Advances in Intelligent Systems and Computing 932

Álvaro Rocha
Hojjat Adeli
Luís Paulo Reis
Sandra Costanzo *Editors*

New Knowledge in Information Systems and Technologies

Volume 3

Springer

Mobile CrowdSensing Privacy

Teresa Guarda[1,2,3(✉)], Maria Fernanda Augusto[1,4], and Isabel Lopes[3,5]

[1] Universidad Estatal Península de Santa Elena – UPSE, La Libertad, Ecuador
tguarda@gmail.com, mfg.augusto@gmail.com
[2] Universidad de las Fuerzas Armadas-ESPE, Sangolqui, Quito, Ecuador
[3] Algoritmi Centre, Minho University, Guimarães, Portugal
isalopes@ipb.pt
[4] BITrum-Research Group, C/ San Lorenzo 2, 24007 León, Spain
[5] UNIAG (Applied Management Research Unit), Polytechnic Institute of Bragança, Bragança, Portugal

Abstract. Information and communication technologies have been evolving rapidly, providing more and more alternative ways of accessing information, accessible through multiple paths and devices, transforming IoT into a giant digital system. This heterogeneous diversity ecosystem allows travel to the CrowdSensing era. Information in its role of reducing uncertainty is responsible for finding ways and shortcuts that increase efficiency and reduce the waste of time in the decision-making process. The massive spread of IoT devices has led to CrowdSensing, a sensor-based ecosystem of many different formats and technologies, in which information created by sensors is essential for decision-making processes and for improving business process efficiency. Service providers are beginning to design new business models that consider the smart things scenario, providing sensing as a service (SaaS). This article aims to provide insight into the Mobile CrowdSensing application environment by focusing on issues related to privacy of participant.

Keywords: IoT · Sensing · Mobile CrowdSensing · Privacy

1 Introduction

Wireless technologies, sensor networks, smart, wearable networks, coupled with new IoT models and the diffusion of their uses, are creating new sources of business value, and bringing numerous challenges to privacy, security, and data integrity [1].

Gartner estimates that by 2020, 20 billion things will be connected to the Internet, including smartphones, computers, and dedicated-function objects. Mentioning that IoT will have a major impact on the economy, turning many businesses into digital businesses and facilitating new business models [2].

In 2020, Gartner estimates internet-connected things will outnumber humans 4-to-1, creating new dynamics for marketing, sales and customer service [2].

Cloud computing, and mobile devices are the primary assistant for the reception and use of sensors information. Currently in the Smart Cities, each citizen with a mobile device becomes a provider of relevant information to improve the public

Á. Rocha et al. (Eds.): WorldCIST'19 2019, AISC 932, pp. 621–628, 2019.
https://doi.org/10.1007/978-3-030-16187-3_60

administration. Smartphones are equipped with a number of embedded sensors such as GPS, accelerometer, gyroscope, brightness, microphone, camera and others that allow the detection of environmental data, and so they can be interpreted and processed by various applications, creating this global scenario the opportunity for the development of applications that make use of the ability to detect mobile devices, transforming the collected data into useful information [3].

The scope of CrowdSensing is a newly application paradigm that enables ubiquitous mobile devices with enhanced sensor capabilities to collect and share local information toward a common goal [4]. Sensing devices potentially collect confidential data from individuals, being privacy a key problem [5]. The sensing data must be protected against unauthorized access, being CrowdSensing participant privacy an emerging challenge.

The aim of this article is to provide an insight into the Mobile Crowd Sensing application environment by focusing on issues related to privacy of participant in CrowdSensing systems.

In Sect. 2 we present the MCS concepts. After in Sect. 3, some MCS privacy threats are presented. Finally, in Sect. 4 we presents some final considerations.

2 Mobile CrowdSensing

The process of sensing is used in the management of Smart Cities through the monitoring of urban areas and observation of the dynamics of communities, aiming to provide managers with information essential for decision-making on a wide range of subjects, such as the sensing of environmental factors allow authorities or agencies to obtain data and inform the public about traffic conditions, noise pollution, air pollution, water quality, public safety, among other things, informing what happens, when and what happens when something happens [6].

In the context of smart cities, sensing combines the omnipresence of smartphones with the ability of sensors to collect data that depict different aspects of the city, being used to improve citizens' lives and to help decision makers in city management [3].

