A NFP Model for Internet of Things applications

Sabrina Sicari, Alessandra Rizzardi,
Alberto Coen-Porisini
DISTA, Dipartimento di Scienze Teoriche e Applicate
Universita' degli Studi dell'Insubria
Via Mazzini 5 21100 Varese, Italy
(sabrina.sicari, alessandra.rizzardi,
alberto.coenporisini)@uninsubria.it

Cinzia Cappiello
Dipartimento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Piazza Leonardo da Vinci 32, 20133 Milano, Italy
cinzia.cappiello@polimi.it

***Abstract*—Internet of Things (IoT) involves heterogeneous technologies (i.e., WSN, RFID, actuators) able to exchange data acquired from the environment in order to provide services to the requesting users. In such a scenario the privacy and the quality (i.e., in terms of accuracy, timeliness, completeness) of the handled information represent critical issues. In fact, the provided services must be customized according to the users preferences and habits and have to manage both users personal information and data from different sources, therefore it needs to guarantee privacy and data quality level. This work proposes a UML general conceptual model, which defines the entities involved in the IoT context, their relationships, facing privacy policies definition and data quality assessment. Such a model should represent a starting point for the development of IoT privacy-aware solutions, handling data with a well-defined quality.**

***Keywords*—Internet of Things, privacy, data quality, UML model.**

I. Introduction

Internet of Things (IoT) is an innovative paradigm in which different technologies interact among themselves, in order to provide customized services to users. From a technological point of view, the term *things* refers to various physical everyday objects that embed the enabling IoT technologies (e.g., wireless sensor nodes, actuators, RFIDs, and so on) to make them *smart* and suitable to be part of a global network infrastructure [1]. All these devices are able to acquire data from the environment where they are placed and/or to provide different types of information to other devices belonging to the network. Notice that some new interpretations of IoT extend the term things also to the individuals that through the adoption of an appropriate device can broadcast the status of the context in which they are in a specific time. Therefore, users are assimilated to sensors able to provide useful and usable data.

In this context, privacy represents a critical requirement, which can hinder the large scale adoption and diffusion of IoT applications. In fact, since the network infrastructure has to manage environmental and users information, a suitable system which aims to ensure the anonymity of data must be defined. Such a system should guarantee that only authorized devices/users are allowed to access certain types of information even if the use of a wireless communications increases the risk of violation which can lead to attacks such as eavesdropping and masking. For example, in the health-care context, the patients sensitive data should be accessible only to their doctors and not to the rest of the hospital staff or to other patients. Thus if an electrocardiogram machine has to periodically communicate the patient data to a device belonging to a specific doctor, only his/her device must be able to read such information, which has to be transmitted in an encrypted way over the IoT infrastructure designed for the whole hospital.

Besides privacy issue, the IoT system needs to guarantee to the users another NF (Non Functional) property, data quality (DQ): the IoT services should provide accurate and complete information. In fact, in many scenarios, errors or missing values might have critical impact on actions or decisions. In this paper, we evaluate the quality of data by considering three of the main data quality dimensions, i.e., accuracy, timeliness and completeness, and we aim to let the users aware of the reliability of the accessed information. This is an innovative aspect since as pointed out in [2], current available services provide the same information to each requesting user, often without considering his/her requirements and without specifying the level of privacy and DQ of the provided data. From our perspective, the services must be customized according to users preferences and habits. Summarizing, the issues which arise from such a requirement are twofold: on the one hand, there is the need to manage user personal data and, consequently, to preserve the private life, by means of a well-defined level of quality of protection (QoP); on the other hand, there is the need to evaluate data from different sources and, therefore, to compute the relative DQ.

In order to address such an issue it is fundamental to start from the modeling of an IoT infrastructure able to guarantee the user privacy and the adequate DQ. The work presented in this paper defines a UML general conceptual model, which concerns all the entities involved in the IoT context, in order to define ad hoc privacy policies and a DQ level. Notice that such a model represents the starting point for the development of IoT privacy-aware solutions, exploiting data with a well-defined quality.

The paper is organized as follows. Section 2 briefly analyzes the current state of the art. Section 3 presents a sketch of a defined system architecture for IoT. Section 4 deeply discusses the proposed model, in particular dealing with privacy and DQ issue. Section 5 describes an application example which aims at illustrating the effectiveness of the presented model. Section 6 ends the paper and provides some hints for future works.

