5

Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities

Jens-Matthias Bohli[1], Peter Langendörfer[2], and Antonio F. Skarmeta[3]

[1]*NEC Lab Europe*
[2]*IHP MicroElectronics*
[3]*Universidad de Murcia, Spain*

Abstract

The Internet of the Future will be an essential part of the knowledge society and will provide new information-based business. The usage of the Internet of Things for large-scale, partially mission-critical systems creates the need to address trust and security functions adequately.

The vision of SMARTIE[1] (Secure and sMArter ciTIEs data management) is to create a distributed framework for IoT based applications sharing large volumes of heterogeneous information. This framework is envisioned to enable end-to-end security and trust in information delivery for decision-making purposes following data owner's privacy requirements. New challenges identified for privacy, trust and reliability are:

- Providing trust and quality-of-information in shared information models to enable re-use across many applications.
- Providing secure exchange of data between IoT devices and consumers of their information.
- Providing protection mechanisms for vulnerable devices.

[1] This work is partially funded by EU FP7 Project SMARTIE contract 609062.

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 225–244.

SMARTIE will address these challenges within the context of Smart Cities. In this chapter we will present the SMARTIE focus on the security, trust and privacy of the Internet-of-Things infrastructure and the generated data. The dissemination of collected data and use of information must be protected to prevent harm to the control and management of the smart city infrastructure and to the citizen. Privacy-protection and access control to the data is necessary to convince data owners to share information in order to allow better services in the city. SMARTIE envisions a data-centric paradigm, which will offer highly scalable and secure information for smart city applications. The heart of this paradigm will be the "information management and services" plane as a unifying umbrella, which will operate above heterogeneous network devices and data sources and will provide advanced secure information services enabling powerful higher-layer applications.

5.1 Security, Privacy and Trust in Iot-Data-Platforms for Smart Cities

5.1.1 Overview

One of the main aims of Smart City technologies is to provide different optimization mechanisms for different aspects of data management. Data is gathered from various sources owned by different administrative domains. Noteworthy parts are data from public and private transportation providers, data from mobile users, captured for instance with their smart phones, surveillance data and videos from private and public organisations and a vast amount of sensors and meters, attached to machines and infrastructures, distributed throughout the city. All this information is stored in a variety of different places, for instance it can remain locally in the sensors or company internal databases, in social networks, in data storage located in private data centres or even in a public cloud storage service.

Figure 5.1 shows the components of a typical smart city information system. From this picture it is clearly visible that information needs to cross multiple administrative boundaries and can be used for multiple purposes — in fact it could be used for, at the time of gathering, unknown purposes. Also actuation decisions can be taken in a coordinated way between multiple control centres or data providers. Hence it is clear that there is a need of an information sharing platform in which data flows from various sources and from different

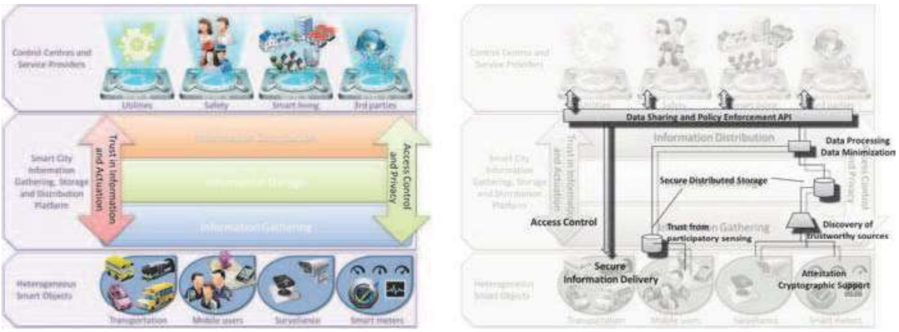
Control Centres and Service Providers
Utilities
Safety
Smart living
3rd parties
Smart City Information Gathering, Storage and Distribution Platform
Trust in Information and Actuation
Information Distribution
Information Storage
Information Gathering
Access Control and Privacy
Heterogeneous Smart Objects
Transportation
Mobile users
Surveillance
Smart meters
Data Sharing and Policy Enforcement API
Information Distribution
Data Processing
Data Minimization
Secure Distributed Storage
Access Control
Trust from participatory sensing
Discovery of trustworthy sources
Secure Information Delivery
Attestation
Cryptographic Support

Fig. 5.1 Architectural components.

administrative boundaries need to be treated in a secure and privacy preserving way. To ensure this, security and privacy need to be part of the platform by design and may not be added later on. The design goal and challenge is allowing user/service control of the data accessible and at the same time providing solution for easily configured management of the process.