A new sensing paradigm called Mobile CrowdSensing (MCS) has been taking advantage of the wide range of capabilities to monitor and share common interest information collected through sensors embedded in mobile devices to support individuals and businesses in the decision-making process [7]. The collection can be carried out opportunistically or in a participatory way. In an opportunistic way the user initially has access to the application for data sensing, and later sends autonomously the detected data to a back-end server for processing; in turn, in the participatory way, users performs an action through the smartphone providing the sensed data [8–10].

MCS refers to the great diversity and heterogeneity of sensors through which individuals collectively share data and extract information to measure and map phenomena of common interest [11], and uses mobile devices equipped with sensors to collect data from the surrounding environment [10].

MCS provides a new way of seeing and perceiving the world, involving anyone in the process of sensing, allowing to increase the service of IoT, as well build smarter heterogeneous networks that interconnect things with things, things with people, and

people with people [12]. Being MCS environments highly dynamic, where mobile devices, the data type of each sensor and the quality in terms of accuracy, latency and reliability can change randomly [3, 13].

MCS uses crowd sourcing for large-scale sensing, leveraging the mobility and sensing capabilities of participants' devices as well as the existing communication infrastructure, making deployment easier and reducing costs, since it is not necessary to build a specific infrastructure, as in conventional sensors networks [13].

Compared to other sensing approaches with user participation, in the case of MCS, all data collection and information actions (registration) are done from the mobile device of the participating user of the service, connected to any Internet access network [14], often without the need to register in real time.

The overall model of activities to be developed in MCS has three dimensions: Sensing activity, Data generation; and Data processing (Fig. 1). In the 1st dimension, activities are defined according to the objectives outlined, and an application is created \made available to the participants. The 2nd dimension, data generation can be performed in the individual context by mobile sensing, or in the social context in mobile social networks (MSN), including all data collection and registration. In the 3th dimension is carried out the processing of the data collected from all the participants, to post prior dissemination of results.

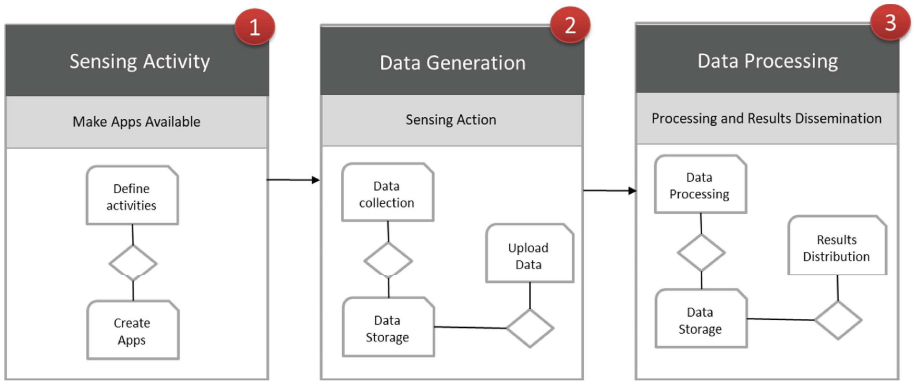

Fig. 1. Mobile CrowdSensing activities model dimensions.

Table 1. Mobile CrowdSensing categories.

Categories	Description
Environmental	*Monitoring natural phenomena such as levels of noise or pollution in a particular city. These applications allow the monitoring of several large-scale environmental phenomena*
Infrastructure	*Include large-scale phenomena related to public infrastructure. Examples of this type of application include the road conditions, availability of parking, traffic congestion measurement in real time, among others*
Social	*Participants share monitored information among themselves to collaborate for a common cause*

MCS applications can be classified into three different categories based on the type of phenomena to be monitored: environmental; infrastructure; and social [15] (Table 1).

3 Participant Privacy

WP29 (Article 29 Data Protection Working Party), European privacy and data protection adviser, established by Article 29 of Directive 95/46/EC, has decided to give a specific opinion on the consideration that IoT represents a large number of privacy and data protection challenges, some of which are new and other traditional ones, which will increase simultaneously with the exponential increase of data processing, resulting from the continuous evolution of IoT.

WP29 identifies the following privacy and data protection challenges in IoT: lack of control and asymmetry of information; quality of user consent; redefinition of the original data processing; identification of patterns and relationships; and limitations on the possibility of maintaining anonymity when using services (Table 2). And these are also the challenge of MCS.