II. Related Work

Since IoT paradigm finds application in many different fields, from health-care (i.e., patients remote monitoring), home automation (i.e., energy consumption control), smart cities (i.e., traffic control, smart parking system), commerce (i.e., inventory management, production chain, customization of the shopping at the supermarket) to environmental montoring (i.e., civil protection), it is important to define ad hoc privacy solutions in order to correctly handle sensitive data. In fact, for all of these applications users require the protection of their own personal information, which could regard their movements, their habits, their interactions with other people, their private life. In order to satisfy user requests, besides privacy requirement it needs to evaluate the trustworthiness of the data sources and, in general, the data quality. In literature there are some works proposing approaches facing either privacy requirement or data quality.

In [3] is proposed a data tagging for managing privacy in IoT. Data representing physical phenomena or related to individuals are tagged with their privacy properties. Tagging within resource-constrained sensors raises several issues due to the expensive tags computation. A well-investigated solution is based on the k-anonymity. For example, in [4] is presented an access control protocol where the privacy is controlled by the users themselves. Context aware k-anonymity privacy policies and filters are designed and privacy protection mechanisms are investigated, in which users can control which of their personal data is being collected and accessed and when, and who is collecting and accessing such data. In addition, [5] presents Continuously Anonymizing STreaming data via adaptive cLustEring (CASTLE). It is a cluster-based scheme which ensures anonymity, freshness and delay contraints on data streams, since most of the existing privacy preserving techniques (e.g., k-anonymity) are designed for static data sets and not for continuous, unbounded and transient streaming data. [5] models k-anonymity on data streams and defines k-anonymized clusters exploiting quasi-identifier attributes. [6] analyzes the privacy risk that occurs when a Static Domain Name (DNS) is assigned to a specified IoT terminal smart device. In this work the authors propose a privacy protection enhanced DNS scheme for smart devices, which can authenticate the original users identity and reject illegal accesses. In [7] privacy and access control mechanisms are considered together. It is presented a fully decentralized anonymous authentication protocol aimed at implementing privacy-preserving IoT applications. Such a proposal is based on a credential system, which defines two roles for the participant nodes: Users, which are the nodes originating the data and Data Collectors, which are the entities responsible for the collection of data only from authorized Users; Users can anonymously authenticate themselves in front of Data Collectors proving the ownership of a valid Anonymous Access Credential (AAC) encoding a particular set of attributes. Such a system relies on no central organization: the parameters required by the system are generated in a cooperative way.

As regards data quality, in the past years it has been mainly investigated in the database area. Currently, in several literature contributions data quality has been recognized as one of the main issues to address in the IoT research field. In fact, the volume of data and the variety of the sources arise new challenges in data quality field in which researchers and practitioners aim to evaluate the ”fitness for use” of data sets [8]. In [9], authors claim the need of control over data sources to ensure their validity, information accuracy and credibility. Data accuracy is also one the aspect on which the authors of [10] focus on. They observe that the presence of many data sources raises the need to understand the quality of that data. In particular, they state that the data quality dimensions to consider are accuracy, timeliness and the trustworthiness of the data provider. Anyway, the huge number of data sources is considered as positive for data fusion and for the extraction and provision of advanced services. Besides temporal aspects (i.e., currency) and data validity, a literature contribution focused on pervasive environments adds another important dimension such as availability [11]. Authors defined new metrics for the cited quality dimensions for the IoT environment and evaluate the quality of the real-world data available on an open IoT platform called Cosm. They showed that data quality problems are frequent and they should be solved or at least users should be aware of the poor quality of the used data sources. Anomaly detection techniques are widely employed to remove noises and inaccurate data in order to improve data quality. However, there are no available solutions which propose an approach able to manage both privacy and data quality requirements in IoT environment at the same time. In fact, the existing proposals address only partially the privacy issues and lack to define a complete model, which identifies all the entities involved in the IoT infrastructure and also focuses on services requirements (i.e., QoP and DQ).

