in the way they collect data about people and their behaviors;
- this sentiment is echoed throughout the survey, with half of people across markets distrusting their connected devices to protect their privacy and handle their information in a respectful manner (53%);
- on top of not trusting the device itself to keep data secure, 75% of people agree there is a reason for concern about their data being used by other organizations without their permission;
- the security concerns are serious enough to deter almost a third (28%) of people who do not own smart devices from buying one; security concerns are as strong a deterrent as the price of a device;
- people have concerns about security and privacy but do not know how to adapt and adjust device settings in a way that might allay these fears. 80% of the people surveyed are aware of how to set and reset passwords, but only 50% are aware of how to disable the collection of data about users and their behaviors.

The above findings highlight that user trust is an essential factor in realizing the potential of the IoT. Digital security design is increasingly a key factor for IoT devices in all of their components and to prevent vulnerabilities in one part from jeopardizing the security of the entire device or system in which it is embedded.

D. BEST PRACTICES FOR RISK AND SECURITY

Security risk management within Information and Communications Technology (ICT) identifies security risks and the steps to be taken to mitigate those risks, both on the hardware and software/platform side [27], [28]. These measures primarily include three aspects: the use of software, the use of hardware, and finally the employment of qualified people to maintain an operating environment that is safe from threats. Security prevention measures need to be addressed at each layer of the OSI model, due to elements of vulnerability, in order to mitigate risks:

- Physical layer threats can cause a Denial of Service (DoS) leading to the unavailability of application.
- Data Link layer threats include switch security aspects, such as Address Resolution Protocol (ARP) spoofing, MAC flooding, and spanning tree attacks, which can be mitigated, e.g., by modifying network switch configuration.
- Network and transport layers threats can cause unauthorized retrieval of endpoint identity or unauthorized access to internal systems and could be reduced or solved by implementing Network Address Translation, Access Control Lists, or firewall technologies;
- for session and presentation layers both user and data unauthorized accesses can be mitigated by using encryption and authentication methods, using simple login/password methods or more robust biometric systems [29], [30];
- Application layer threats include backdoor attacks and can be avoided with the use of set-up tools, such as virus scanners or WebInspect.

Because total risk elimination is not possible, the focus of best practices is on mitigating security risks. In [31], an IoT attack taxonomy was proposed to underline security vulnerabilities for diverse scenarios targeting different system assets and aiming to compromise distinct security objectives. The four categories of attacks also considered in this paper are:

1) Device: attacks causing anomalous functioning of the IoT system, which are performed, for example, by hardware ports, as node tampering, through the malicious code injection leading to system dysfunction, trojans, jamming, or remote firmware update.
2) Infrastructure: attacks that target the ''back end'' of a system, which is the data access layer, including data storage and data processing, threatening the physical integrity or availability of data or devices located at the edge of the network.
3) Communication: attacks that compromise the exchange of data between IoT devices, threatening communication technology, standards, protocols, and channels. This category also involves the network layer (i.e., switching, routing, protocols).
4) Service: considers service-type attacks involving inherent functionality that a system is able to provide (i.e., application layer attacks). Phishing attacks, social engineering, and control hijacking, malicious scripts, cryptanalysis attacks, exploitation of buffer overflow vulnerabilities, and all the attacks that attempt to extrapolate sensitive information from applications.

Different factors need to be considered at various stages of risk management as illustrated in Fig. 1. For example, the

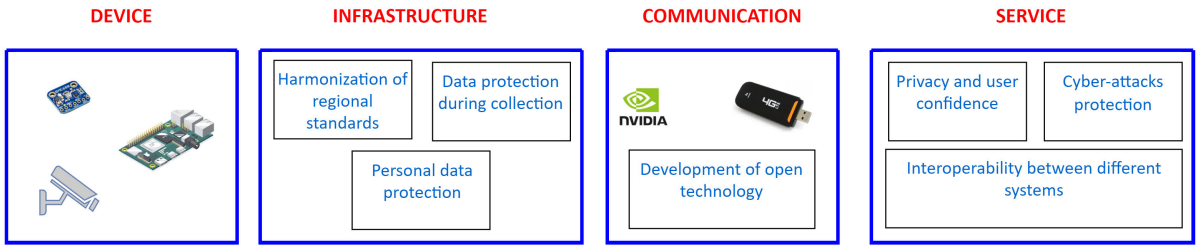

FIGURE 1. Taxonomy for risk management.

devices used fall between sensor and basic commercial-grade electronic devices. These devices represent the means of data acquisition, so their hardware and software design directly influences the expected outcome in terms of privacy and cybersecurity. The context and environment in which the system it is located (i.e., public or private), the data storage (i.e., public cloud, a private network of servers, a data center, or a combination of these), the hardware, and the software designed to work with specific hardware, represent some of the key element involved in infrastructure design. The created infrastructure aims to achieve a harmonization of regional standards, that is, to provide a set of uniformly recognized procedures for risk limitation and management. In addition, another crucial aspect is the protection of data during acquisition, a practice that is not commonly used and generally employs intermediate steps that increase the risk index. Last, but not least, personal data is now treated according to regional or continental types of legislation that has led to the definition of ''personal data protection''. According to graphic standards, more evolved telecommunication standards, and the development of open-type technologies, at the communication level there is a continuous technological innovation of the open type, accessible, integrable and employable in different scenarios. Modern services must evolve to meet the growing demands of safeguarding user trust and their data, fostering interoperability among diverse systems, and upholding rigorous cybersecurity standards to defend against cyberattacks.

Responsibilities also vary depending on whether the data is protected by appropriate software (i.e., customer responsibility) or whether the cloud provider is considered to be in charge of the infrastructure. Acquired data, of any nature, travels within a network that can be public, private, or both. A private network requires security. Nowadays, networks provide different levels of security starting from the security of the equipment (i.e., devices), to the software level with firewalls (i.e., infrastructure), to the encryption of data in transit in addition to traffic segmentation through routing policies (i.e., communication), and to end with services provided to the users (i.e., service). In general, designers of systems where security is a non-negligible element must take into account certain unavoidable measures, such as encrypting data at every stage of acquisition, controlling access to data and the network, and having a global view of the activities carried out within the system. Just think of the many connection ports for a particular service associated with a particular standard such as UDP or TCP, the well-known ports (e.g., 22/TCP SSH), or the registered (e.g., 1194/UDP OpenVPN) and unregistered (5800/TCP VNC) ports, as well as the free ports (e.g., 49152 to 65535). Therefore, each of these stages presents critical issues and potential flaws that can pose greater or lesser risks to the proper functioning of a system, or in the worst case, theft of sensitive data that can be traced back to individuals.

In Section IV-A, two real IoT systems are introduced in order to describe the application of the aforementioned best practices for privacy and security concerning the design and implementation of an IoT-based application. The goal is to highlight the rules that need to be observed in order to ensure personal data protection in line with EU regulations.

IV. BEST PRACTICES IMPLEMENTATION

This section presents two real IoT use cases in order to show what are the main steps to practically secure a system according to the best practices presented in section III. The technical detail of the systems (i.e., the use cases) are not the subject of this article and has been extensively discussed in a work previously presented by the authors [3]. This section is structured as follows: subsection IV-A shortly describes the two use cases, while subsection IV-B provides an overview of the main choices made to secure the systems according to the best practices.