All parties involved in the overall systems such as sensors and actuators, end users, data owners but also service providers need strong mechanisms for reliability and trust. Users and residents of the system will require fine-grained access and data privacy policies they want to enforce. For instance, a user might be willing to share location information with family and friends and make the information available in aggregated form for improvement of the public transport. But the same user might not want the information to be used by other 3rd-party service providers. New applications and synergies are possible if the data is shared between multiple domains. However, several challenges need to be overcome to make this possible. Creating a platform for sharing IoT-type of data is per se a huge challenge.

5.1.2 Risks to a Smart City IoT Platform

We predict that smart city data will eventually be stored in the cloud and employ cloud computing techniques, due to the high scalability of resources and computing performance and reduced cost in maintenance and operation. In this case, the smart city management system inherits also the security and privacy risks of cloud computing, for instance the compromise of cloud servers or data abuse by insider attacks. Additionally the Smart Cities infrastructure is also interacting with sensors and actuators in order to gather data and control critical infrastructure functions. This clearly requires to authenticate and authorize the access and to provide trusted information in a secure and privacy-preserving way.

These examples and developments show the importance of security, privacy and trust in smart city applications. The actual damages caused by possible threats can range from small interferences in the system to personal losses/exposure of private information. With more information and management and control the smart city assets being available over ICT networks, the risk and impact of security or privacy threats is foreseen to be increasing and can have profound and serious consequences for the community.

A smart city infrastructure, as pictured above, is exposed to several risks such as attacks on the control infrastructure, poisoning of data, and leakage of confidential data. SMARTIE will focus on challenges that concern privacy, security and trust of the information available in the smart city. An attacker can simultaneously attack on multiple layers:

- Manipulate the sensor measurements to infiltrate the system with wrong data, e.g. to cause certain actuations
- Attack the sensors and actuators physically to obtain credentials
- Attack or impersonate network components to act as a man-in-the-middle
- Obtain sensitive data or cause actuation by attacking the sharing platform with forged or malicious requests

Standard network security tools such as firewalls, monitoring or typically access control will not suffice to prevent such sophisticated attacks due to the distributed nature of the IoT and the problem of defining/finding trusted parties. It is essential that security is built into the infrastructure rather than being added as an extra plug-ins. An effective protection approach is to have security in depth, where data and services are protected by several independent systems. The challenge will be to design solutions where no single server has significant power to control the infrastructure or to access significant amounts of data.

5.2 First Steps Towards a Secure Platform

Past and current projects, such as UbiSec&Sense, SENSEI, WSAN4CIP provide already some solutions on which a platform as outlined above can build.

We present in this section certain components, which can be used as building blocks, but also components that need further development to be suitable for the type of platform SMARTIE aims for.

5.2.1 Trust and Quality-of-Information in an Open Heterogeneous Network

In SMARTIE and in other IoT systems, systems belonging to different owners need to cooperate. Such a cooperating system can be denoted as a system of systems (SoS). It is an entity composed of independent systems that are combined together in order to interact and provide a given service, which cannot be provided by the individual systems when not cooperating. The major properties of SoS especially for application fields as those intended in the SMARTIE project are dependability, security and privacy. Dependability comprises the following attributes:

- Availability — readiness for correct service
- Reliability — continuity of correct service
- Safety — absence of catastrophic consequences on the system user and its environment
- Integrity — lack of inappropriate system alternations
- Maintainability — ability to undergo updates and repairs

During the last years, the idea that security is needed to ensure real dependability has gained a certain level of acceptance and incidents such as the Stuxnet worm have demonstrated this pretty clear. The main aspects of security are confidentiality (absence of unauthorized disclosure of information), integrity, (the prevention of unauthorized modification or deletion of information) and availability for authorized actions.

All systems within a SoS have their own life, can work without interaction with other systems and are managed by different authorities. To ensure the appropriate cooperation and desired level of dependability and security within the SoS, a SoS management layer has to be designed and developed.

There is a limited theory on how to SoS should be managed [19]. The authors present five characteristics that give possible representation of fundamental building blocks for realizing and managing SoS.

