Location Privacy in Smart Cities Era

Raed Al-Dhubhani[1(✉)], Rashid Mehmood[2], Iyad Katib[1],
and Abdullah Algarni[1]

[1] Department of Computer Science,
FCIT, King Abdulaziz University, Jeddah 21589, Saudi Arabia
raldhubhani@stu.kau.edu.sa,
{iakatib,amsalgarni}@kau.edu.sa
[2] High Performance Computing Center, King Abdulaziz University,
Jeddah 21589, Saudi Arabia
Rmehmood@kau.edu.sa

Abstract. In recent years, smart city concept was proposed to provide sustainable development to the cities and improve the quality of citizens' life by utilizing the information and communication technologies. To achieve that, smart city applications are expected to use IoT infrastructure to collect and integrate data continuously about the environment and citizens, and take actions based on the constructed knowledge. Indeed, identification and tracking technologies are essential to develop such context-aware applications. Therefore, citizens are expected to be surrounded by smart devices which continuously identify, track and process their daily activities. Location privacy is one of the important issues which should be addressed carefully. Preserving location privacy means that the released sensitive location data of citizens are used only for the desired purpose. In reality, adopting the citizens' for smart city applications depends on their trust on the used technologies. In this paper, we review smart city architectures, frameworks, and platforms to highlight to what extent preserving location privacy is addressed. We show that preserving location privacy in smart city applications does not get the required attention. We discuss the issues, which we think should be addressed to improve location privacy preservation for smart city applications. Accordingly, we propose a location privacy preservation system for smart city applications.

Keywords: Location privacy · Smart cities · IoT

1 Introduction

An increase in the ratio of world's population that live in urban areas is estimated to rise from 50.5% in 2010 to 59% by 2030 [1]. Due to the population growth, large cities are expected to encounter challenges, such as resources exhaustion, traffic congestion, and air pollution. The concept of smart city has emerged as a result of the need to mitigate the effects of the cities' population growth by introducing an effective management for the city's infrastructures and resources. In addition, urban planning and policy making can be optimized using such technologies. Smart city applications are

R. Mehmood et al. (Eds.): SCITA 2017, LNICST 224, pp. 123–138, 2018.
https://doi.org/10.1007/978-3-319-94180-6_14

predicted to improve the citizens' quality of life by addressing important sectors such as healthcare [2], transportation [3], energy [4], education [5], and public safety [6].

In recent years, many smart city projects were implemented around the world, which aim to provide smart environment, smart mobility, and smart living for citizens [7]. For instance, a smart city application was developed to improve the transportation system in Singapore [8]. One of its main features is the capability to predict in advance the availability of parking spaces at the driver's destination on the expected arrival time. To get an effective management of a smart city's resources, citizens should be continuously connected to the Internet [7]. Technologies such as big data and computational intelligence are expected to play an important role in manipulating the huge amount of data collected by citizens to meet the goals of smart cities [9, 10].

According to [11], IoT is defined as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment". It is expected that by 2020, the number of Internet of Things (IoT) devices will be 50 billion while the world population will be 7.6 billion [12]. As expected, IoT represents the best infrastructure for smart city applications.

Despite their benefits, IoT devices are expected to significantly increase the threats of the individuals' privacy leakage. In fact, citizens will be surrounded by IoT devices which are continuously monitoring and reporting the status and activities happening in the environment. According to [13], life in a smart city is the same as life under surveillance. Therefore, the challenge is how to ensure the privacy and security of a huge amount of data gathered by a variety of autonomous devices in a heterogeneous environment through the sensing, transmitting, processing, and storing phases. In addition to that, using localization-enabled devices introduces the risk of the unauthorized tracking of citizens. Clearly, providing secure, trustworthy, and privacy-preserving IoT infrastructure is essential to the success of IoT deployment [14]. In other words, the shortcoming of addressing such issues in IoT will limit the citizens' adoption for smart city applications.

Privacy preserving is a fundamental human right which is protected by international and national laws. It represents one of the main issues which should be addressed in smart cities and IoT context. According to [14], there are two main principles which should be followed in developing any IoT system to gain the users' trust. The first principle states that the user privacy should not be violated, while the second principle emphasizes the need to maintain the user's control over his/her related operations. In smart cities, the citizens' privacy is identified in five dimensions [15]. These dimension are: owner privacy, identity privacy, location privacy, footprint privacy, and query privacy.

Location privacy is one of the important privacy dimensions which should be addressed carefully. In fact, anonymizing the location data is not enough, while using background knowledge (e.g. geographic maps) could lead to re-identify the user who produces the location data [16]. According to [17], location privacy is defined as "a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others". In [18], a survey was conducted to analyze to what extent the users accept sharing and trading their location data. The survey shows that the respondents realize the privacy risks resulted from sharing their location data. At the same time, the survey shows that their willingness to share the location data depends on many factors, such as the context, the expected benefits, and the trust level in the party which the data will be shared with. Therefore, preserving location privacy is essential to get the citizens' trust in IoT infrastructure and smart city applications. According to [19], privacy by design is the best practice to overcome the privacy threats. In recent years, many smart city architectures, frameworks, and platforms are proposed, which take into consideration the security and privacy issues. In many case, the goal is to provide an end-to-end security and privacy.