A. REAL USE CASES

The proposed systems concern the monitoring of the flow of people and vehicles in smart cities. The flow of people is a particularly relevant issue, especially because of the recent health emergency that is affecting the entire world population. The monitoring of these flows involves both indoor spaces (e.g., shopping malls) and large outdoor events (e.g., music concerts). Moreover, the monitoring of pedestrian flows allows the statistical analysis and the determination of origin-destination matrices that can be treated and studied for the optimization of bus frequencies of urban mobility services. Therefore, the pedestrian flow is closely related to the vehicular flow. Its monitoring and control allow flexible, dynamic, and real-time management of vehicular flows. Both systems have been installed in the city of Cagliari

(Sardinia, Italy) and take as input the detection of smartphones and vehicle license plates, which are discussed in more detail in the following subsections.

1) CROWDING MONITORING SUB-SYSTEM

The Wi-Fi standard has been established as one of the key technologies in the field of connecting portable devices such as smartphones, tablets, and other wearable devices. It is particularly popular with smartphones, because it easily provides Internet connectivity in many places, thanks to the growing number of hotspots and open wireless networks available. Regardless of whether it is in active status or not, the Wi-Fi radio interface sends data packets, containing the unique MAC address identifier, attributable in some cases to the unique address of the card and therefore to the individual device. The technique of detecting the presence of individuals and monitoring their movements using this information is known as Wi-Fi tracking. MAC addresses are designed to be persistent and globally unique and represent the physical address of the network interface of mobile devices. They are transmitted by the devices within the MAC frames together with a series of other information for the maintenance of the network infrastructure. Through these data, it is possible to obtain an impression of the device that transmitted them. The processing of these data allows our system to obtain statistical and real-time information regarding urban mobility.

Taking into account this, a system for counting people's attendance in a specific area has been implemented. Through an external network card connected to a Raspberry Pi device, the Wi-Fi traffic of mobile devices is ''sniffed'', by analyzing the MAC addresses. The crowding monitoring sub-system represented in Fig. 2 (left box) ensures that the MAC addresses already acquired are not counted multiple times. It has a maximum operating range of about 50 m and can be used both indoors (e.g., for counting utilities inside a bus or in a room) and outdoors (e.g., for counting near a traffic light). An example of a use case is smartphone detection of users on public vehicles (e.g., buses or trains). A proof of concept was carried out and tested in the city of Cagliari. In particular, the devices were installed:

- on public transport vehicles (i.e., onboard);
- close to public transport stops (i.e., in fixed points).

Once the network and power connections were defined, all the devices had the task of transmitting all the processed data to an IoT platform, created ad hoc to process and manage all the information coming from the urban area. The data was transmitted after being processed, thus it was necessary to acquire the data, perform the on-board processing of the data through anonymization techniques, and transmit the already anonymized data in order to guarantee privacy.

2) MOBILITY MONITORING SUB-SYSTEM

Similar to crowding monitoring, vehicle tracking requires a similar technique involving both vehicle type and exact vehicle identification through the license plate. The system designed and tested on a real scenario consists of a system of cameras appropriately placed to monitor road intersections or traffic circles. The cameras are used as image and video acquisition sensors and are able to operate in different weather conditions, both day and night. The cameras are connected via ethernet link to an NVIDIA Jetson NX processing unit that performs the following operations:

1) the board receives the license plate images as input;
2) a numerical conversion is performed through a neural network named Automatic License Plate Recognition (ALPR);
3) an irreversible anonymization algorithm is applied that associates a Hash to each license plate, preventing the original license plate from being traced.

The mobility monitoring sub-system in Fig. 2 (right box) shows the vehicle detection system composed of different levels. The cameras make a continuous video and frame the rear of the vehicles passing along a particular gate or road lane. The processing unit performs a screening of the frames received from the camera, electing the best frame characterized by low noise and best brightness. The ALPR algorithm deals with the conversion of the image into an alphanumeric string containing the sequence of characters of the identified license plate. This string represents the input of the Hash algorithm that converts in pseudorandom mode the license plate data into a 512-bit string. The system has been designed not to store the license plate data in any storage medium. The license plate image data converted to a string is directly provided as input to the Hash algorithm for the anonymization process. The anonymized data is kept in a temporary volatile memory, aggregated with other anonymized data, and finally sent via LTE as soon as a buffer of appropriate size is filled. The proposed system sends the anonymized data to a database (DB) installed within a Social IoT (SIoT) platform, called Lysis, where the data can be appropriately reprocessed for determining hourly, daily, monthly, and yearly statistics. The Lysis platform is an SIoT platform carried out for distributed IoT applications involving socially connected objects [32]. The aggregated data can be processed to work out statistics on the directions taken by vehicles at a particular city junction. In this way, further decisions could be made about the dynamism of traffic light timings in order to streamline traffic through real-time analysis.

B. BEST PRACTICES REALIZATION

In this subsection, techniques used to protect data after their acquisition are presented. In the first phase, the sensitive data is acquired and immediately pre-processed transforming it into a Hash key, a special class of Hash functions that has some properties that make it suitable for encryption [33]. It is a mathematical algorithm that maps arbitrary-length data into a fixed-size binary string called a Hash value. This Hash function is designed to be unidirectional, which is hard to invert: the only way to recreate the input data

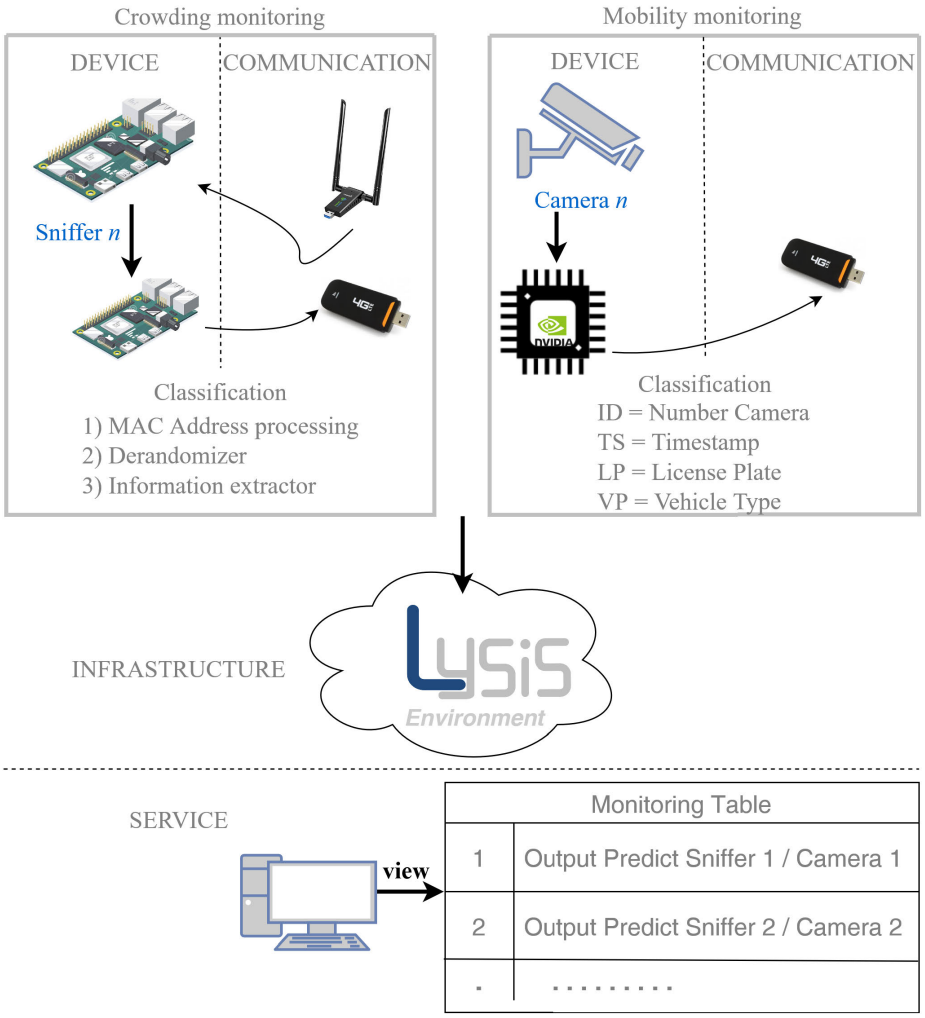

FIGURE 2. Taxonomy for pedestrian and vehicular detection system.