III. System Architecture

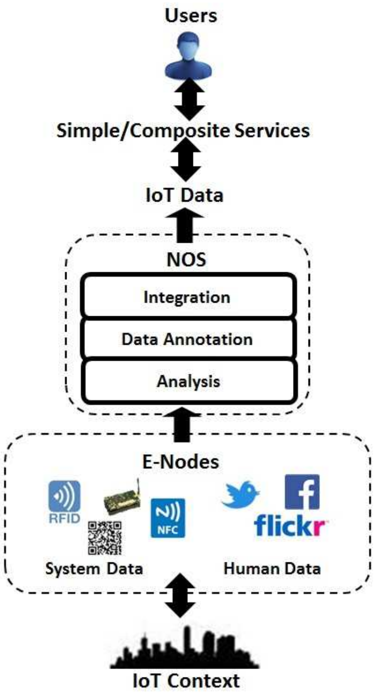

Fig. 1. System Architecture

The reference system architecture is sketched in Fig. 1 [12]. Data are provided from the environment in which the IoT system is deployed by a set of heterogeneous technologies that are referred with the term *E-Nodes*. Such technologies may require different communication systems (e.g., NFC, UWB, IEEE802.15.x, Bluetooth) and include nodes which generate data automatically (i.e., wireless sensors, RFID, smart tags and so on), referred as *System Data*, and nodes which provide data by users (i.e., social networks), referred as *Human Data*. In order to handle such an heterogeneous and huge amount of information *NOS (NetwOrked Smart Objects)* are defined and used. *NOS* is a computationally powerful smart node and has a three-layer structure, which consists of *Analysis*, *Data Annotation* and *Integration* layer. *NOS*s acquire the raw data provided by *E-Nodes* and process them according to the *Analysis* and *Data Annotation* layers shown in Fig. 1, in order to provide in output a normalized representation of the gathered information, called *IoT Data*. The *Analysis* layer is responsible for the assessment of data security and privacy (i.e., data integrity, anonymity, confidentiality, authentication) and quality level (i.e., data source reputation, provenance, freshness, accuracy). The *Data Annotation* layer represents the information obtained from the *Analysis* layer according to a well-specified syntax and includes also a semantic description of the data content; more in details, the data are annotated with a set of metadata (i.e., a score for each security and DQ requirement). The *Integration* layer allows to integrate data coming from different sources according to the specific users service requests. Notice that such a layer takes into account the user requests regarding privacy and data quality level in order to choose the data that better satisfy user needs in the different application scenarios.

Hence, the *NOS* layer can be connected to IP-based networks (i.e., Internet, Intranet), enabling nodes and users to access to the offered services. In fact, the end-users interact with the system by requesting the services provided by the IoT system itself. A service is simple or atomic if the users are enabled to access to one source, whereas it is composite if multiple sources are integrated. Such a set of services, made available by *NOS*s, can be directly and dinamically configured by a network administrator and can be orchestrated by a remote server through standard Web services approaches.

IV. NFP Model

In the heterogeneous IoT context appears fundamental to provide a well-defined model, suitable for all the IoT applications and architectures, able to guarantee a level of privacy and data quality, specifying both involved entities and their relationships within the IoT infrastructure. In order to develop privacy-aware services (atomic or composite) using data with a certain level of quality, this paper proposes a general UML conceptual model, which describes and analyzes the privacy and DQ issues faced at each level of the system architecture presented in Section III. Such a model is shown in the UML class diagram in Fig. 2. The main involved actors are *Node*, *IoTPlatform*, *Service* and *User*.

A. Node

From a technological point of view, the different adopted technologies, *E-Nodes*, involved in the acquisition of information from the environment, such as wireless sensor networks (WSN), RFID, nanotechnologies, actuators and so on, are represented by the class *Node*. Such a class is extended by the sub-classes representing the mentioned technologies (the note *incomplete* means that there are *other types of such nodes which have not been mentioned*). Each instance of the class *Node* is characterized by a pair function-role, identified by *NodeRole* and *NodeFunction* classes. *NodeRole* [13] is a concept strictly related to the privacy issues. Therefore, three classes extending *NodeRole* are introduced: (i) *nSubject* represents the node that senses or generates the data; (ii) *nProcessor* represents the node which processes data by executing some actions on them (i.e., forwarding, aggregation); (iii) *nController* represents