In this paper, we review smart city architectures, frameworks, and platforms to highlight to what extent preserving location privacy is addressed. We show that preserving location privacy in smart city applications does not get the required attention. We discuss the issues, which we think should be addressed to preserve location privacy in smart city applications. We propose location privacy preservation system for smart city applications.

2 State of the Art

In recent years, many architectures, frameworks, and platforms are developed for IoT-based applications in general, and for smart city applications in particular. They show a wide variation in addressing the privacy and security issues. In some cases, a limited support is provided, while in others the goal is to provide an end-to-end privacy and security support. In this section, we review the main works in this area, and discuss how particularly the location privacy is addressed. We show that preserving location privacy is either supported partially or supported for very specific use cases. This emphasizes that preserving location privacy does not get the required attention to address all its related requirements.

In [20], an architecture for smart cities is proposed (see Fig. 1). In this architecture, three stakeholders are identified to access the data collected by IoT devices. The stakeholders are the citizens, community service providers, and city management. The proposed architecture consists of control and services layer, network layer, and sensing layer. Using cloud computing is proposed to overcome the big data issues. The architecture is proposed to support two types of services, which are Individual services and community service. For each type of service, a control center is used, which contains a web interface, service management, database management, and knowledge discovery section. The sensing layer entities send their data through the network layer to the control center, where it is processed on the fly and then stored in the database. In this architecture, the privacy features are proposed to be implemented in the control and services layer.

In [21], a framework is proposed to address the citizen's privacy concerns regarding the smart city technologies by proposing two dimensions. The first dimension represents how the citizens classify the data by identifying it as personal or impersonal. The second dimension represents the classification according to the data collection purpose, which is either service consumption purpose or surveillance purpose. The two dimensions provides four different areas for the framework, such that each area has its own characteristics regarding the citizen's privacy concerns. The areas

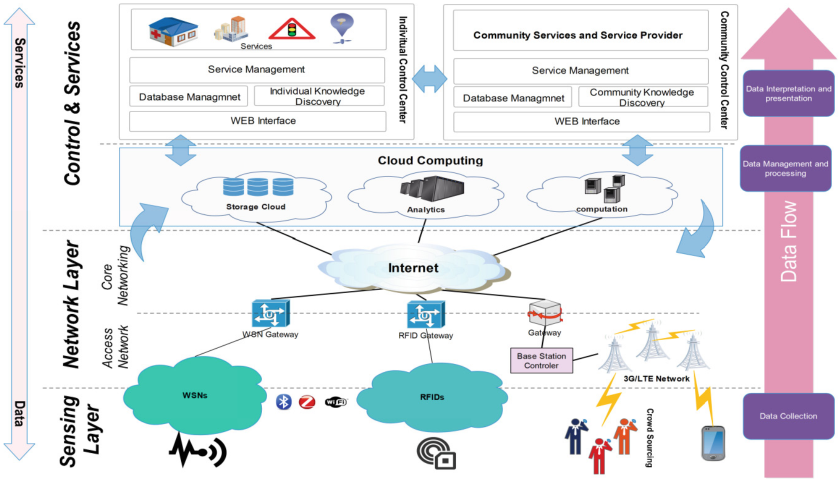

Fig. 1. The proposed smart city architecture in [20]

are: personal data for surveillance purposes, personal data for service purposes, impersonal data for surveillance purposes, and impersonal data for service purposes.

In [22], SSServProv is proposed as a security and privacy-aware framework for service provisioning in smart cities (see Fig. 2). The framework provides end-to-end privacy and security features. A detailed list of stakeholders is identified, and the contribution of each in smart city applications is modeled. Eight main roles are identified for stakeholders, which are service consumers, trusted service providers, untrusted service providers, IT specialists, data custodians, standard governing bodies, domain experts, and others. The security and privacy are addressed for all stakeholders, by

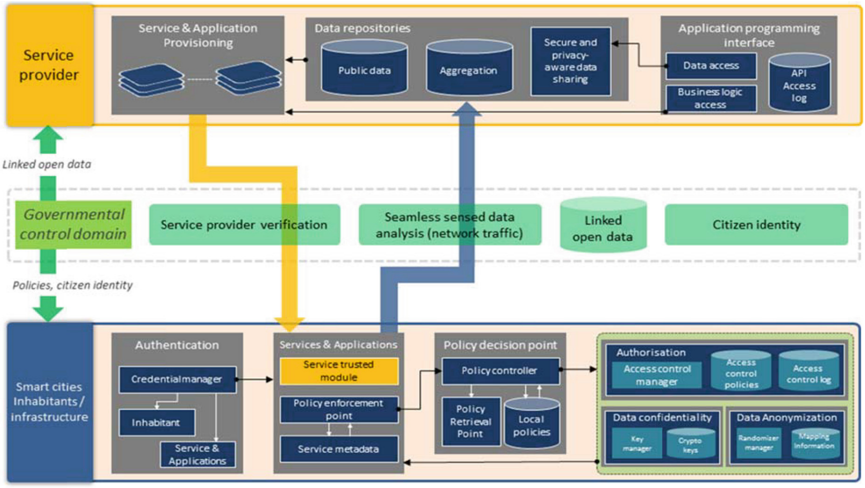

Fig. 2. SSServProv framework [22]

taking into consideration that each stakeholder could be a victim or an attacker. The governmental control domain is proposed in this framework as the controlling authority, which ensures the commitment of service providers and citizens to the defined policies and regulations. The governmental control domain has the following components: service provider verification, citizen identity, seamless sensed data analysis, and linked open data. The proposed components in the citizens and infrastructure layer are: authentication, services and applications, policy decision point, authorization, data confidentiality, and data anonymization. For the service provider layer, the components are: service and application provisioning, data repositories, and application programming interface.