from the output of an ideal Hash function is to attempt a brute-force search for possible inputs to see if there is correspondence. Alternatively, it could be used a rainbow table of matching hashes. Hash functions provides a more reliable and flexible method of data retrieval than any other data structure, it is synchronized, and it contains unique element. The main drawback is that operations on Hash functions take constant time on average. Thus, hashing is not effective when the number of entries is very small. The system needed to be able to guarantee the privacy of collected data during acquisition, processing, transmission, and storage, providing specific measures to assure users' anonymity. Considering the identification procedure, collected data needed to be anonymized, to comply with current legislation concerning the privacy and the processing of personal data, before it can be used for tracking the terminal itself. Moreover, efforts were made to identify the best way forward for the subsequent transmission of the acquired data. During the design phase, various problems emerged regarding the transmission of sensitive data by devices to the platform:

- where to perform the anonymization after data acquisition, which is a choice that involves both the software and the hardware;
- how to perform the anonymization, in order to guarantee the NOT traceability data in a reverse process.

In this section, we will therefore give an estimate in terms of privacy and security of both proposed systems.

1) PRIVACY

It is attributable to something that is inherently special or sensitive to people. In our specific case, the MAC address of a smartphone and the license plate of a vehicle are undoubtedly pieces of information that can be traced to specific people. The preliminary phase consisted of a cost-benefit evaluation of the anonymization algorithms offering the optimal performance for handling the processed sensitive data. Table 1 summarizes the main algorithms analyzed.

Secure Hash Algorithm (SHA) algorithms (SHA-256, SHA-384, and SHA-512) belong to the MD family of Hash functions [35]. The SHA-256-bit "double" algorithm

TABLE 1. Anonymization algorithms.

Algorithm Name	Advantages	Disadvantages
SHA-512 [34]	Best security level between the options	Computational costs higher than SHA-256 "double"
SHA-256 "double" [35]	Good level of security	High computational costs
MD5 [36]	Lower computational cost of the three	Not safe enough; they increase collisions

processes the message twice with the same technique of anonymization. SHA-512 [34] may be used to Hash a message M, having a length of k bits, where k is a number between 0 and 2^{128}. It is the third generation of cryptographic hash algorithms developed by NIST. It is based on different principles compared to SHA-256, using a construction called SPONGE to provide resistance against potential cryptanalytic attacks that could impact SHA-256. Nowadays, it has no significant known vulnerabilities and is considered secure. Although SHA-3 was published after SHA-2, it is not yet widely used like SHA-256, but it is gradually gaining popularity. SHA-512 uses a 3 steps solution: a) a message schedule of eighty 64-bit words, b) eight working variables of 64 bits each, c) a Hash value of eight 64-bit words. The final result of SHA-512 is a 512-bit message digest. Version 5 of the MD algorithm was also considered. MD5 algorithm output is a process that is much shorter than the two previous cases, and it consists of only 32 characters. We can therefore say that with an attack "by trial" (brut-force attacks) it is more likely to be decrypted. It also increases the number of collisions occurring during encryption. Collision means the result obtained when two different input data produce the same output string from a Hash encryption block. In the MD5 the collisions increase enormously compared to the Hash 256 and 512. Therefore, there is an increase of the risk in the rescue of sensitive data and they would risk to be not more univocal. A representation of the acquisition and anonymization process is presented in Listing 1.

Level 3 of the mobility monitoring sub-system depicted in Fig. 2 sends to the cloud various information about the analyzed vehicles. SHA-512 can be applied to license plates in the context of ensuring data integrity and security. Here are some potential use cases for SHA-512 with license plates.

- License Plate Verification: Each license plate can be hashed using SHA-512 to generate a unique identifier or checksum. This hashed value can then be used for verification purposes, ensuring that the license plate information has not been tampered with or modified.
- Secure Database Storage: When storing license plate data in a database or system, the license plate numbers can be hashed with SHA-512 before being stored. This helps protect the privacy of the actual license plate numbers while still allowing for efficient matching and lookup operations.
- Authentication and Access Control: SHA-512 can be used in authentication systems where license plate information is used as an identifier. For example, in automated toll collection systems or parking access control, the license plate number can be hashed and compared against a stored hash to grant or deny access.
- Secure Communication: When transmitting license plate data over a network or between systems, SHA-512 can be used to generate a hash of the data for authentication and integrity checks. The receiving system can verify the integrity of the data by comparing the received hash with a calculated hash of the received license plate information.

By applying SHA-512 to license plate data, it adds an additional layer of security and helps ensure the integrity and privacy of the information. However, it's important to consider other security measures such as secure key management and encryption, in addition to the use of hash functions, to provide comprehensive data protection.

Each vehicle is stored in the database with the following data:

- the *"_id"* is a number assigned by the MongoDB database when storing the data;
- the *"Cam_num"* represents the camera and the frame that is selected as the best among those acquired for converting the image to alphanumeric code;
- the *"Date"* represents the acquisition date of the frame selected by the system;
- the *"Time"* represents the exact time of acquisition of the selected frame;
- the *"Vehicle Type"* is the classification returned by the YOLO neural network that identifies the vehicle type;
- the *"Anonymous Plate"* is the result of applying the SHA-512 algorithm, a unique code for each license plate detected;
- the *"Frequency"* represents the detection frequency of a specific license plate.

Using SHA-512 with MAC addresses can be helpful in certain scenarios to ensure data integrity and security. Here are some potential use cases for applying SHA-512 to MAC addresses:

- Data Integrity: MAC addresses can be hashed using SHA-512 to create a fixed-length, unique identifier for each MAC address. This hash can be used to verify the integrity of the MAC address, ensuring that it has not been tampered with or modified during transmission or storage.
- Anonymization: In certain privacy-sensitive applications, it may be desirable to anonymize MAC addresses. By applying SHA-512 to the MAC address, a hashed value can be obtained that hides the original MAC address while still allowing for identification and matching purposes when necessary.
- Access Control: In secure systems, SHA-512 can be used to authenticate and authorize devices based on their MAC addresses. The MAC address can be hashed and compared to stored hash values to grant or deny access to a network or a specific resource.

- Data Storage and Lookup: When storing MAC addresses in databases or systems, using SHA-512 can help protect the privacy of the original MAC addresses. By storing the hashed values instead of the actual MAC addresses, it adds an additional layer of security against unauthorized access or data breaches.