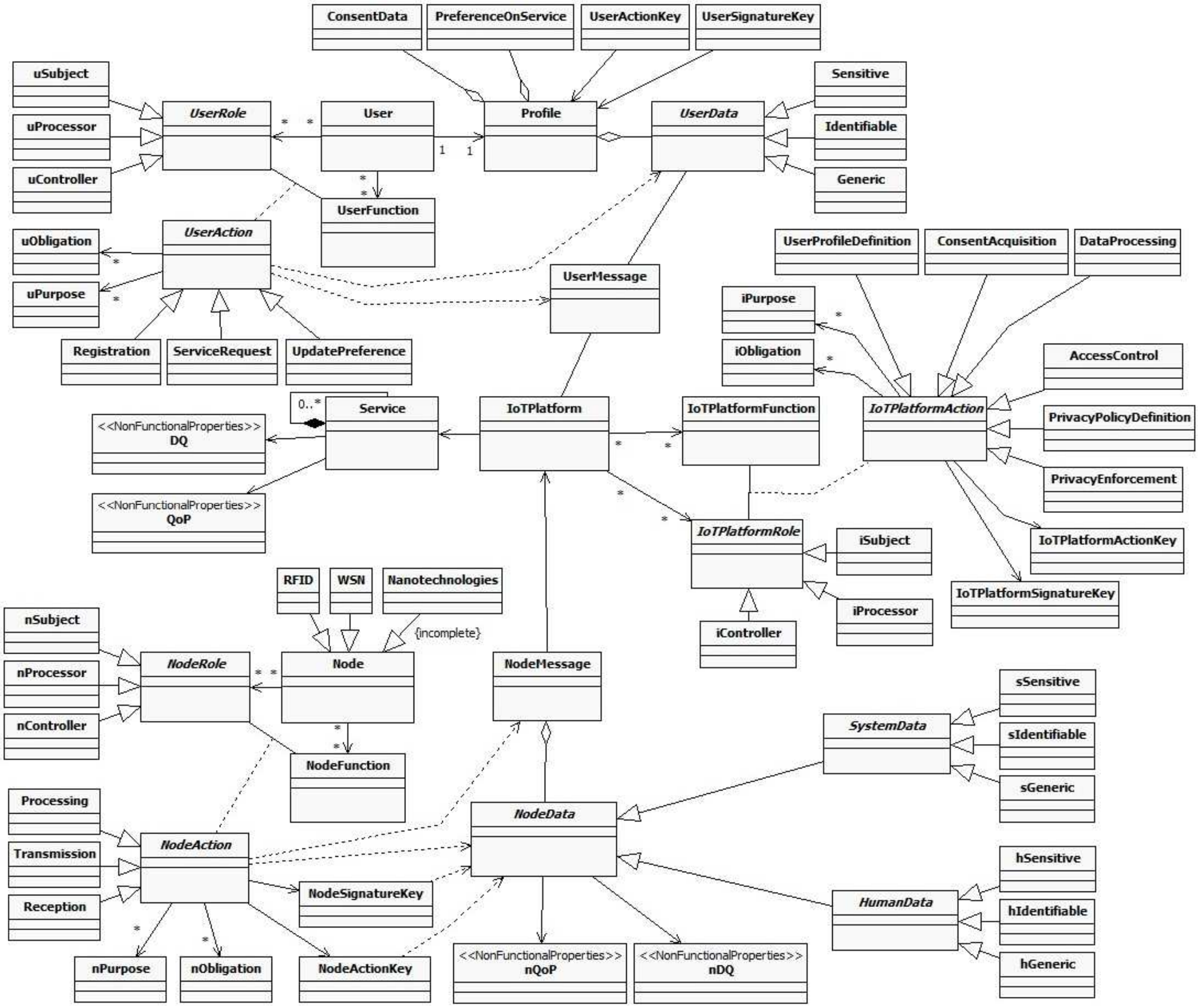

Fig. 2. Network Privacy Class Diagram

the node which verifies that the actions perfomed on data satisfy the defined privacy policies [14] [15] [16]. As regards *NodeFunction*, that represents the task performed by a node in the network in which it operates, the UML model does not specify any sub-class, since the functions depends on the specific IoT application context in which the system is employed (e.g., shopping retail, hospital, university).