In [23], a framework for smart cities is proposed (see Fig. 3). Three layers are defined in the framework, which are the information world, the communication world, and the physical world. The identified framework components are sensing components, heterogeneous network, processing unit, and control and operating components. Using existing privacy and security solutions is proposed to provide the privacy and security features, like access control, anonymity, and encryption.

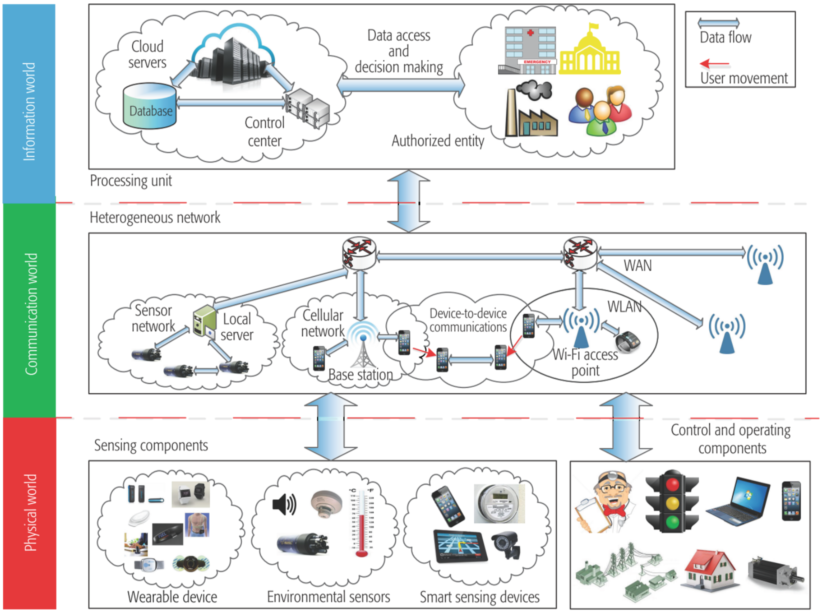

Fig. 3. The proposed framework in [23]

IoT-A was introduced by one of the European FP7 projects as an Architecture Reference Model for Internet of Things [24]. IoT-A aims to facilitate the development of IoT-related solutions by providing an efficient integration to the service layer, and hence enabling the interoperability of IoT systems. To achieve that, a set of concepts and relations are defined, which can be used to construct an abstract view for IoT entities relationships. IoT-A defines five models which are Domain Model, Functional Model, Communication Model, Information Model, and Trust, privacy, and security model. The domain model is a structural perspective which represents the Virtual Entities and their attributes and relationships. The domain model uses the following concepts: User, Virtual Entity, Physical Entity, Augmented Entity, Resource, Device, and Service. The interaction between a User and a Physical Entity is done through a Service, where each Virtual Entity represents a Physical Entity in the digital world. Composing a Physical Entity and its associated Virtual Entity represents an Augmented Entity. The relationship between the Physical Entity and its corresponding Virtual Entity is accomplished by using one or more ICT Devices which facilitate the interaction and information gathering about the Physical Entity. There are three types of ICT Devices: Sensors, Tags, and Actuators. Resource is a software component which is used to provide data from or actuate a Physical Entity. To make the Resource accessible, it is attached to a Service. Functional model identifies a set of Functionality Groups and their interactions (see Fig. 4). Trust, security, and privacy model are addressed by using the components: Identity Management, Authentication, Authorization, Trust and Reputation, and Key Exchange and Management. To achieve the privacy, IoT-A requires the following properties:

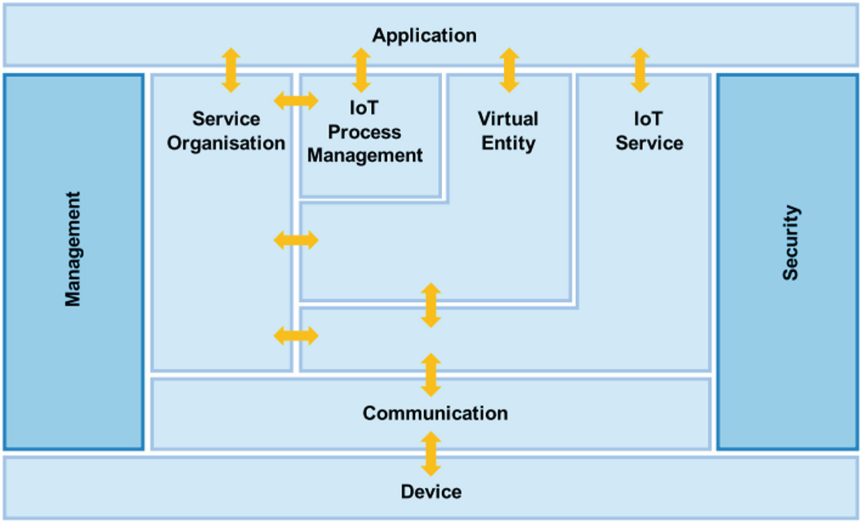

Fig. 4. Functional model of IoT-A [25]

- The subject has the option to share or not to share the data.
- The subject has full control on the used privacy mechanism.
- The subject has the option to decide the purpose for which the collected data should be used.
- The subject is notified who uses the data and when.
- Disclosing the data of the subject is kept strictly for the needed data only, and the anonymization is used whenever possible.