It is important to note that while SHA-512 can provide data integrity and some level of privacy protection, MAC addresses are unique identifiers that can still be correlated and traced within a network environment. Additionally, it's crucial to consider other security measures, such as encryption, secure key management, and access control policies, in conjunction with the use of hash functions to ensure comprehensive data protection. Similarly, as shown in Listing 2, each MAC address is stored in the database with the following data:

- the *"_id"* is a number assigned by the MongoDB database when the data is stored;
- the *"ANTENNA"* represents the identifier of the Wi-Fi antenna that is performing the sniffing operations;
- the *"MAC_ADDRESS"* is the MAC address anonymized through the SHA-512 algorithm, a unique code for each MAC address detected;
- the *"FLAG"* identifies the nature of the MAC address, between random or not, unicast or broadcast type;
- the *"TIMESTAMP"* is the time of acquisition of the MAC address expressed as the number of seconds elapsed since an arbitrary date, i.e., midnight (UTC) on January 1, 1970, a time named *epoch*;
- the *"DATA_ISO"* is the date and time of acquisition expressed in commonly used notation;
- the *"SEQ"* represents the sequence number of the data acquired;
- the *"FREQUENCY"* is the transmission frequency of signals associated with a particular MAC address;
- the *"POWER_dBm"* is the signal strength of the mobile device, received by the sniffer;
- the *"CHANNEL"* is the channel used in signal transmission in the communication between sniffer and mobile device.

Therefore, from a privacy perspective, appropriate privacy policies have been adopted to ensure the protection of individuals without having to ask for specific consent. In fact, the data is anonymized without allowing the operator to trace the original data in any way, whether the vehicular license plate or MAC address of the mobile device.

2) RISKS AND SECURITY

The proposed system is subjected to a rigorous methodology that assesses cybersecurity and risks according to the NIST guidelines [9]. Each element in the chain requires special arrangements to provide an overall level of security against data loss or tampering. As defined in the previous session, the first practice adopted is to treat the data to ensure people's privacy. Second, not only data encryption is applied but


```
{
  "_id": "61852f89c4bdfdl3132a838d",
  "Cam_num": "CameraA_frame8",
  "Date": "2022-10-05",
  "Time": "14:20:09",
  "Vehicle Type": "Car",
  "Anonymous Plate": 6761540816179993000,
  "Frequency": 1
},
{
  "_id": "61852f96c4bdfdl3132a838f",
  "Cam_num": "CameraA_frame11",
  "Date": "2022-10-05",
  "Time": "14:20:22",
  "Vehicle Type": "Car",
  "Anonymous Plate": 5867417241934044000,
  "Frequency": 1
},
{
  "_id": "61852fa2c4bdfdl3132a8391",
  "Cam_num": "CameraA_frame6",
  "Date": "2022-10-05",
  "Time": "14:20:34",
  "Vehicle Type": "Car",
  "Anonymous Plate": 3382733926990473700,
  "Frequency": 1
}
```


LISTING 1. License plate data anonymization.


```
{
  "_id": "630753d69fe96018a17d7ae0",
  "ANTENNA": "1",
  "MAC_ADDRESS": "65f07ae34bl45da58e4c68c5132d02b
  ee49a54519b19364e6acfl04cd0200888",
  "FLAG": "00",
  "TIMESTAMP": "1661424596.702367814",
  "DATA_ISO": "2022-09-25 12:49:56",
  "SEQ": "3762",
  "FREQUENCY": "2412",
  "POWER_dBm": "-72",
  "CHANNEL": 1
},
{
  "_id": "630753d69fe96018a17d7adf",
  "ANTENNA": "1",
  "MAC_ADDRESS": "f6806fb25e41e22c7d0e580272d39743
  847dc634d72a80f07b8db6eee5dabfab",
  "FLAG": "00",
  "TIMESTAMP": "1661424596.523373132",
  "DATA_ISO": "2022-09-25 12:49:56",
  "SEQ": "28",
  "FREQUENCY": "2412",
  "POWER_dBm": "-83",
  "CHANNEL": 1
}
```


LISTING 2. License plate data anonymization.

encryption of the entire data transmission chain is offered, from acquisition to cloud storage. The high protection achieved has three main aspects, which are detailed below:

- **logistics aspects** - logistics aspects are related to the physical scenario in which the proposed systems operate. Defining the risk scenario is one of the main aspects to be evaluated from the perspective of tampering, equipment theft, or the possibility of physically connecting external devices. The possibility that the systems may be within the reach of potential tampering or intrusions is a high index of risk. Otherwise, difficult access

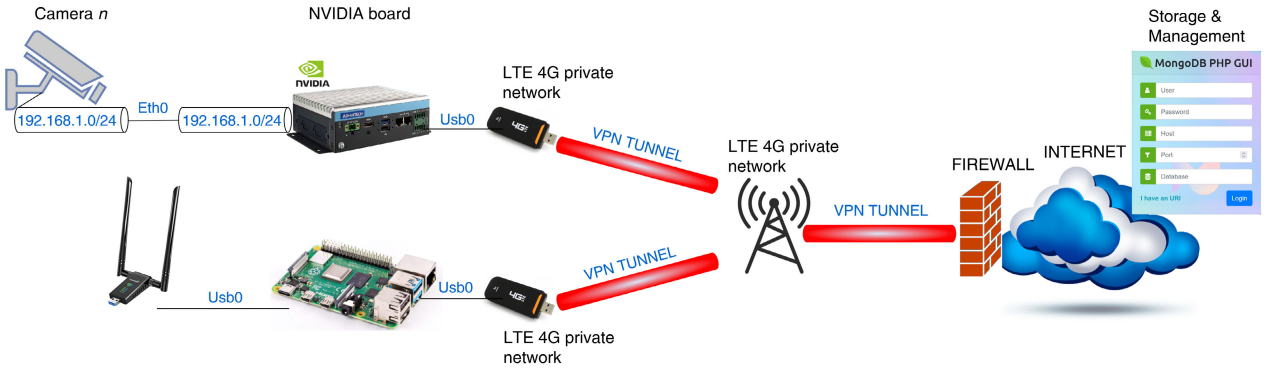

FIGURE 3. Practical best practices implementation and cybersecurity assessment.

to the hardware system represents a rare likelihood with marginal consequences. The sniffing and vehicular monitoring systems were installed within a very low-risk scenario primarily for two reasons. The systems are installed within the *Port System Authority of the Sea of Sardinia*, in special sites that are not easily accessible, on poles at a height of 5 to 7 meters above the ground. In addition, the area is fully video-surveilled adding additional protection for hardware sniffing and vehicular monitoring systems. Logistically, very high-security criteria have been met, with very low-risk configurations against tampering and intrusion on the hardware system.

- **connection of modules**: the hardware/software system is composed of several modules that interact with each other, Each connection represents a criticality and vulnerability for the entire system. Starting from the data acquisition sensor, through processing and ending with data transmission and storage, there are different types of information transmission medium, wireless or wired, public or private, with or without a firewall for appropriate filtering of information. In the two proposed systems, the connection between the sensor and acquisition board is wired, Ethernet with private IP addressing, and USB. The processing units have no wireless-enabled radio interface, while the connection to the 5G LTE network is through a 5G LTE USB drive.