With the pair function-role it is associated the class *NodeAction*, which specifies the set of actions that can be undertaken by the node itself. The identified actions are: *Processing*, when a node performs some operations on data; *Trasmission* or *Reception*, when the node sends or receives data from another node. An action is executed under *nPurpose* that specifies the reason under which it is possible to handle data (i.e., marketing purpose, research purpose, health purpose). *NodeAction* is also associated with one or more *nObligation*s, in order to model the fact that the execution of a set of actions is guaranteed by the processor and/or the controller at the end of the processing activities (e.g., whenever an inconsistency or a privacy violation is found, some countermeasures, such as generation of an error/alert message, have to be taken). In order to guarantee integrity, confidentiality and non repudiation, two kinds of keys, named *NodeSignatureKey* and *NodeActionKey* are associated to *NodeAction*. Communications among nodes happen exchanging instances of the class *NodeMessage*. A message is composed of several heterogeneous types of data (e.g., numbers, text, multimedia), which can contain different information, depending on their source; therefore the instances of abstract class *NodeData* may be distinguished, in agreement with the system architecture in Section III, in:

- *SystemData*, which represents the data generated by the IoT system (e.g., the information provided by a locator tag related to the movements of a particular user or object)

- *HumanData*, which includes the data produced by users, for example by means of a social network

Moreover, both system and human data are classified in three different categories, represented in the diagram as extensions of *SystemData* and *HumanData* classes:

- *sIdentifiable* and *hIdentifiable*, which represent the information used to uniquely identify nodes (i.e., node identifier)
- *sSensitive* and *hSensitive*, which include information that should not be freely accessible, because they may reveal private acquired data
- *sGeneric* and *hGeneric*, which represent other generic information, not included in the previous classes

To each instance of *SystemData* or *HumanData* is associated *nQoP* and *nDQ* information, which represent the non functional properties regarding the level of privacy and data quality respectively.

B. User

Besides nodes, another fundamental actor is represented by the class *User*. Such a class concerns all humans that could interact with the IoT system, for example by means of their personal devices (e.g., smartphones, NFC, tablet). Notice that users are distinguished from nodes due to the fact that the former require one or more services to the infrastructure, while the latter acquire the necessary information to provide such services. In addition, in order to provide each user with the best services he/she requires a personal *Profile* is defined. *Profile* includes the following information: an aggregation of *ConsentData*, which represents the acceptance of the agreement established with the service provider (i.e., the consent to handle user personal data for specific purposes and under some obligations); an aggregation of *PreferenceOnService*, used to customize the services on the basis of user requirements; the keys exploited to address privacy issues, distinguished in *UserSignatureKey* and *UserActionKey*. *Profile* also concerns *UserData*, which can be further classified in: *Identifiable*, including data referred to the user identity (i.e., first and last name); *Sensitive*, containing information related to user's private life and habits, such as health conditions, food intolerances, religious beliefs and so on; *Generic*, regarding general information not belonging to the previous classes. Each user is associated with a pair function-role. Class *UserRole* is extended in a similar way as class *NodeRole*, because a user could represent *uSubject*, *uProcessor* or *uController* of the transmitted or provided data. In details, *uSubject* is the owner of the data, *uProcessor* is who handles *uSubject* data and *uController* represents who verifies the compliance with the defined privacy policies and related to user profile. As regards *UserFunction*, it strinctly depends on the application context. To each pair function-role is also associated the respective *UserAction*, which includes a set of actions. In fact, a user, before interacting with the IoT system, has to firstly register himself/herself (*Registration* class). Moreover, *ServiceRequest* represents the user requests in terms of the activities in which the user is interested in. *UpdatePreference* represents the capability of the users to change at any time their preferences expressed in their own profile. As for nodes, specific *uPurpose* and several *uObligation*s are associated to each action; for example, users, before requesting services, have to register themselves. Furthermore, the communications among users and *IoTPlatform* occur by means of packets, which are instances of *UserMessage* class. Notice that, in an IoT scenario, the nodes and the users number varies over the time.

C. IoTPlatform

Looking at the system architecture presented in Section III, the heterogeneous data, acquired by the nodes, are handled by *NOS*, represented into the model by *IoTPlatform*. *IoTPlatform* has a crucial role and, in fact, it performs different tasks described by the class *IoTPlatformAction*. As the nodes and the users, also *IoTPlatform* plays different roles, represented by *IoTPlatformRole* class, and functions, represented by *IoTPlatformFunction* class, in relation to the current action and the application domain. *IoTPlatformRole* is extended by *iSubject*, *iProcessor* and *iController* classes, which represent, respectively, the owner of the data, the processor which executes some actions on data, and the verifier of the performed actions. As regards *IoTPlatformAction*, the main *IoTPlatform* tasks are:

- *UserProfileDefinition*, which models the acquisition of the users data and preferences, required for the execution of the best suited services
- *ConsentAcquisition*, which represents both the user acceptance of the agreement with the requested service, and the user data management, according to the established privacy policies
- *AccessControl*, which represents the execution of the access control operations of an user registered within the IoT system. Notice that such an action allows to restrict the access to the system only to authorized and pre-registered users
- *PrivacyPolicyDefinition* which represents the definition of a policy in order to ensure user privacy and, in particular, anonymity
- *PrivacyEnforcement* is required in order to force the compliance with the defined privacy policies, under which the user has given the consent to handle his/her data

For *IoTPlatform* several *iPurpose*s and *iObligation*s have to be specified, in order to guarantee the performing of the proper actions when only particular conditions are verified. *IoTPlatform* deals in particular with encryption and decryption keys; in fact, *IoTPlatform*, when a node (i.e., a device) or a user enters the system, has to provide the credentials and the keys to allow a future and protected interaction with the offered services. *IoTPlatform* owns both *IoTPlatformSignatureKey* and *IoTPlatformActionKey* required to perform the access control, authentication and privacy control operations, and the signature and action keys belonging to the nodes and the users, as described in Section IV-A and IV-B respectively.

On the basis of the action to be performed, nodes and users have to exploit a defined encryption mechanism on owned/transmitted data. When a new node or user begins to interact with *IoTPlatform*, in a secure way it sends the proper signature and action keys that will be used in all the communications with the IoT system. Clearly, notice that each user/node has an unique signature key, which represents an access credential, while the action key is directly related to the pair function-role currently played by the user/node and it is used to exchange message and to encrypt sensitive data referring to the instances of *sIdentifiable*/*nIdentifiable* data. Such a behavior ensures the privacy compliance of the transmitted information, both from users/nodes towards *IoTPlatform* and from *IoTPlatform* towards the requesting users. Each user/node encrypts its data with its proper action key. When *IoTPlatform* receives a request of data from a user, it performs some queries in order to establish, firstly, if the user is authorized to get such data and, secondly, which are the user's preferences in relation to the NF properties of the requested services. Notice that the defined solution supports any kind of encryption techniques and any key distribution mechanism, although the details related to such issues are out of the scope of this work.

D. *Service*

Exploiting the nodes data, *IoTPlatform* provides services (atomic or composite) which satisfy user needs. *Service* is one of the core class of the model, since all the IoT system activities turn around the request and provision of services. In fact, the users give information related to their identity, life style, interests and preferences under well-defined privacy policies, in order to obtain a customized service. Such a service has to guarantee several non functional properties, which include: (i) Data Quality (*DQ*), since data are collected from different sources, it needs to model the state of consistency, validity, freshness and accuracy of the provided data and (ii) Quality of Protection (*QoP*), which regards the insurance of well-defined levels of privacy and security. Notice that the services are classified in atomic and composite.

V. An Application Example

In order to clarify the applicability and the effectiveness of the privacy model presented in Section IV, we describe an application example exploiting a university campus domain. In such a scenario, a student, a professor, an employee or a simple visitor take advantage from an ad-hoc advanced application, able to guide him/her through the campus, in order to interact with physical objects and obtain specific digital services in relation to his/her profile. A specific application running on the users personal smartphones is in charge of providing the user with the expected personalized contents. A sketch of the described scenario is shown in Fig. 3.

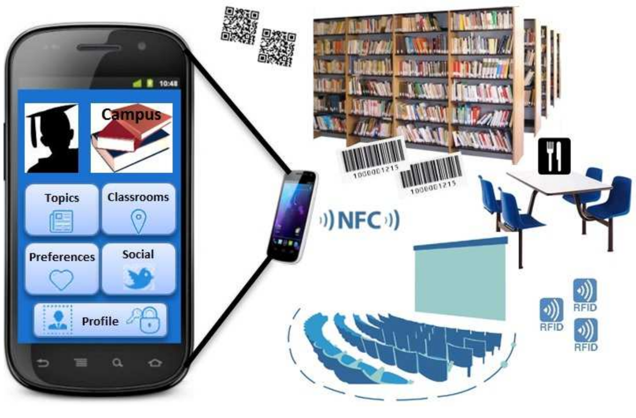

Fig. 3. IoT University Campus Scenario

Notice that student, professor and employee represent instances of the class *User*, and each of them owns a personal profile (*Profile*). In fact, a student will be interested in different services with respect to professor or employees. For example, a student may be interested in information related to the classrooms for studying, the classrooms where lessons or exams will take place, or the presence of the professor in a classroom, in order to establish whether s/he is early or late for a meeting or a lesson. An employee, instead, may want to monitor the state of classrooms occupancy. Finally, a professor may want to be informed about his/her class schedules or conferences. Consequently, each user owns a personal profile, in relation to his/her role (*UserRole*) and function (*UserFunction*) within the infrastructure: we have students profiles, professors profiles, employees profiles and so on, each of which is further customized with strict information related to his/her actions and needs within the university campus (i.e., curriculum, faculty membership, classroom preferences).