- Aggregating or reasoning the subject's disclosed data does not lead to infer the identity of the subject.
- The subject's data is used only for the agreed purpose and not used beyond that purpose.

In IoT-A, location privacy does not get the required attention, where it is addressed by a suggestion to use Identity management component to provide anonymization for location data.

OpenIoT is an open source IoT platform which enables the interoperability of IoT services in the cloud [26]. The aim of OpenIoT is to integrate the heterogeneous sensor networks and IoT services in one platform. The sensors middleware is one of the main components in OpenIoT which facilitates the data collection from virtually any sensor. In OpenIoT, collecting and discovering data are implemented using Publish/Subscribe principles. To provide security and privacy, OpenIoT implements following components: identity management, authentication, and authorization. In OpenIoT, location privacy is not addressed, because no specific component has been implemented to manipulate the location privacy.

COMPOSE is an open source IoT-based platform for developing smart city applications [27]. To address the privacy and security issues, COMPOSE implements the following components: Identity Management, Security Monitors, Policy Decision Points, Service Instrumentation, Static Analysis, Authentication-Authorization-Accounting (AAA) Manager, Provenance Manager, and Trust and Reputation Manager. Data Provenance is metadata which is used for logging all data transactions between different COMPOSE entities. Trust and Reputation component provides an estimation of the trustfulness of data sources within Compose based on the popularity and the data accuracy of the data sources. Policy decision points are used to enforce the security and privacy requirements. In COMPOSE, location privacy is not addressed, because no specific component has been implemented to manipulate the location privacy.

FIWARE is a European project which aims to provide the core platform of the Future Internet to facilitate the development of IoT based applications and smart city applications [28]. FIWARE platform consists of open source components called Generic Enablers which are public and open source. FIWARE platform provides many Generic Enablers to support the security and privacy requirements. For preserving location privacy, Location Generic Enabler applies authentication and authorization techniques to provide the location data using three levels of location data accuracy, which are low, medium and high.

Secure and sMARter ciTIEs data management (SMARTIE) is an IoT-based platform for smart city applications [29]. SMARTIE was developed based on IoT-A. The aim of developing SMARTIE is to provide a secure platform which has the capability to store, process, and share large volume of data collected by heterogeneous IoT devices. Security, privacy, and trust are the main issues which are considered in developing SMARTIE platform. The vision is to deliver end-to-end security and trust and meeting the privacy requirements of the data owner's. SMARTIE is a policy-enabled platform which provides functional components to provide decentralized policy-based access control and encryption to the citizen's sensitive data. The functional components in the security functional group are: identity management, authentication, authorization, key exchange & management, and trust & reputation. To preserve the location privacy in SAMRTIE, PrivLoc is introduced as a component to prevent the location tracking in the geo-fencing services by applying coordinates translation [30].

COSMOS is a IoT-based framework which introduces the decentralized and autonomous management of IoT devices motivated by social media technologies [31]. The aim is to support smart city applications by providing smart, autonomous, and reliable things. The architecture of COSMOS is based on IoT-A. The aim of COSMOS is to deliver end-to-end privacy and security. The following components are used for providing the security and privacy: authentication, authorization, key management, integrity, accountability, nonrepudiation and privacy filters (Privelets). Privelets are introduced as privacy functional components which apply the data minimization principle to preserve the privacy by controlling the data sharing to be in the minimum level. To achieve that, Privelets use Fuzzy logic to share data by supporting three levels of data accuracy, which are low, medium, and high. In COSMOS, Privelets are used to preserve location privacy.

REliable, Resilient and secUre IoT for sMart city applications (RERUM) is a project which applies the concept of privacy, security, and reliability in design to the IoT devices for the smart city context [32]. It focuses on the development of IoT devices which are considered as the weakest point in IoT systems. To achieve that, lightweight and energy efficient security and privacy mechanisms are proposed to be implemented in the IoT devices. RERUM suggests embedding and running many components in the IoT devices, like device-to-device authentication, data encryption, secure storage, geo-location privacy, and trusted routing. The project provides an IoT-based framework for smart city applications. It proposes also a smart object hardware prototype which enables embedding the security and privacy in IoT devices. RERUM focuses on four use cases, which are: smart transportation, environmental monitoring, home energy management, and indoor comfort quality monitoring. The security functional components of RERUM are: integrity generator/verifier, data encrypter/decrypter, device-to-device authenticator, credential bootstrapping client/authority, policy enforcement point, identity agent, attribute need reporter, policy decision point, policy retrieval point, and secure storage. The privacy functional components of RERUM are: consent manager, privacy policy enforcement point, privacy dashboard, deactivator/activator of data collection, privacy policy checker, anonymization/pseudonym manager, de- pseudonymizer, and privacy enhancing technologies for geo-location. The trust functional components of RERUM are: trust configurator manager, reputation rules configurator, trust engine, inaccuracy alert producer, and inaccuracy alert reactor. In RERUM, preserving location privacy is provided by the privacy enhancing technologies for geo-location component which uses the aggregation vectors scheme. Aggregation vectors scheme generates a random number of vectors with random start and end points selected from the sensed location points, such that these random vectors are shared instead of the citizen's accurate location points.