  A VPN (Virtual Private Network) is a technology that enables the creation of a secure and encrypted connection between a device and the Internet. This connection is made through a VPN server, which acts as a mediator between the device and the Internet. When a VPN is used, Internet traffic is routed through the VPN server, which encrypts the data and hides the IP address. This makes it more difficult for third parties, such as hackers, advertisers, or government agencies, to track online activities. Some common reasons for using a VPN include:

  – Privacy: VPNs can help protect your privacy by encrypting your internet traffic and hiding your IP address.
  – Security: VPNs can help secure your online activities, particularly when using public Wi-Fi networks, which are often insecure.
  – Access to restricted content: VPNs can allow you to access websites and content that may be restricted in your location or country.
  – Bypassing censorship: VPNs can help bypass internet censorship and restrictions imposed by governments or ISPs.
  – Remote access: VPNs can allow you to access your company's network or resources from outside the office, as well as provide secure access to remote servers or devices.

  When using a VPN, it is important to choose a reputable provider that does not log your activities or sell your data. Using a VPN may slow down internet connection due to the additional processing required to encrypt and decrypt data.
- **policies - back-end**: incoming traffic to the cloud and subsequently to the database, undergoes a final check by a firewall that monitors incoming traffic through a predefined set of security rules to allow or block certain events. If not properly configured, the firewall could allow traffic from any commercial 4G LTE connection to pass through. Best practices require the use of a private 4G network segment instead of commercial 4G communications. This choice introduces selectivity of allowed traffic through appropriate configuration of the firewall that recognizes that traffic as the only traffic authorized for entry to the cloud and storage on the database. Last but not least, cloud data storage requires a 5-input authorization essential for write and read operations: user, password, host (i.e., private IP), port, and database name.

Strict adherence to the three principles described above ensures a very high degree of security and a very low-risk index. The precautions taken allow encryption of the sensed data and transmission of the encrypted data over an encrypted private network, ensuring the highest index of security at the network level. The architecture of the sub-systems has been shown in Fig. 3. The cameras are connected to the NVIDIA

TABLE 2. Pedestrian system status of devices and interfaces.

Component	Interfaces	Status
Wi-Fi dual antenna	USB	enabled
Raspberry Pi 4 B+	Ethernet USB 1 USB 2 USB 3 USB 4 Bluetooth radio interface Wi-Fi radio interface Raspi OS Login	disabled enabled (dual Wi-Fi antenna) disabled disabled disabled disabled disable Psw 12 alphanumeric + symbols elements
LTE USB	USB	enabled
LTE connection	4G private network + tunnel VPN	enabled
Firewall	LTE private traffic segmentation	enabled
Link VM - MongoDB	root ssh	User ********** Password ****** Host **.***.**.*** Port "xyzty "

TABLE 3. Vehicular system status of devices and interfaces.

Component	Interfaces	Status
GIFRAN camera	Ethernet only	enabled
Link GIFRAN Camera - NVIDIA Board	Ethernet only	enabled
NVIDIA Board	Ethernet USB 1 USB 2 USB 3	enabled enabled (usb 4G LTE) x x
NVIDIA Board	Operating system access	Psw 12 alphanumeric + symbols elements
LTE USB	USB	enabled
LTE connection	4G private network + tunnel VPN	enabled
Firewall	LTE private traffic segmentation	enabled
Link VM - MongoDB	root SSH	User ********** Password ****** Host **.***.**.*** Port "xyzty "

video card through an Ethernet link and private network addresses 192.168.1.0/24. The USB 4G drive is connected directly to a USB port provided with the NVIDIA video card on which a VPN tunnel network has been configured. The traffic travels on a private 4G network segment, which is recognized by the 4G network and the firewall attested inbound to the cloud on which the database has been installed. A similar procedure takes place in the pedestrian monitoring system. A dual USB Wi-Fi antenna and a USB 4G drive are connected to the Raspberry Pi board on which a VPN tunnel network has been configured. Each sniffer and vehicular monitoring system is equipped with a 4G SIM with a private network segment. No wireless Wi-Fi connections were employed in the described system. On both the NVIDIA board and the Raspberry Pi, only those processes strictly necessary for the required basic operation were kept active. Superfluous or unnecessary processes were appropriately killed. Table 2 and Table 3 summarize the status of the interfaces involved in the pedestrian and vehicular traffic sniffing systems. The two systems are based on different data acquisition systems and are united by transmitting over a private LTE network and VPN tunnel. Similarly, data storage and management are done in the cloud following additional input checks by a firewall.

V. BEST PRACTICES EVALUATION

Best practices evaluation in privacy and security refers to the assessment and analysis of recommended approaches, techniques, and procedures aimed at safeguarding sensitive information and protecting computer systems from unauthorized access, data breaches, and cyber threats. This evaluation process involves examining various practices and determining their effectiveness, relevance, and efficiency in the context of privacy and security. The goal of evaluating best practices in privacy and computer security is to identify robust and effective approaches that can be implemented to protect sensitive information, maintain the confidentiality, integrity, and availability of data, and safeguard computer systems from potential threats and attacks. Continuous evaluation and improvement of security measures are essential due to the evolving nature of cyber threats and the technology landscape.

A. RISK ASSESSMENT

The mathematical risk assessment according to the NIST method provides a structured approach to identify and address security risks in a telecommunications system. However, it is important to note that the application of this method requires technical expertise and specific knowledge of threats and security countermeasures. Involving qualified cybersecurity professionals may be helpful in conducting a comprehensive risk assessment in the specific context of the described telecommunications system. The mathematical risk assessment using the NIST method for a telecommunications system consisting of a sensor, Raspberry Pi, LTE dongle, private 4G network, VPN tunnel, firewall, and cloud can be performed through the following process:

1) Risk Identification: begin by identifying the specific threats and vulnerabilities associated with the described telecommunications system. For example, potential threats may include unauthorized access to the sensor or Raspberry Pi, network attacks on the 4G connection, compromise of the cloud, etc. Vulnerabilities could be misconfigurations, lack of authentication or encryption, absence of security patches, etc.
2) Risk Assessment: evaluate the likelihood of each threat and the potential impact on the system. Use objective methods to assign a numerical estimate to the probability and impact. For instance, you could use a scale from 1 to 5 to represent probability (1 = very low, 5 = very high) and another scale from 1 to 5 to represent impact (1 = negligible, 5 = very high).
3) Determination of Risk Levels: using the results of the risk assessment, combine the probability and impact to

TABLE 4. Risk assessment score for each considered threat.

Probability	Impact
1: Very low probability of threat or breach	1: Negligible impact on operations and security
2: Low probability of threat or breach	2: Limited impact on operations and security
3: Moderate probability of threat or breach	3: Moderate impact on operations and security
4: High probability of threat or breach	4: Significant impact on operations and security
5: Very high probability of threat or breach	5: Very high impact on operations and security

determine the risk levels for each threat. You can use a risk assessment matrix to assign a numerical risk level to each threat.

4) Risk Treatment: based on the identified risk levels, develop and implement mitigation measures to reduce the risks to an acceptable level. For example, you might implement a properly configured firewall, use encryption for the VPN connection, adopt stringent security policies for accessing data in the cloud, etc.
5) Monitoring and Review: once the mitigation measures are implemented, continuously monitor the telecommunications system to detect any new threats or vulnerabilities. Conduct periodic reviews to ensure that the security measures remain effective and make changes if necessary.

To mathematically evaluate the risk assessment of a generic system consisting of several blocks, it is necessary to multiply the corresponding probability and impact values for each threat to obtain a risk score for each, according to equation (1):

$$Risk\ Score = Probability \times Impact \tag{1}$$

where the *Probability* of a risk event occurring is usually represented as a numerical value between 0 and 1, where 0 indicates that the event is impossible, and 1 indicates that the event is certain. To convert probability to a 1 to 5 scale, the conversion shown in Table 5 can be used.