- Autonomy — the ability to make independent choices — the SoS has a higher purpose than any of its constituent systems, independently or additively.
- Belonging — happiness found in a secure relationship — systems may need to undergo some changes to be part of SoS.
- Connectivity — the ability of system to link with other systems — systems are heterogeneous and unlikely to conform to a priori connectivity protocols and the SoS relies on effective connectivity in dynamic operations.
- Diversity — distinct elements in a group — SoS can achieve its purposes by leveraging the diversity of its constituent systems.
- Emergence — new properties appear in the course of development or evolution — SoS has dynamic boundaries, which are always clearly defined, SoS should be capable of developing an emergence culture with enhanced agility and adaptability.

SoS is often viewed as a network in the literature [20]. For management of SoS the "best practices" based on ISO standard ISO/IEC 7498 principles of network management should be used. The ISO defines terminologies, structure, activities for management of IT networks. These principles have been developed based on a systematic approach and thus, can be considered as guideline for the description of other kinds of networks as well. Since we are mainly concerned with heterogeneous groups of devices/services we will call such a SoS a Federation of Systems (FoS).

The need of cooperation in a Federation of Systems requires that the individual systems within FoS have to be trustworthy, and that there is a minimal level of trust between the involved systems. The transitive trust can be used to extend trusted relationship within the group. Kamvar et al. [21] present a reputation system for P2P that aggregates the local trust values of all of the users in a natural manner, with minimal overhead in terms of message complexity. The approach is based on the notion of transitive trust. The idea of transitive trust leads to a system which computes a global trust value for a peer by calculating the left principal eigenvector of a matrix of normalized local trust values. The non-transitive trust and reputation management scheme for wireless sensor networks is presented by Boukerch et al. [22] The approach uses localized trust and reputation management strategy, hence avoiding network-wide flooding. Each node in the network is able to establish a trust value with other interacting entities.

FAIR (fuzzy-based aggregation providing in-network resilience) [43] is an example how trust can be established and maintained at least between a base station and sensor node in the field. The strength of FAIR is the compatibility with the aggregation hierarchy that makes FAIR well suitable for medium size or large sensor networks. In a smart city scenario, smaller sets of sensors are more likely and we present a variant for trusted Quality of Information (QoI) computation that is particularly well-suited for small unattended networks [44].

The variant is based on a two-step *aggregate-and-confirm* approach. There are three roles pseudo-randomly distributed among the nodes at the beginning of each epoch: the Aggregator Node, the Normal Nodes and the Storage Nodes. The protocol consists of two message rounds, where each message is authenticated and broadcasted:

(1) Periodically, the aggregator node triggers the network to start an aggregation process; each node senses the environment and sends back its measurement.

(2) The aggregator node collects all the values, removes the outliers and computes the aggregate, which consists of the result and a measure of precision. This precision expresses the dispersion of the "genuine" data set. Based on this tuple, each node checks that the result is correct by comparing it with its own measurement and outputs a confirmation digest, encrypted with a pairwise key shared with the base station. Those confirmations are collected and stored by the storage nodes, which keep them for the base station.

Figure 5.2 gives an overview on those two protocol rounds.

The base station does not play any role in the aggregation process; it just retrieves the aggregated results and delivers it to the end user. To do so, the base station authenticated broadcasts to the network the epoch desired. Every node that was a storage node at this epoch and recorded the result sends it back together with the precision and the list of confirmation messages. Thanks to these two parameters, the base station can extract a measure of the Quality of Information (QoI) in order to evaluate the quality of the aggregation process.

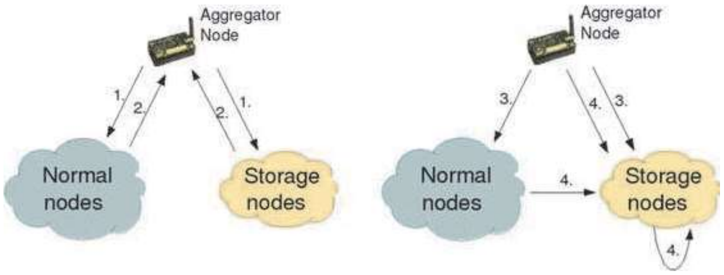

Fig. 5.2 General overview of the protocol: 1. AN triggers the network 2. Network sends back measurements 3. AN aggregates data and send back the tuple [result; precision] 4. Every node checks the result and sends a confirmation message to the SN.

5.2.2 Privacy-preserving Sharing of IoT Data

To the large extent, the IoT data may be of personal nature and therefore it is important to protect it from unauthorised entities accessing it. Privacy is one of the most sensitive subjects in any discussion of IoT protection [23].