3 The Shortcomings of Existing Works and Proposed Requirements

We have reviewed the various works related to location privacy for emerging smart city environments and it is clear that the existing proposals deal with location privacy at a much abstract level such as information privacy. Some works have dealt with location privacy on detailed level; however, these have failed to take account of correlation between multiple continuous locations of an individual and the correlation of locations across multiple individuals, devices and systems.

We therefore assert that, in order to preserve the location privacy in smart city environment, two main requirements should be satisfied. The first requirement is ensuring smart city applications receive only the minimum level of location data accuracy they need to operate. The second requirement is ensuring that correlating the location data collected by smart city applications will not lead to increasing the level of location accuracy released to these applications. Satisfying these requirements need a location obfuscation mechanism which has the capability to introduce customized levels of accuracy to provide the requirements of smart city applications and also preserve citizen's location privacy. In addition, measuring the location privacy leakage resulted from the shared location data is also required.

In addition, the following issues should be addresses to preserve the citizen's location privacy in smart city applications.

- Smart city applications are context-based, so the required level of location accuracy in normal situations may vary in emergency situations.
- Citizen's IoT devices should be grouped into clusters (e.g. home, work, mobile), such that each cluster has its own location privacy characteristics and hence its own required privacy policies.
- Applying the location privacy policies for a cluster of devices should be based on its type (stationary or mobile) and the corresponding potential privacy leakage.
- For stationary clusters (like home and work), they produce sensitive data about fixed locations, and obfuscating fixed locations should not cause privacy leakage which may lead to improve the accuracy of these fixed locations.
- On the other hand, mobile clusters require addressing the potential correlation produced by the continuous reporting of different obfuscated locations.
- The possibility that a smart city application can collect the citizen's location data from more than one IoT device requires applying correlation analysis to ensure that the collected data from different IoT devices can't be used to improve the location accuracy shared with the application.
- As a result of the need of smart city applications for continuous data collection, citizens should have the capability to customize policies to manage the location data sharing when they are located in areas which are identified as sensitive.
- The contribution of citizens to build a consolidated location profile using their location data is useful to indicate the privacy leakage produced by sharing the location data of the different city areas.

- It is required to address the correlation produced by an IoT device which collects and shares location data and can be linked to more than one citizen, especially if the device is installed in shared areas (e.g. home or office).

4 The Proposed Location Privacy Preservation System

The previous section presented the shortcomings of the state-of-the-art on location privacy preservation in smart cities. We also presented the requirements for and issues surrounding location privacy preservation in smart cities. This section proposes a location privacy preservation system aimed at smart cities. Figure 5 shows the architecture of the proposed system. The architecture has the following components: Context Analyzer, Devices Clustering Manager, Correlation Manager, Policies Manager, Obfuscation Manager, Personal Location Profile Manager, and Consolidated Location Profile Manager.

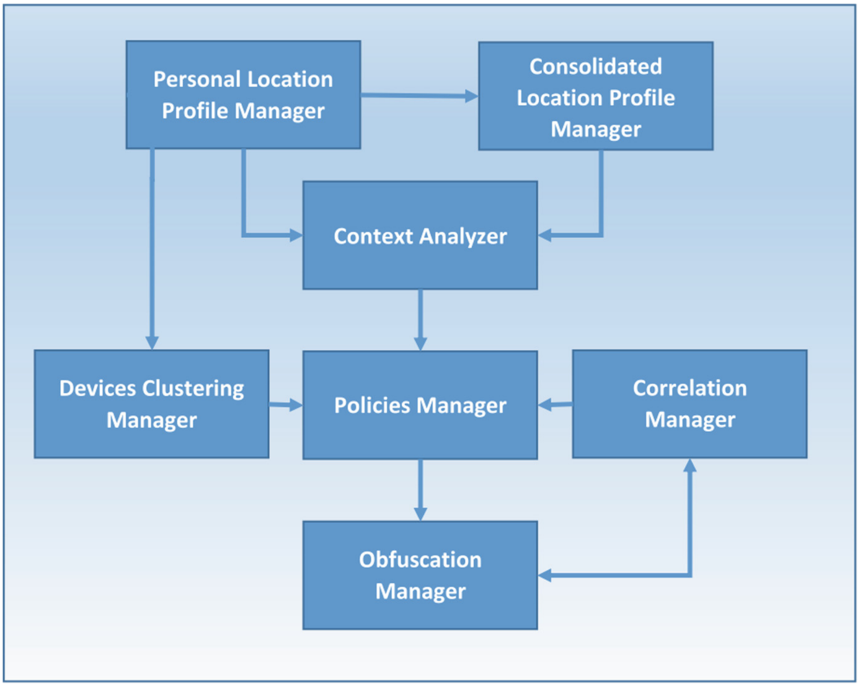
Personal Location Profile Manager
Consolidated Location Profile Manager
Context Analyzer
Devices Clustering Manager
Policies Manager
Correlation Manager
Obfuscation Manager

Fig. 5. Architecture of the proposed system

4.1 Context Analyzer

The purpose of this component is to notify the Policies Manager about the citizen's current context, in order to apply the corresponding policy. This component is required to identify when the citizen is located in a sensitive area, where applying specific policies with a higher level of location privacy is required. In addition, the component should identify emergency situations which requires applying specific policies for emergency situations which require sharing the citizen's location with high accuracy. The component uses Personal Location Profile to identify areas which are visited frequently by the citizen to apply a higher level of privacy policy on them. The Context Analyzer should use also Consolidated Location Profile which is created by all the citizens to identify the privacy level of the citizen's current area based on consolidated statistics.