The *Impact* of a risk event describes the severity of its consequences. It is also represented as a numerical value between 1 and 5, where 1 indicates negligible impact, and 5 indicates very high impact (see Table 4).

The *Risk Score* Calculation is simply calculated by multiplying the probability and impact values together. The resulting risk score will range from 1 to 25 (5 levels for probability multiplied by 5 levels for impact), where 1 indicates the lowest risk, and 25 indicates the highest risk. To calculate the risk level of n cascaded blocks with probability p_n and impact i_n, can be used the following equation (2):

$$Total\ Risk\ Score = \prod_{n=1}^{\infty} p_n i_n \tag{2}$$

where p_n represents the probability of each individual block, i_n represents the impact of each individual block, and n is the number of cascade blocks. In the context of risk assessment, the risk level can be ascertained from the overall risk score through the application of a 5-level scale, or any other scale that aligns with the specific requirements of the risk assessment process at hand. In our specific case, the classification shown in Table 6 has been adopted.

TABLE 5. Probability of risk event.

Probability	% Chance	Description
1	0 - 20	Very Low Probability
2	21 - 40	Low Probability
3	41 - 60	Moderate Probability
4	61 - 80	High Probability
5	81 - 100	Very High Probability

TABLE 6. Overall risk score.

Overall Risk score	Risk Level	Level
< X	Low Risk	1
X - Y	Moderate Risk	2
Y - Z	Moderate-High Risk	3
Z - W	High risk	4
> W	Very High Risk	5

TABLE 7. Risk assessment score for each considered threat.

Risk assessment			
Threat	Probability according to Table 5	Impact	Risk Score
Wi-Fi dual antenna	0.20	1	0.20
Raspberry Pi 4 B+	0.82	4.5	3.69
NVidia Graphic board	0.78	4.5	3.51
LTE usb	0.44	3	1.32
Public 4G LTE connection	0.68	4	1.32
Private 4G LTE connection	0.42	3	1.26

The specific values of X, Y, Z, and W would depend on risk assessment criteria and the scale used. Please note that when calculating the overall risk score, it is essential to consider that the probability and impact values should be on the same scale and should be appropriately normalized or standardized if necessary. Additionally, this formula assumes that the cascaded blocks are independent of each other in terms of risk. If the blocks are not entirely independent, additional considerations may be needed in the risk assessment process.

It is essential to note that risk assessment is an iterative and dynamic process that should be regularly conducted to keep the system protected against evolving threats. Additionally, the specific numerical values for probability, impact, and risk scores may vary based on your specific analysis of the system and its operational context.

B. COMPARATIVE ANALYSIS

A comparative analysis of a multiplicative type of risk assessment necessarily requires either the same number of blocks, essentially a normalization, or a maximum risk assessment if there is no further information about possible risk reduction countermeasures. Although individual blocks are fairly well employed in the literature, their combined use within a chain starting from the acquisition sensor,

TABLE 8. Risk assessment score for each considered threat and related works.

Risk assessment										
Threat	Proposed method	[37]	[38]	[39]	[40]	[41]	[42]	[43]	[44]	[45]
Wi-Fi dual antenna	*									*
Wi-Fi internal antenna	*								*	*
Raspberry Pi 4 B+	*								*	*
NVidia Graphic board	*	*	*	*	*	*	*	*		
LTE usb	*									
Public 4G LTE connection	*									
Private 4G LTE connection	*									

passing through a dedicated transmission system, and ending in cloud storage, represent a scenario that from the best of our knowledge does not find similar works. This paper proposes a computer forensic expertise that results in the determination of a probability, then the risk score of the individual block. For example, in our specific case, given the same Raspberry Pi equipped with a generic operating system downloaded from the Internet with the default configurations, it has a determined and measured higher probability than the same operating system treated appropriately by excluding all unnecessary processes or excluding the communication of all ports that are not strictly essential. The first step took place within a computer forensics lab where each block was subjected to several tests that allowed the determination of the values shown in Table 7. These tests are often referred to as ''security testing'' or ''penetration testing''. A **penetration test** is an active security analysis of the system, where a team of security experts (ethical hackers) tries to discover vulnerabilities in the system using the same methods that could be exploited by external attackers. This may involve application vulnerability testing, network intrusion testing, and other techniques to determine the system's resistance to different types of attacks. **Vulnerability Testing** involves using automated tools to perform a scan of the system to look for known or common vulnerabilities. Security testers use specialized software to identify potential weak points in the system and services. **Security Code Review** involves a manual or automated review of the application's source code to identify potential programming-related vulnerabilities, such as ''injection'' or ''cross-site scripting'' vulnerabilities, whereas, in **Physical Security Testing** the system's physical security measures are evaluated, such as physical access to facilities, server security, and network device access control. Finally, **Compliance Testing** aims to verify if the system complies with specific security standards, such as GDPR compliance or Payment Card Industry Data Security Standard (PCI DSS) for payment card operations. Table 8 highlights the commonalities between the proposed work and other work in the literature on major vehicular and environmental monitoring issues. Only a few works present a partial match with the proposed system. However, in order to conform the evaluation between works with different weights, it was necessary to perform a normalization taking into account the common parts and how the vulnerabilities present in each block were considered. Fig. 4 shows the risk score

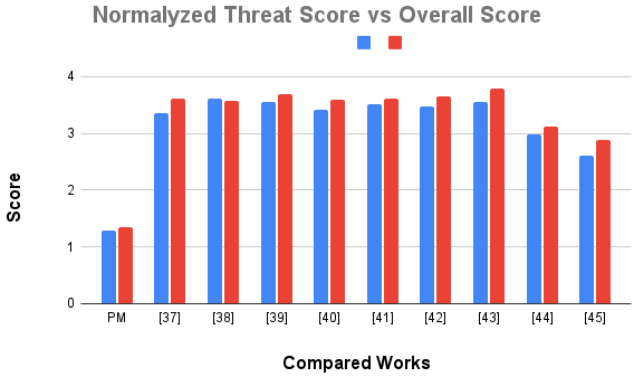

FIGURE 4. Risk score calculation: normalized threat versus overall scores.

calculation based on equation (2). The results obtained show the results of forensic expertise and risk score calculation both with normalized threat assessment and in the case of calculating values based on the classical mathematical treatment. Of particular interest is the result of the proposed method (PM) with a normalized threat score of 1.26. It is important to note that in the works considered (i.e., [32], [33], [34], [35], [36], [37], [38], [39], [40]), with the same methodology applied, the score always stands at values ranging from 2.83 up to 3.55, with an increase in risk falling in the 224%-282% range. In addition, the overall score also shows a similar trend but with even more pronounced values. Compared with the PM, which is around 1.3, the overall score of the considered papers stands at values between 2.8 to 4.7. These values lead to an overall risk assessment that is in the range 215%-361% compared to PM. The PM has some of the lowest scores on record, determined through common rules and through risk treatment policies. The results obtained show how each block properly treated, allows for a reduction in cyber risks and an increasing need for protection of one's privacy.