In order to exploit the provided *Service*s, each user has to be registered to *IoTPlatform*. During the registration phase, *IoTPlatform* requires some personal information (i.e., first name, last name, age, role within the university) and also provides him/her the credentials to access the system itself: *SignatureKey*. Information such as first/last name and phone number are classified as identifiable data, whereas age and nationality are classified as generic data, since they can be exploited only for statistical purposes. As regards a student, s/he specifies his/her preferences about the classrooms or the school subjects s/he is interested in. An important step is that each user has to give the consent for the processing of personal information in order to let the system to use his/her preferences to provide customized services. Such personal information will be used according to the established privacy policies (e.g., an information can be used for a specific purpose and under a proper obligation). All these data belong to the user profile and are stored also by *IoTPlatform*.

After the registration, the user downloads the application on his/her smartphone, possibly equipped with technologies such as Bluetooth, ZigBee and/or NFC and connected to the Internet through Wi-fi or 3G. The service provider gives the necessary credentials to the smartphone, which aim to guarantee the access to the service itself by means a secure communication. Notice that such credentials are instances of the class *UserActionKey*.

In such a scenario we assume the installation of a number of *Node*s (i.e., locators), which are fixed devices exploited in order to track people movements in real-time. Locators are able to detect and process the signals from the users smartphones and, then, send data to the service provider or to other data management infrastructures. On the one hand, the data collected by the system can be used for different purposes (i.e., performing analysis, making decisions about the management of the university itself). For example, exploiting classrooms occupancy information, the employees may plan an optimized distribution among courses; another interesting analysis may regard the use of the personal car to reach the university by both students and other people, in order to design a more efficient parking management; if the campus provides a cafeteria service, users might express some preferences in relation to personal tastes or intolerances, which can be taken into account in the menu definition. On the other hand, during his/her permanence in the university, the student/professor receives the information according to his/her preferences (e.g., conferences on topics of interest). Therefore, also the smartphones are able to interact with the smart objects; for example, they can retrieve information from the tags placed on the shelves in the athenaeum library. In fact, a student/professor may be guided within the campus library, in relation to his/her topics of study or preferences, explicitly declared to the service provider. In this case, the books or the bookshelves must be equipped with tags, which can provide the user with a lot of different contents, such as the volume title, authors, year, a brief summary and so on.

Moreover, the smartphone application may be connected with a social network, through which users can share their own experiences or, viceversa, the administrator of university social network page can communicate advices, university initiatives or other information related to the university. Notice that it arises the distinction between system and human data, since within the university are handled both data provided by devices and information from the social network. More in details, after the registration, the users can connect themselves to *IoTPlatform* through their smartphones or other personal devices (i.e., notebook, tablet) using the exchanged credentials and then can communicate through *IoTPlatform* with the nodes belonging to the network. The services are provided to the users taking into account both *Profile* and *PreferenceOnService*, which can be specified by the user through the downloaded application itself.

In such a context the customers have to be aware about the confidentiality and the quality of the received and transmitted data; on the other side, we have that also the university employees and managers have to be aware of the accuracy, completeness and integrity of the retrieved information. The definition of specific privacy policies, according to the users consesus, aims to guarantee the desired level of privacy. The privacy policies are stored in *IoTPlatform* that guarantees the access control, the key management and the enforcement of the privacy policies themselves. Notice that the proposed solution preserves the user privacy, since, without an ad-hoc approach, from users behavior it is possible to derive some habits and, therefore, sensitive data; for example, the lessons attendance of a particular student or users preferences in terms of nutrition if s/he benefits of the cafeteria service (e.g., a user can point out ingredients s/he does not want to include in his/her menu, for example for ethical or religious duties). Hence, *IoTPlatform* guarantees high accuracy, freshness and completeness on the provided data, in order to satisfy user requirements in terms of DQ.