4.2 Devices Clustering Manager

This component is responsible to manage the citizen's clusters of IoT devices that have the localization capability. Stationary and mobile clusters have different requirements in terms of location privacy, and hence require different policies. Therefore, the purpose of this component is to work with the policies manager to identify the required policies based on the cluster type which the IoT device belongs to. This component is responsible for managing the membership of IoT devices to the clusters, and when the membership of an IoT device should be changed from one cluster to another. For example, IoT devices which belong to the mobile cluster should be moved to the stationary clusters when the citizen reaches home.

4.3 Correlation Manager

This component aims to detect the potential privacy leakage produced by correlating the location data shared with smart city applications. First, sharing location data by multiple devices of a citizen to the same smart city application could produce privacy leakage. Second, sharing location data of multiple citizens sensed by the same device to the same smart city application could produce privacy leakage. This component works with the Policies Manager to ensure that the shared location data does not lead to privacy leakage.

4.4 Policies Manager

This component is responsible to manage sharing the location data by applying the required policy based on the current context, the involved cluster of IoT devices, and the detected level of privacy leakage by Correlation Manager. By specifying the suitable sharing policy, Policies Manager enforces the Obfuscation Manager to apply that policy.

4.5 Obfuscation Manager

Obfuscation Manager has the capability to apply different levels of obfuscation for citizen's location data to provide the minimum level of accuracy required to each smart city applications. Policies Manager controls the performance of Obfuscation Manager by choosing the required obfuscation level to enforce the selected policy.

4.6 Personal Location Profile Manager

This component is used to build a statistical profile about the citizen mobility. This component is used by the Context Analyzer to infer the locations which are frequently visited by the citizen, which requires applying higher levels of preserving privacy to ensure that they are not used to de-anonymize the citizen. This component works with the Policies Manager to apply policies with high level location privacy for these locations.

4.7 Consolidated Location Profile Manager

This component is used to build a consolidated profile about the mobility of all citizens to provide an overall mobility view. The objective is to provide consolidated statistics to the Context analyzer about the mobility patterns of citizens in the different areas which can be used to specify the required obfuscation levels based on the area mobility density.

5 Discussion

5.1 The Scenario

Alice and Bob are a couple who live in a smart city and have a smart autonomous vehicle. The city provides a smart transportation system for its citizens. To preserve the citizen's security and privacy, identity management and preserving location privacy systems are hosted in the secure and trusted ICT infrastructure of the city. To provide a reliable smart transportation service, the smart transportation system is hosted and operated by one of the international giant ICT service providers.

Identity management is used for three main purposes. First, it is used to ensure that the service is provided for legitimate citizens only. Second, it is used to block malfunctioned devices (e.g. as a result of a hardware failure or an attacked device) from providing the smart transportation service with invalid data. Third, it is used to provide the anonymization service for the citizens by providing pseudonyms to be used for accessing the smart transportation system.

The smart transportation system provides the traffic routing and prediction services. The routing service optimizes the trips routes of citizens in order to minimize their traveling time. In addition, it provides the priority for emergency vehicles (e.g. ambulance and firefighting) by re-routing other vehicles in the area to make space for emergency vehicles. It is used also to distribute the traffic through the city in a balanced way to keep the level of noise and air pollution within the allowed ranges. Finally, it provides instant notifications about the road status (e.g. accidents, closed roads, etc.). The predication service is used to estimate the expected travel time of trips.

The smart transportation application is installed in the smart autonomous vehicle. The application senses and shares the environment's noise and air pollution continuously. In addition, Alice and Bob use an app installed in their smart phones to connect to the smart transportation system to plan for their trips in advance and check the traffic status and the estimated travel time. The smart autonomous vehicle is equipped with a GPS sensor, noise sensor, and air pollution sensor.

Alice and Bob realize that providing their accurate locations to the smart transportation system enhance the service quality of smart transportation system. At the same time, they concern about their location privacy especially when they are at home and work, and when they visit a sensitive location (like hospitals, clinics and one of their frequent locations). Their goal is to ensure that sharing their location data with an overseas service provider will not lead to de-anonymize them by the service provider. They also concern about the privacy leakage caused by correlating their shared location data, which reduces their location privacy. They hope that their smart city provides a preserving location privacy system that enables them to configure a set of policies to preserve their location privacy.

To satisfy their location privacy needs, they propose the following policies:

- At home, the location should be obfuscated within a range of 500 m.
- At work, the location should be obfuscated within a range of 300 m.
- At sensitive and frequent locations, the location should be obfuscated within a range of 400 m.
- At low traffic density areas, the location should be obfuscated within a range of 200 m.
- In emergency cases (e.g. the existence of an ambulance in the surrounding area), the accurate location should be shared.
- Otherwise, the location should be obfuscated within a range of 30 m.
- The obfuscation process should take into consideration the potential privacy leakage resulted from correlating the shared location data.

5.2 Evaluation of the Proposed System

In this section, we discuss seven cases based on the scenario described in the previous section. We address realistic cases which happen for Alice and Bob when they go to work on any ordinary working day using their own autonomous vehicle. We show how our proposed system can manipulate these cases to preserve their location privacy.