Sensing devices potentially collect sensitive data from individuals [5], being privacy a key problem. Data captured by sensing must be protected against unauthorized (unauthorized) access, and be used only for the efficiency of some CrowdSensing services or activity to be performed. And that should be done with the knowledge and endorsement of who is making the information available (the participant), complying with the data protection laws in force in the country.

The guarantee of privacy is one of the pillars of modern society and the rule of law. It can be defined as a right of control by the individual about the circulation of their personal information, a right to not have their data registered or used by third parties.

GPS sensor readings usually record private information of participants, and when GPS sensing data are sharing participants' privacy can be compromised. Therefore, it is necessary to preserve the security and privacy of the participant.

On the other hand, in MCS systems, personal information may not be obtained directly, but inferred from aggregated data, as is the case of objects\things with RFID tags, which allow the user to be traced and identified and may create privacy problems. Sharing personal data on MCS systems can raise privacy concerns. it is essential that new techniques for protecting user privacy are developed, allowing their devices to contribute reliably. Then it's necessary to ensure that participants' data are not disclosed to unreliable third parties

Privacy is the right of each individual to maintain and control the set of information that surrounds him or her and may decide whether, when, why and by whom this information can be obtained and used. Due to MCS unique characteristics, privacy involves the right of the user/participant to remain intruder-free, and autonomous. The privacy in MCS has concerns with the direct disclosure of the identity of the participants as well as with the disclosure of sensitive attributes that allow to infer about the identity of the participants [13, 15].

From the participants' point of view, privacy threats can occur when the participant receives a specific task and shares their preferences during the assignment of this task

Table 2. WP29 privacy and data protection challenges in IoT.

Challenges	Description
Lack of control and asymmetry of information	The interaction between objects that communicate automatically, and between objects and back-end systems will result in the generation of data streams that can hardly be controlled with the traditional tools used to ensure the proper protection of the interests and rights of the data subjects. This issue of lack of control also concerns areas such as cloud computing or big data, and is even more challenging when it is thought that different emerging technologies can be used in combination, as is the case with MCS
Quality of user consent	*In many cases, the user may not be aware of the processing of data by certain devices. The possibility of rejecting certain services is not a viable alternative in IoT, and the classic mechanisms used to obtain consent are difficult to apply. Therefore, new ways of obtaining user consent for connected devices should be considered by their manufacturers*
Redefinition of the original data processing	*The increased amount of data generated by IoT in combination with modern data analysis and cross-matching techniques may give rise to secondary uses of the same data, whether or not related to the processing purpose initially assigned to the devices. That is, apparently insignificant data collected from devices can be used to infer information with a totally different purpose from the initial one*
Identification of patterns and relationships	*Although each device generates data streams in isolation, its collection and subsequent analysis can easily reveal individual patterns, behavior, preferences and habits. As seen in the redefinition of the original data processing, knowledge can be generated from trivial information, through profiling the sensor data*
Limitations on the possibility of maintaining anonymity when using services	*The full development of IoT capabilities can put pressure on the current possibilities of anonymous use of services and limit the possibility of remaining anonymous*

or notifies the server that accepted the task, in this case some attributes such as location, types of tasks in which the participant is interested, as well as some attributes of the sensor can be revealed [16]. In this case it is possible to argue that this information alone may not violate privacy, but may allow the "attacker" to track the tasks selected by the participant and thus reveal their identity or other sensitive attributes [17]. Among

the attributes that can be used to track participants we can refer participant IDs and IP addresses, then participant's privacy must be protected at device level when communicating with the server, on server storage, and on processing.

As a way to maintain the privacy of participants various techniques are used: user preferences; anonymity; user preferences; anonymity in the distribution of tasks; Data Disturbance (see Table 3) [16, 17] [18].

Table 3. Techniques to maintain the privacy of participants.

Techniques	Description
Anonymity	*Although the use of anonymity techniques is very white, the intent is to remove any information that may identify participants or other entities during the distribution and performance of tasks*
User preferences	*Allow participants to configure their privacy preferences, thus enabling them to control the data collection process to be sensed*
Anonymity in the distribution of tasks	*Data collection from a sensor is usually triggered by tasks that specify the sensing modes based on, so tasks are only distributed to devices that meet the requirements of these*
Data disturbance	*Data disturbance adds noise to the sensor data before it is shared, and noise can be added to the data without compromising its accuracy*

4 Conclusions

At present cloud storage mechanisms are mature, sensor technologies and the evolution of IoT implementation models are quite accelerated, and the access devices are ready.