This example presents a complete IoT application concerning all the entities defined in the model in Section IV, in which users, smart objects and services interact in order to exchange useful information for everyday life and long-term decisions.

VI. Conclusions and Future Work

IoT is characterized by a huge heterogeneous amount of sources and related data, which are handled for satisfying users different needs. In order to guarantee the real diffusion of the IoT paradigm it is required to deal with some key NF properties, in particular QoP and DQ that require the definition of solutions which address such issues at the early steps of the service definition. In this direction it is important to provide a conceptual model, which supports the other phases towards the development. The defined model is able to identify the IoT involved entities (i.e., users, services, technologies) and represent the relationships among them, focusing on privacy and DQ issues. In the next future we will focus on the design phase and on the definition of ad hoc protocols, exploiting the defined model.

References

[1] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Elsevier Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[2] D. Barbagallo, C. Cappiello, A.Coen-Porisini, P. Colombo, M. Comerio, F. D. Paoli, C. Francalanci, and S. Sicari, "Towards the definition of a framework for service development in the agrofood domain: A conceptual model," in *WEBIST 2012*, Porto, Portugal, April 2012.

[3] D. Evans and D. Eyers, "Efficient data tagging for managing privacy in the internet of things," in *Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012*, Besancon, France, November 2012.

[4] X. Huang, R. Fu, B. Chen, T. Zhang, and A. Roscoe, "User interactive internet of things privacy preserved access control," in *7th International Conference for Internet Technology and Secured Transactions, ICITST 2012*, London, United Kingdom, December 2012.

[5] J. Cao, B. Carminati, E. Ferrari, and K. L. Tan, "Castle: Continuously anonymizing data streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp. 337–352, May 2011.

[6] Y. Wang and Q. Wen, "A privacy enhanced dns scheme for the internet of things," in *IET International Conference on Communication Technology and Application, ICCTA 2011*, Beijing, China, October 2011.

[7] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving iot target-driven applications," *Computers & Security*, vol. 37, pp. 111–123, September 2013.

[8] R. Y. Wang and D. M. Strong, "Beyond accuracy: What data quality means to data consumers," *J. Manage. Inf. Syst.*, vol. 12, no. 4, pp. 5–33, Mar. 1996. [Online]. Available: http://dl.acm.org/citation.cfm?id=1189570.1189572

[9] B. Guo, D. Zhang, Z. Wang, Z. Yu, and X. Zhou, "Opportunistic iot: Exploring the harmonious interaction between human and the internet of things," *J. Netw. Comput. Appl.*, vol. 36, no. 6, pp. 1531–1539, Nov. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2012.12.028

[10] A. Metzger, C.-H. Chi, Y. Engel, and A. Marconi, "Research challenges on online service quality prediction for proactive adaptation," in *Software Services and Systems Research - Results and Challenges (S-Cube), 2012 Workshop on European*, June 2012, pp. 51–57.

[11] F. Li, S. Nastic, and S. Dustdar, "Data quality observation in pervasive environments," in *Proceedings of the 2012 IEEE 15th International Conference on Computational Science and Engineering*, ser. CSE '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 602–609. [Online]. Available: http://dx.doi.org/10.1109/ICCSE.2012.88

[12] S. Sicari, C. Cappiello, F. D. Pellegrini, D. Miorandi, and A. Coen-Porisini, "Nos architecture," Tech. Rep., Dec. 2013.

[13] Q. Ni, A. Trombetta, E. Bertino, and J. Lobo, "Privacy-aware role based access control," in *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, ACM*, New York, USA, 2007.

[14] S. Sicari, L. A. Grieco, G. Boggia, and A. Coen-Porsini, "Dydap: A dynamic data aggregation scheme for privacy aware wireless sensor networks," *Elsevier Journal of Systems and Software*, vol. 88, no. 1, pp. 152–166, Jan. 2012.

[15] S. Sicari, L. Grieco, A. Rizzardi, G. Boggia, and A. Coen-Porisini, "Seta: A secure sharing of tasks in clustered wireless sensor networks," in *Proc. of IEEE WiMob*, Lyon, France, Oct. 2013.

[16] S. Sicari, A. Coen-Porisini, and R. Riggio, "Dare: evaluating data accuracy using node reputation," *Elsevier Computer Networks*, vol. 57, no. 15, pp. 3098–3111, Oct. 2013.