Case 1: Alice and Bob leave home at 7 AM. Devices Clustering Manager detects that, changes the membership of their smart phones and smart vehicle from Home cluster to Mobile cluster, and finally notifies the Policies Manager to activate the proper policy. Policies Manager notifies the Obfuscation Manager to enforce the proper policy.

Case 2: On their way, the smart vehicle uses the obfuscated locations produced by the Obfuscation Manager to retrieve the routing information from the smart transportation system, and to geo-tag the sensed data before sharing them. The Obfuscation Manger cooperates with the Correlation Manager to detect and minimize the privacy leakage.

Case 3: On their way, smart transportation system detects an ambulance in their neighborhood, so the Context Analyzer receives that notification, and notifies the Policies Manager to activate the proper policy. Smart transportation system receives an accurate version of the location data, and it provides a new route for the autonomous vehicle to handle the current situation. The Context Analyzer detects the end of the emergency situation, so it notifies the Policies Manager to activate the proper policy. Hence, Policies Manager notifies the Obfuscation Manager to enforce the proper policy.

Case 4: When they reach work, the Devices Clustering Manager detects that, changes the membership of their smart phones and smart vehicle from Mobile cluster to Work cluster, and finally notifies the Policies Manager to activate the proper policy. Next, Policies Manager notifies the Obfuscation Manager to enforce the proper policy.

Case 5: Alice has an appointment in the hospital. So, on their way to return home, they go to the hospital. The Context Analyzer uses the Personal Location Profile Manager to detect that they are located in a sensitive area, so it notifies the Policies Manager to activate the proper policy. Policies Manager notifies the Obfuscation Manager to enforce the proper policy.

Case 6: On their way to return home, the road is closed for an emergency situation. So, the Smart transportation system provides the autonomous vehicle with an alternative route. In the alternative route, the Context Analyzer uses the Consolidated Location Profile Manager to detect that they are using a road with low traffic density, so it notifies the Policies Manager to activate the proper policy. Hence, Policies Manager notifies the Obfuscation Manager to enforce the proper policy.

Case 7: When they return home, Devices Clustering Manager detects that, changes the membership of their smart phones and smart vehicle from Mobile cluster to Home cluster, and finally notifies the Policies Manager to activate the proper policy.

6 Conclusion

An increase in the ratio of world's population that live in urban areas is estimated to rise from 50.5% in 2010 to 59% by 2030. As a result, large cities are expected to encounter challenges, such as resources exhaustion, traffic congestion, and air pollution. In recent years, smart city concept was proposed to provide sustainable development to the cities and improve the quality of citizens' life by utilizing the information and communication technologies. To achieve that, smart city applications are expected to use IoT infrastructure to collect and integrate data continuously about the environment and citizens, and take actions based on the constructed knowledge. Indeed, identification and tracking technologies are essential to develop such context-aware applications. Therefore, citizens are expected to be surrounded by smart devices which continuously identify, track and process their daily activities. Location privacy is one of the important issues which should be addressed carefully. Preserving the location privacy means that the sensitive location information of citizens' are released only to authorized parties, and used for the desired purpose. In reality, adopting the citizens' for smart city applications depends on their trust on the used technologies. In this paper, we reviewed smart city architectures, frameworks, and platforms to highlight to what extent preserving location privacy is addressed. We showed that preserving location privacy in smart city applications does not get the required attention. We discussed the issues, which we think should be addressed to preserve location privacy in smart city applications. We proposed an architecture of preserving location privacy system for smart city applications.

Acknowledgments. The work carried out in this paper is supported by the HPC Center at King Abdulaziz University.

References

1. United Nations Human Settlements Programme., Cities and climate change : global report on human settlements 2011. Earthscan (2011)
2. Woznowski, P., Burrows, A., Diethe, T., Fafoutis, X., Hall, J., Hannuna, S., Camplani, M., Twomey, N., Kozlowski, M., Tan, B., Zhu, N., Elsts, A., Vafeas, A., Paiement, A., Tao, L., Mirmehdi, M., Burghardt, T., Damen, D., Flach, P., Piechocki, R., Craddock, I., Oikonomou, G.: SPHERE: a sensor platform for healthcare in a residential environment. In: Angelakis, V., Tragos, E., Pöhls, Henrich C., Kapovits, A., Bassi, A. (eds.) Designing, Developing, and Facilitating Smart Cities, pp. 315–333. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44924-1_14
3. Schlingensiepen, J., Nemtanu, F., Mehmood, R., McCluskey, L.: Autonomic transport management systems—enabler for smart cities, personalized medicine, participation and industry grid/industry 4.0. In: Sładkowski, A., Pamuła, W. (eds.) Intelligent Transportation Systems – Problems and Perspectives. SSDC, vol. 32, pp. 3–35. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-19150-8_1
4. Bonetto, R., Rossi, M.: Smart grid for the smart city. In: Angelakis, V., Tragos, E., Pöhls, Henrich C., Kapovits, A., Bassi, A. (eds.) Designing, Developing, and Facilitating Smart Cities, pp. 241–263. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44924-1_12
5. Wolff, A., Kortuem, G., Cavero, J.: Towards smart city education In: 2015 Sustainable Internet and ICT for Sustainability (SustainIT), pp. 1–3 (2015)
6. Coelho, J., Cacho, N., Lopes, F., Loiola, E., Tayrony, T., Andrade, T., Mendonça, M., Oliveira, M., Estaregue, D., Moura, B.: ROTA: a smart city platform to improve public safety. New Advances in Information Systems and Technologies. AISC, vol. 444, pp. 787–796. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-31232-3_74
7. Khatoun, R., Zeadally, S.: Smart cities: concepts, architectures, research opportunities. Commun. ACM **59**(8), 46–57 (2016)
8. Eckhoff, D., Zehe, D., Ivanchev, J., Knoll, A.: Smart city-to-vehicle — measuring, prediction, influencing. ATZelektronik Worldw. **12**(2), 60–63 (2017)
9. Alam, F., Mehmood, R., Katib, I., Albogami, N.N., Albeshri, A.: Data fusion and IoT for smart ubiquitous environments: a survey. IEEE Access **5**, 9533–9554 (2017)
10. Suma, S., Mehmood, R., Albugami, N., Katib, I., Albeshri, A.: Enabling next generation logistics and planning for smarter societies. Procedia Comput. Sci. **109**, 1122–1127 (2017)
11. Gartner: Internet of things – Gartner IT glossary. http://www.gartner.com/it-glossary/internet-of-things/. Accessed 29 Aug 2017
12. Evans, D.: The Internet of Things How the Next Evolution of the Internet Is Changing Everything (2011)
13. Wadhwa, T.: Smart cities: toward the surveillance society? In: Araya, D. (ed.) Smart Cities as Democratic Ecologies, pp. 125–141. Palgrave Macmillan UK, London (2015). https://doi.org/10.1057/9781137377203_9
14. Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., Vasilakos, A.V.: The quest for privacy in the internet of things. IEEE Cloud Comput. **3**(2), 36–45 (2016)