VI. CONCLUSION

Security and privacy issues are a major concern in the IoT scenario, which have barely been approached in the literature, in particular concerning real IoT systems and applications. This paper identifies and discusses the best practices to face IoT-related privacy and security issues, following the latest NIST guidelines and the European GDPR privacy regulation. Two real IoT-based use cases are presented, one focused on crowding monitoring and one focused on a vehicular mobility

application, which have been specifically implemented by following the set of procedures and guidelines provided by the identified best practices to minimize the occurrence of privacy and security issues. The computation of the risk assessment score on the implemented IoT systems has demonstrated that following the proposed best practices these systems achieved an overall risk score of 1.3, which is from 215% to 361% lower than that achieved by comparable IoT systems proposed in the literature studies. Thus, the proposed best practices can effectively reduce the occurrence of security and privacy issues in real IoT systems.

In future works, we aim to consider different IoT-based applications to further highlight the relevance of taking into account the proposed best practices when designing IoT systems in order to reduce the occurrence of security and privacy issues. Moreover, alternative evaluation approaches may be considered and even proposed, which need to evolve based on ongoing technology- and regulation-related advancements.

REFERENCES

[1] B. Jovanovic. (2022). *Internet of Things statistics for 2022—Taking Things Apart*. [Online]. Available: https://dataprot.net/statistics/iot-statistics/

[2] Paloalto. (2020). *2020 Unit 42 IoT Threat Report*. [Online]. Available: https://iotbusinessnews.com/download/white-papers/UNIT42-IoT-Threat-Report.pdf

[3] M. Fadda, M. Anedda, R. Girau, G. Pau, and D. D. Giusto, "A social Internet of Things smart city solution for traffic and pollution monitoring in Cagliari," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2373–2390, Feb. 2023.

[4] A. Floris, R. Girau, S. Porcu, G. Pettorru, and L. Atzori, "Implementation of a magnetometer based vehicle detection system for smart parking applications," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2020, pp. 1–7.

[5] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108771.

[6] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wireless Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, 2020.

[7] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Comput. Sci. Rev.*, vol. 38, Nov. 2020, Art. no. 100312.

[8] N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in IoT," *e-Prime, Adv. Electr. Eng., Electron. Energy*, vol. 4, Jun. 2023, Art. no. 100158.

[9] *Security and Privacy Controls for Information Systems and Organizations*, Standard NIST SP 800-53, National Institute of Standards and Technology, 2022. [Online]. Available: https://www.nist.gov/

[10] *Report From the Commission to the European Parliament, the Council, the European Economic and Social Committee: Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics*, Eur. Union, Brussels, Belgium, 2020, p. 64.

[11] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[12] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, Apr. 2018.

[13] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020.

[14] C. A. de Souza, C. B. Westphall, R. B. Machado, L. Loffi, C. M. Westphall, and G. A. Geronimo, "Intrusion detection and prevention in fog based IoT environments: A systematic literature review," *Comput. Netw.*, vol. 214, Sep. 2022, Art. no. 109154.

[15] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A security taxonomy for IoT," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 163–168.

[16] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[17] U. Tariq, A. O. Aseeri, M. S. Alkatheiri, and Y. Zhuang, "Context-aware autonomous security assertion for industrial IoT," *IEEE Access*, vol. 8, pp. 191785–191794, 2020.

[18] H. M. J. Almohri, L. T. Watson, and D. Evans, "An attack-resilient architecture for the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3940–3954, 2020.

[19] Z. Ma and J. Zhang, "Efficient, traceable and privacy-aware data access control in distributed cloud-based IoD systems," *IEEE Access*, vol. 11, pp. 45206–45221, 2023.

[20] M. G. Samaila, C. Lopes, É. Aires, J. B. F. Sequeiros, T. Simões, M. M. Freire, and P. R. M. Inácio, "A preliminary evaluation of the SRE and SBPG components of the IoT-HarPSecA framework," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–7.

[21] GDPR. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[22] CCPA. (2021). *California Consumer Privacy Act (CCPA)—State of California—Department of Justice*. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[23] PIPL. (2021). *The PRC Personal Information Protection Law*. [Online]. Available: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

[24] D. Walentek, "Datafication process in the concept of smart cities," *Energies*, vol. 14, no. 16, p. 4861, Aug. 2021.

[25] Gemalto. (2017). *Gemalto Survey Confirms That Consumers Lack Confidence in IoT Device Security*. [Online]. Available: https://www6.gemalto.com/state-of-iot-security-2017-press-release

[26] Building Trust. (2019). *The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things*. [Online]. Available: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

[27] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 108040.

[28] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," *Comput. Netw.*, vol. 191, May 2021, Art. no. 108005.

[29] P. Ruiu, A. Lagorio, M. Cadoni, and E. Grosso, "Enhancing eID card mobile-based authentication through 3D facial reconstruction," *J. Inf. Secur. Appl.*, vol. 77, Sep. 2023, Art. no. 103577.

[30] G. L. Masala, P. Ruiu, and E. Grosso, "Biometric authentication and data security in cloud computing," in *Computer and Network Security Essentials*. Springer, 2018, pp. 337–353.

[31] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K. R. Choo, "Consumer, commercial, and industrial IoT (in)security: Attack taxonomy and case studies," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 199–221, Jan. 2022.

[32] R. Girau, S. Martis, and L. Atzori, "Lysis: A platform for IoT distributed applications over socially connected objects," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 40–51, Feb. 2017.

[33] J. Wang, W. Liu, S. Kumar, and S.-F. Chang, "Learning to hash for indexing big data—A survey," *Proc. IEEE*, vol. 104, no. 1, pp. 34–57, Jan. 2016.

[34] *Hash Functions | CSRC*, Standard NIST SP 800-106 SHA-512, NIST, 2017. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/examples/SHA512.pdf

[35] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), M. Matsui and R. J. Zuccherato, Eds. Berlin, Germany: Springer, 2004, pp. 175–193, doi: 10.1007/978-3-540-24654-1_13.

[36] W. ZheLong, D. Yan, W. Qing, L. XiJian, and G. Liang, "Research on software comparison of electric energy data acquire terminal based on MD5 algorithm," in *Proc. Chin. Autom. Congr. (CAC)*, Oct. 2017, pp. 845–849.
[37] Q. Wang, X. Lu, C. Zhang, Y. Yuan, and X. Li, "LSV-LP: Large-scale video-based license plate detection and recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 1, pp. 752–767, Jan. 2023.
[38] Y. Gao, H. Lu, S. Mu, and S. Xu, "GroupPlate: Toward multi-category license plate recognition," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 5586–5599, May 2023.
[39] S. Luo and J. Liu, "Research on car license plate recognition based on improved YOLOv5m and LPRNet," *IEEE Access*, vol. 10, pp. 93692–93700, 2022.
[40] H. Shi and D. Zhao, "License plate localization in complex environments based on improved GrabCut algorithm," *IEEE Access*, vol. 10, pp. 88495–88503, 2022.
[41] I. H. El-Shal, O. M. Fahmy, and M. A. Elattar, "License plate image analysis empowered by generative adversarial neural networks (GANs)," *IEEE Access*, vol. 10, pp. 30846–30857, 2022.
[42] X. Fan and W. Zhao, "Improving robustness of license plates automatic recognition in natural scenes," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18845–18854, Oct. 2022.
[43] M. S. Beratoglu and B. U. Töreyín, "Vehicle license plate detector in compressed domain," *IEEE Access*, vol. 9, pp. 95087–95096, 2021.
[44] Y. Li, J. Barthelemy, S. Sun, P. Perez, and B. Moran, "A case study of WiFi sniffing performance evaluation," *IEEE Access*, vol. 8, pp. 129224–129235, 2020.
[45] W. Chang, B. Huang, B. Jia, W. Li, and G. Xu, "Online public transit ridership monitoring through passive WiFi sensing," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7025–7034, Jul. 2023.