Therefore, data privacy is one of the crucial aspects of IoT. The amount of data generated by IoT will be huge. Single pieces of information, i.e., single measurements, in most cases do not represent a significant threat for the owners of IoT devices (temperature at a location, even heart rate of a person at a given moment). However, given that the devices are generating data continuously, it is obvious that unauthorized access to such wealth of data can cause significant problems and can be used to harm the owners of the data (and possibly others, depending on the context of the data). Therefore, it is of paramount importance to protect access to IoT data. On the other hand, the power of IoT lies in the ability to share data, combine different inputs, process it and create additional value. Hence, it is equally important to enable access to data generated by other IoT devices, while preventing the use of data in un-authorized or undesired ways.

The existing initiatives such as FI-WARE [24] address the privacy issue within the Optional Security Service Enabler [25]. The issue of privacy is concerned with authorization and authentication mechanisms. This includes a policy language to define which attributes (roles, identity, etc.) and credentials are requested to grant access to resources. It includes a (data handling) policy language that defines how the requested data (attributes and credentials) is handled and to whom it is passed on. Finally, it includes the means to release and verify such attributes and credentials. It is also important to consider the mechanisms enabling the protection of information based on encryption algorithms within the secure storage. In terms of the privacy policy implementation, one of the viable solutions is privacy by design, in which users would have the tools they need to manage their own data [26].

The fundamental privacy mechanisms lie in the intelligent data management so that only the required data is collected. Detecting the redundancy, data is anonymised at the earliest possible stage and then deleted at the earliest convenience. Furthermore, the processing of collected data will have to be minimised according to a strict set of rules so that it cannot be re-used. The proposed approach will define such methodology together with the mechanisms for the secure storage based on efficient cryptographic algorithms suited for the resource constrained environments.

Misconceptions of what "personally identifiable information" is have originated multiple privacy scandals over the last years. Naively anonymised data that rely on the fallacious distinction between "identifying" and "non-identifying" attributes are vulnerable to re-identification attacks. Notable examples of supposedly anonymised data release which led to lawsuits in the US are the AOL search queries and the Netflix Prize dataset. While some attributes can be identifying by themselves any attribute can be identifying in combination with others. For example: zip code, sex and birth date combined uniquely identify 87% of the US population [27].

Information disclosure access control must be aware of metrics drawn from data analysis to assess the true risks of privacy breaches. In order to do that, concepts like K-Anonymity and Differential Privacy will be used.

5.2.3 Minimal Disclosure

Individuals wish to control their personal information in the online domain, especially as more and more sensors are available that could be linked to the user in order to generate data. Organisations that are responsible for handling the information of individuals, seem to be minimally concerned with this wish, as can be seen from the large number of severe data leaks during the past years. One guiding principle, data minimisation, is hardly ever practiced and almost never enforced, which leads to very limited user empowerment with respect to privacy. On the other hand, the service providers which rely on the personal data of their users are asking for more accurate and detailed information, preferably authenticated by a trusted party such as the government.

Three features of privacy-friendly credentials are informally described in NSTIC [28] documents:

(1) Issuance of a credential cannot be linked to a use, or "show," of the credential even if the issuer and the relying party share information, except as permitted by the attributes certified by the issuer and shown to the relying party.
(2) Two shows of the same credential to the same or different relying parties cannot be linked together, even if the relying parties share information.
(3) The user agent can disclose partial information about the attributes asserted by a credential. For example, it can prove that the user if over 21 years of age based on a birthdate attribute, without disclosing the birthdate itself.

Several technologies like U-Prove [29] and IdeMiX have been developed in order to support this need in order to reduce the information to be disclosed.

5.2.4 Secure Authentication and Access Control in Constrained Devices

Embedded systems and especially wireless sensor nodes can be easily attacked. This is due to the fact that they are normally unprotected by cryptographic means. This is due to the fact that both types of devices suffer from severe resource constraints e.g. energy resources and processing power so that standard cryptographic approaches cannot be applied. Thus there is a necessity of development of the lightweight cryptographic solutions, which take the above mentioned constraints into consideration and are able to ensure the needed level of the security.

