Privacy and Security of Mobile Users in Smart Cities: A Reference Architecture

Sabrina Ichou*, Slimane Hammoudi†, Amel Benna‡, Abdelkrim Meziane‡ and Alfredo Cuzzocrea§

*ESI
Algiers, Algeria
s_ichou@esi.dz

†ESEO-TECH
Angers, France
Slimane.Hammoudi@eseo.fr

‡CERIST
Algiers, Algeria
{abenna,ameziane}@cerist.dz

§University of Calabria
Rende, Italy
alfredo.cuzzocrea@unical.it

Abstract—Privacy and Security in big data and smart cities play a major role to ensure better quality of citizens life. Privacy emphasizes on the data being collected, shared, and used in the right manner, and security focuses on protecting the data from intruders' attack, and exploitation of data for other purposes such as criminal behavior. This paper aims to discuss the issue of privacy and security of mobile users in big data and smart cities. First, based on big data privacy and security challenges, classification, and models, we identify the privacy and security requirements for a mobile user. Then, we propose a generic architecture and an algorithm for the management of privacy and security of a mobile user in a smart environment. This architecture groups the main components required for implementing the proposed algorithm that ensure the privacy and security of mobile users in smart cities.

Index Terms—Privacy, Security, Mobile Users, Big Data.

I. INTRODUCTION

Smart cities have become one of the main trends in Information and communication Technologies (ICT) where different means are made available in the city (e.g., sensor networks, open data platforms, expert systems) to collect and analyze different data for the purpose of informing and recommending services to citizens [8], [20].

In the above literature, several methods and paradigms are explored in order to protect the privacy and security of the mobile user in smart city [14], [22], [24], among which the privacy and security in the context of Big data [10], [23]. Indeed, a huge quantity of data is provided by the mobility and activities of mobile users in smart cities.

The term Big Data has garnered widespread attention in academia, industrial community, businesses and society, and has continued to grow exponentially since then [3], [5], [13]. Although some scholars assume big data originated in the mid-nineties, with no reports of published literature work for over a decade [16].

With the rapid development of the Internet, mobile users leave a lot of data traces on the Internet every day, leading to data stream analytics paradigms [6], [7], [17]). With the lack of privacy and security mechanisms, criminals could collect information on the Internet and then conduct illegal activities such as reselling, fraud, etc., which have seriously affected social stability and harmony [19]. From an external risk perspective, there are multiple occurrences of cyber security hackers breaking into multiple private electronic databases, linking fields together, and subsequently leveraging that data to obtain confidential information [21].

We aim in this work to discuss the issue of mobile user privacy and security. More precisely, we aim to make the following contributions:

1) Identify the main requirements that should be met in the development of privacy and security of a mobile user in smart cities.
2) Present a generic architecture and an algorithm for privacy and security of a mobile user in smart cities based on the proposed requirements.

The rest of this paper is organized as follows: Section 2 identifies the requirements of privacy and security of a mobile user. Section 3 provides an architecture and an algorithm for the management of privacy and security for the mobile user based on the defined requirements. Section 4 is a summary of some related works. Section 5 concludes the paper and presents some future works.

II. BACKGROUND

This section introduces the privacy and security challenges of mobile users, the classification of privacy and security in big-data, and the privacy protection and security models.