MATTEO ANEDDA (Senior Member, IEEE) received the M.Sc. degree (summa cum laude) in telecommunication engineering and the Ph.D. degree in electronic and computer engineering from the University of Cagliari, in 2012 and 2017, respectively. He was a Visiting Erasmus Student with the University of Basque Country, Bilbao, Spain, in 2010, for eight months, where he carried out the M.Sc. thesis under the supervision of Prof. P. Angueira. He was a Visiting Researcher with Dublin City University, Ireland, under the supervision of Prof. G. Muntean, in 2015, and Universidad de Montevideo, Uruguay, under the supervision of Prof. R. Sotelo, in 2016, for seven months each. In 2020, he was a Short Visiting Professor with the Department of Electronics and Computers, Transilvania University of Braşov, Romania. Since 2017, he has been a Research Fellow with the Department of Electrical and Electronic Engineering, University of Cagliari. His research interests include real-time applications, 5G networks and network selection, the IoT and smart cities, adaptive multimedia streaming, and heterogeneous radio access environments. He is a Senior Member of the IEEE Broadcast Technology Society, the IEEE Communications Society, and the IEEE Vehicular Technology Society.

ALESSANDRO FLORIS (Member, IEEE) received the M.Sc. degree in electronic engineering and the Ph.D. degree in electronic and computer engineering from the University of Cagliari, Italy, in 2011 and 2017, respectively. Since 2011, he has been a member of the Net4U Laboratory (https://sites.unica.it/net4u/), Department of Electrical and Electronic Engineering (DIEE), University of Cagliari, and the Italian University Consortium for Telecommunications (CNIT). He is currently an Assistant Professor with the University of Cagliari. His main research interests include quality of experience (QoE)-based assessment of multimedia systems, QoE-based networks and application management approaches, sustainable multimedia communication, and the Internet of Things (IoT) applications for smart cities.

ROBERTO GIRAU (Member, IEEE) received the M.S. degree in telecommunication engineering and the Ph.D. degree in electronic engineering and computer science from the University of Cagliari, Cagliari, Italy, in 2012 and 2017, respectively. From 2012 to 2020, he was a Researcher with the Department of Electrical and Electronic Engineering, University of Cagliari, developing an experimental platform for the social Internet of Things. Since 2021, he has been a Research Fellow with the Department of Computer Science and Engineering, University of Bologna, Bologna, Italy. His main research interests include the IoT with particular emphasis on its integration with social networks, software engineering, smart cities, and cloud computing.

MAURO FADDA (Senior Member, IEEE) received the Ph.D. degree in electronic and computer engineering from the University of Cagliari, Cagliari, Italy, in 2013. He was an Assistant Professor with the Department of Electrical and Electronic Engineering, University of Cagliari. In 2012, he was a Visiting Ph.D. Student with the Department of Electronics and Telecommunications, Faculty of Engineering of Bilbao, University of the Basque Country (UPV/EHU), Leioa, Spain. In 2020, he was a Short Visiting Professor with the Department of Electronics and Computers, Transilvania University of Braşov, Brasov, Romania. He is currently a Researcher of telecommunications with the Department of Biomedical Sciences, University of Sassari, Sassari, Italy. He has coauthored an extensive list of articles published in journals and international conference proceedings. His research interests include telecommunications issues, cognitive radio systems, signal processing for radio communications, the transmission and processing of multimedia data, and state-of-the-art digital systems. Since 2011, he has been a member of the National Interuniversity Consortium for Telecommunications (CNIT). In March 2020, he was elected as the Chair of the Italian Chapter of the Broadcast Technology Society of the Institute of Electrical and Electronic Engineering (IEEE). He has served as a chair for various international conferences and workshops. He is an Associate Editor of IEEE Access and a Topic Editor of *Sensors*.

PIETRO RUIU received the master's degree in telecommunications engineering and the Ph.D. degree in electrical, electronics and communications engineering from Politecnico di Torino, in 2006 and 2018, respectively. From 2007 to 2013, he was a Researcher with the Istituto Superiore Mario Boella (ISMB), in the field of computing infrastructure, studying technologies, such as cloud computing, grid computing, high-performance computing (HPC), and virtualization. From 2013 to 2018, he was the Head of the Infrastructures and Systems for Advanced Computing (IS4AC) Research Unit, LINKS Foundation, with main interests in heterogeneous infrastructures, cloud automation, data privacy, energy efficiency of computing, and network resources. He is currently a Researcher Fellow (tenure track) with the Department of Biomedical Science, University of Sassari. His research interests include computer vision, artificial intelligence, and computing infrastructures. He was an organizer and a TPC member of several international conferences and workshops.

MASSIMO FARINA received the M.S. degree in law from the University of Cagliari, Italy, and the Ph.D. degree in computer law from the University of Bologna, Italy. Since 2006, he has been an Assistant Professor of computer and new technologies law with the Department of Electrical and Electronic Engineering (DIEE), University of Cagliari, where he is currently a Data Protection Officer. He is also a Coordinator of ICT4Law and Forensics. His research interests include data protection, computer crimes, digital forensics, and juridical protection of software.

ALESSANDRO BONU is currently a Contract Lecturer in computer forensics techniques, such as a module of the computer engineering, cybersecurity, and artificial intelligence course, with the University of Cagliari. In December 2011, he joined the Abissi Team as a Project Manager, the Head of Cyber Forensics Assets and Supports, and the CEO of governance activities. He has 20 years of experience as a Systems Infrastructure and Security Engineer with Tiscali S.p.A. and Engineering S.p.A. During the career, various certifications and specializations have been achieved. He is a digital forensics activity specialist, CTU, partner of CLUSIT, and AIP ITCS. During the career, various certifications and specializations have been achieved. He is a digital forensics activity specialist, CTU, partner of CLUSIT, and AIP ITCS. He collaborates closely with the DirICTo Network and the ICT4 Law and Forensics Laboratory, Department of Electrical and Electronic Engineering, University of Cagliari, for activities related to computer forensics and digital investigation.

DANIELE D. GIUSTO (Senior Member, IEEE) received the Laurea (M.S.) degree in electronic engineering and the Dottorato di Ricerca (Ph.D.) degree in telecommunications from the University of Genoa, Genoa, Italy, in 1986 and 1990, respectively. Since 2002, he has been a Full Professor of telecommunications with the University of Cagliari, Cagliari, Italy, where he has been a permanent Faculty Member with the Department of Electrical and Electronic Engineering, since 1994. His research interests include smart cities, sensor networks and the IoT, mobile and professional networks, and digital media. He was a recipient of the IEEE Chester Sall Paper Award, in 1998, and the AEI Ottavio Bonazzi Best Paper Award, in 1993. He was the Italian Head of Delegation in the ISO-JPEG Committee, from 1999 to 2018. He has been the Italian Head of Delegation in the ISO-Smart Cities Committee, since its foundation in 2016. He was a member of the IEEE Standard Committee, from 2007 to 2010.

Open Access funding provided by 'Università degli Studi di Cagliari' within the CRUI CARE Agreement