With the evolution of mobile computing, MCS emerges as a new term referring to the sharing of information collected from different mobile devices in order to measure and map phenomena of common interest. In order to perform this collection, there are two possible ways: in a participatory way, where the users exercise an action through the smartphone and make the data available; and opportunistically, where the user initially releases the application's access to the sensed data and the latter, in turn, almost autonomously, sends the data to a back-end server for processing.

Assuming that millions of individuals have at least one mobile device, CrowdSensing applications emerge as an inexpensive and time-consuming alternative, reducing efforts for the development of specialized sensor infrastructures.

Lacking the analytical mechanisms that allow efficiency gains from debugging the information generated by the CrowdSensing, the synchronization between the different technologies and IoT makes the MCS era a reality, which is possible with the sum of the technologies and tools of analysis, with the services of companies specialized in projects of crow sensing, thus making the sensing as a service.

MCS applications are gaining in popularity due to the creation of diverse systems and applications, conquering and involving more and more people, networks and group

of collaborators. In the other hand, the use of MCS also has its risks, in this context privacy.

In spite of the privacy techniques, the participant's privacy must be one of the fundamental points in the construction of future comprehensive privacy-preserving architecture.

References

1. Guarda, T., Bustos, S., Torres, W., Villao, F.: Botnets the cat-mouse hunting. In: 2018 International Conference on Digital Science (2018)
2. Gartner: Leading the IoT. Gartner Insights on How to Lead. Mark Hung, Gartner Research Vice President (2017)
3. Guarda, T., Augusto, M.F., Díaz-Nafría, J.M.: Crowd sensing and delay tolerant networks to support decision making at the routing level. In: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (2018)
4. Khan, W.Z., Xiang, Y., Aalsalem, M.Y., Arshad, Q.: Mobile phone sensing systems: a survey. IEEE Commun. Surv. Tutor. **15**(1), 402–427 (2013)
5. Chen, Y., Zhou, J., Guo, M.: A context-aware search system for internet of things based on hierarchical context. Telecommun. Syst. **62**(1), 77–91 (2016)
6. Theunis, J., Stevens, M., Botteldooren, D.: Sensing the environment. In: Participatory Sensing, Opinions and Collective Awareness, pp. 21–46 (2017)
7. Guo, B., Yu, Z., Zhou, X., Zhang, D.: From participatory sensing to mobile crowd sensing. In: International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops) (2014)
8. Miorandi, D., Carreras, I., Gregori, E., Graham, I., Stewart, J.: Measuring net neutrality in mobile Internet: towards a crowdsensing-based citizen observatory. In: IEEE International Conference on Communications Workshops (ICC), pp. 199–203 (2013)
9. Liu, J., Shen, H., Zhang, X.: A survey of mobile crowdsensing techniques: a critical component for the internet of things. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6 (2016)
10. Guo, B., Wang, Z., Yu, Z., Wang, Y., Yen, N.Y., Huang, R., Zhou, X.: Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm. In: International Conference on ACM Computing Surveys (CSUR) (2015)
11. Peng, D., Wu, F., Chen, G.: Pay as how well you do: a quality based incentive mechanism for crowdsensing. In: Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (2015)
12. Jian, A., Xiaolin, G., Jianwei, Y., Yu, S., Xin, H.: Mobile crowd sensing for internet of things: a credible crowdsourcing model in mobile-sense service. In: International Conference on Multimedia Big Data (BigMM) (2015)
13. Han, G., Liu, L., Chan, S., Yu, R., Yang, Y.: HySense: a hybrid mobile crowdsensing framework for sensing opportunities compensation under dynamic coverage constraint. Commun. Mag. **55**(3), 93–99 (2017)
14. Bellavista, P., Corradi, A., Foschini, L., Ianniello, R.: Scalable and cost-effective assignment of mobile crowdsensing tasks based on profiling trends and prediction: the participact living lab experience. Sensors **15**(8), 18613–18640 (2015)
15. Biskup, J.: Security in Computing Systems: Challenges, Approaches and Solutions. Springer, Heidelberg (2008)

16. Chon, Y., Lane, N.D., Kim, Y., Zhao, F., Cha, H.: Understanding the coverage and scalability of place-centric crowdsensing. In: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (2013)
17. Pournajaf, L., Garcia-Ulloa, D.A., Xiong, L., Sunderam, V.: Participant privacy in mobile crowd sensing task management: a survey of methods and challenges. ACM SIGMOD Rec. **44**(4), 23–34 (2016)