15. Martinez-Balleste, A., Perez-martinez, P., Solanas, A.: The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Commun. Mag. **51**(6), 136–141 (2013)
16. Golle, P., Partridge, K.: On the anonymity of home/work location pairs. In: Tokuda, H., Beigl, M., Friday, A., Brush, A.J.Bernheim, Tobe, Y. (eds.) Pervasive 2009. LNCS, vol. 5538, pp. 390–397. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01516-8_26
17. Duckham, M., Kulik, L.: Location privacy and location-aware computing. Dynamic and Mobile GIS: Investigating Change in Space and Time, vol. 3, pp. 35–51 (2006)
18. Cottrill, C.D., Thakuriah, P.V.: Location privacy preferences: a survey-based analysis of consumer awareness, trade-off and decision-making. Transp. Res. Part C Emerg. Technol. **56**, 132–148 (2015)
19. Federal Trade Commission: "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," (2012)
20. Jalali, R., El-khatib, K., McGregor, C.: Smart city architecture for community level services through the internet of things. In: 2015 18th International Conference on Intelligence in Next Generation Networks, pp. 108–113 (2015)
21. van Zoonen, L.: Privacy concerns in smart cities. Gov. Inf. Q. **33**(3), 472–480 (2016)
22. Khan, Z., Pervez, Z., Abbasi, A.G.: Towards a secure service provisioning framework in a smart city environment. Futur. Gener. Comput. Syst. **77**, 112–135 (2017)
23. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X.S.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)
24. Bassi, A., et al.: Enabling things to talk. Designing IoT solutions with the IoT Architectural Reference Model. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40403-0
25. Bauer, M., et al.: IoT Reference Model. In. In: Bassi, A., et al. (eds.) Enabling Things to Talk, pp. 113–162. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40403-0_7
26. Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J.-P., Riahi, M., Aberer, K., Jayaraman, P.P., Zaslavsky, A., Žarko, I.P., Skorin-Kapov, L., Herzog, R.: OpenIoT: Open Source Internet-of-Things in the Cloud. In: Podnar Žarko, I., Pripužić, K., Serrano, M. (eds.) Interoperability and Open-Source Solutions for the Internet of Things. LNCS, vol. 9001, pp. 13–25. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16546-2_3
27. Doukas, C., Antonelli, F.: A full end-to-end platform as a service for smart city applications. In: 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 181–186 (2014)
28. Ramparany, F., Marquez, F.G., Soriano, J., Elsaleh, T.: Handling smart environment devices, data and services at the semantic level with the FI-WARE core platform. In: 2014 IEEE International Conference on Big Data (Big Data), pp. 14–20 (2014)
29. Bohli, J.-M., Skarmeta, A., Moreno, M.V., Garcia, D., Langendorfer, P.: SMARTIE project: secure IoT data management for smart cities. In: 2015 International Conference on Recent Advances in Internet of Things (RIoT), pp. 1–6 (2015)
30. Bohli, J.M., Dobre, D., Karame, Ghassan O., Li, W.: PrivLoc: preventing location tracking in geofencing services. In: Holz, T., Ioannidis, S. (eds.) Trust 2014. LNCS, vol. 8564, pp. 143–160. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-08593-7_10
31. Voutyras, O., Gogouvitis, S.V., Marinakis, A., Varvarigou, T.: Achieving autonomicity in IoT systems via situational-aware, cognitive and social things. In: Proceedings of the 18th Panhellenic Conference on Informatics - PCI 2014, pp. 1–2 (2014)
32. Tragos. E. Z.: et al.: Enabling reliable and secure IoT-based smart city applications. In: 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS), pp. 111–116 (2014)