State of the Art: There are several lightweight security approaches designed for wireless sensor networks. The SPINS [12] protocols encompass authenticated and confidential communication, and authenticated broadcast. [13] uses asymmetric cryptographic schemes to exchange secret session keys between nodes and symmetric crypto approaches for data encryption. The approach presented in [14] provides authentication and authorization of sensor nodes, a simple but secure key exchange scheme, and a secure defense mechanism against anomalies and intrusions. In addition it supports confidentiality of data and usage of both symmetric and asymmetric schemes. In [15] the authors present LiSP: a lightweight security protocol, which supports all security attributes, but at a high level of power consumption when compared to the protocols described in [14]. The lightweight security approach presented in [16] is based on the RC4 stream cipher. It provides data confidentiality, data authentication, data integrity, and data freshness with low overhead and simple operation. In [17] the authors propose a lightweight security approach based on modification of elliptic curves cryptography. The reduction of the length of the security parameters influences the security level but also helps to save the energy needed for computation and communication. A similar approach is followed in [18]. However, the RSA with limited lifetime is still too expensive for WSNs due to the large size of the messages ($>$512bit). Such a size of the message requires in most of the WSN platforms packet fragmentation what makes the communication expensive and complicated.

When dealing with access control for IoT, the first considered approach consists in the potential applicability of existing key management mechanisms widely used in Internet that allows performing mutual authentication between two entities and the establishment of keying material used to create a secure communication channel. Nevertheless, due to the computational and power restrictions that must be satisfied in IoT networks, existing mechanisms [30] are not applicable for controlling the access to services offered by IoT networks. For example, while public key cryptography solutions demand high computational capabilities, schemes based on pre-shared keys are not applicable since they would require the pre-establishment of symmetric keys between an IoT device with every Internet host.

For this reason, in the literature we can find different works proposing alternative solutions [31, 32] to cope with the access control problem in IoT networks. For example, one of the earliest works in this area is developed by Benenson et al. [33] where a cooperative access control solution is defined. In this work, user authentication is performed by collaboration of a certain group of IoT nodes. Despite this scheme is carefully oriented to minimize the computation overhead in IoT devices, it increases communication overhead. Following this initial contribution, different access control solutions have been proposed for IoT networks. Depending on the employed scheme, we can distinguish between public key cryptography (PKC) and shared key cryptography (SKC) based solutions.

On the one hand, PKC schemes [34–38] are based on Elliptic Curve Cryptography (ECC) in order to reduce the computational requirements on IoT nodes. The different schemes vary on the approach used to implement the ECC based authentication. For example, while some solutions require a Key Distribution Centre to be available all the time, others develop a certificate-based local authentication. However, these proposals suffer from requiring high times to conduct user authentication (in some cases times are greater than 10 seconds).

On the other hand, SKC schemes [39–41] propose the user authentication based on symmetric key cryptography algorithms, which are more efficient than public key schemes. The use of these solutions requires both users and IoT nodes to share a secret key that will be used to carry out mutual authentication before granting the user access to the service offered by the IoT nodes. Compared to PKC, SKC schemes require lower computation and capabilities. Nevertheless, these schemes present serious scalability problems since they require the pre-establishment and pre-distribution of keying material.

In summary, we observe that existing access control solutions for services implemented within IoT networks do not offer a proper solution for future IoT. Furthermore, PKC schemes based on ECC favour scalability [42] given that they do not require the pre-establishment and pre-distribution of keying material. Nevertheless, SKC schemes are more advantageous in terms of computational efficiency.

5.3 Smartie Approach

SMARTIE will design and build a data-centring information sharing platform in which information will be accessed through an information service layer operating above heterogeneous network devices and data sources and provide services to diverse applications in a transparent manner. It is crucial for the approach that all the layers involve appropriate mechanisms to protect the data already at the perception layer as well as at the layers on top of it. These mechanisms shall cooperate in order to provide a cross-layer holistic approach.

SMARTIE will focus on key innovations that strengthen security, privacy and trust at different IoT Layers as depicted in the following table:

IoT layers	Security requirements
Applications (Intelligent Transportation, Smart Energy, Public Safety, Utilities, Service Providers, etc.)	• Authentication, Authorisation, Assurance; • Privacy Protection and Policy Management; • Secure Computation; • Application-specific Data Minimisation; • Discovery of Information Sources
Information Services (In-network Data Processing, Data aggregation, Cloud Computing, etc.)	• Cryptographic Data Storage; • Protected Data Management and Handling (Search, Aggregation, Correlation, Computation);
Network (Networking infrastructure and Network-level protocols.)	• Communication & Connectivity Security; • Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling
Smart Objects (Sensors for data collection, Actuators)	• Data Format and Structures; • Trust Anchors and Attestation; • Access Control to Nodes • Lightweight Encryption

5.3.1 Adaptation and Deployment

In order to demonstrate the advantages and potentially of our approach, we envisage the following application areas for deploying the project architecture.

5.3.1.1 Smart Transportation

Smart City Objectives

- Improving the management of the public transportation networks to foster greater use of sustainable transport modes and to provide time and cost benefits to travellers.

- Involving user smartphones in order to include additional information related to their travels.
- Improving the management of individual motor car traffic, to reduce travelling time in the town, improve traffic flow and reduce fine dust pollution.
- Extending traffic control systems with mobile traffic control systems to react fast on abnormal situations, planned ones (e.g. road reconstruction) and also unplanned ones (e.g. accidents).
- Exploiting heterogeneous wireless sensor networks placed on public transport vehicles and in the environment (streets etc.) e.g. stationary traffic sensors/actuators placed at cruces of the transportation network.

Usage

- Public transportation companies monitor the current demand of travellers for public transportation for certain routes and optimise the number of vehicles to match the demand. They also monitor location of all public vehicles.
- Travel plan component located on the cloud infrastructure calculates the best routing option for the traveller taking into account the traveller location, expected arrival times and current traffic conditions. This information is then forwarded to the associated smartphone application and presented to the traveller.
- City traffic authorities monitor the current traffic conditions:
    - To optimise the traffic lights in order to achieve better traffic flow.
    - To adapt speed limitation signs.
    - To indicate detours in case of road re-construction, accidents or other emergency situations.
- The required adaptation of the individual car traffic is then indicated via adapted traffic light switching, updated electronic traffic sign, etc.

Security and Privacy Challenges

- Information related to location of public vehicles should be accessible to system users according to the access policy and privacy rules.
- All data exchange between the sensor, actuators and backend server should be implemented in a secure manner.
- All the data related to the travellers' location and activity should be considered private, and it should be treated according to the privacy rules.
- Integration systems owned by different parties such as public authorities and private companies providing telematics services.

5.3.1.2 Smart campus

Smart City Objectives

- Monitoring energy efficient in the campus considering energy consumption and energy generation.
- Evaluating real-time behaviour of systems jointly acting as a sustainable ecosystem.
- Providing the user capability to interact with the system to facilitate the improvement of the energy efficiency.

Usage

- Energy Supervisor entity will be able to collect from the different sources: information in real time about building consumption and energy generation from the different entities involved (photovoltaic generators).
- Energy Monitoring entity will collect data from the sensors being deployed and also data aggregated and summarized about the different energy producers to take decisions over different actuators involved in the system.
- Energy Producer will provide data aggregated to the Entity Monitoring based on the agreement established and will provide more detail data to the Energy Supervisor as main regulator.

- User will provide in certain situations their positions and presence information to the Energy Monitoring entity by means of the sensor within the building or light-street pathways.

Security and Privacy Challenges

- Access to the data of the sensor should be controlled based on access control and privacy rules. Hence only certain services of the entity monitoring could read or act over them especially in the case the monitoring entity is a third party.
- The exchange will require mechanisms including data protection and integrity in the transfer between the different parties.
- Scalable and secure management protocol which lets the verification and authentication of new sensors deployed and ensure the extension of the trust domain to new devices in the deployment environment.
- Entities are actually restricted to use the data based on the national protection data law. They will like to explore how to reuse the data and possible being able to share to third parties but also controlling what can be shared based on legislation.
- Data exchange between entities needs to follow data minimization principles and allow traceability.
- User data information exchange could be in some case anonymous and in other case could be needed some control over the distribution of data.

5.4 Conclusion

The Internet of the Future will be a cluster of heterogeneous current and future infrastructures (networks, services, data, virtual entities, etc.) and of usages with mainly decentralized security and trust functions. The emergence of sensing and actuating devices, the proliferation of user-generated content and nascent (Internet-only) services delivery create the need to address trust and security functions adequately.

The idea of the IoT brings new challenges regarding security and in consequence also for privacy, trust and reliability. The major issues are:

- Many devices are no longer protected by well-known mechanisms such as firewalls and can be attacked via the wireless channel directly. In addition devices can be stolen and analysed by attackers to reveal their key material.
- Combining data from different sources is the other major issue since there is no trust relationship between data providers and data consumers at least not from the very beginning.
- Secure exchange of data is required between IoT devices and consumers of their information.

A lot of research effort was put in the protection of wireless sensor networks that might be thought of one of the data sources, but the integration of wireless sensors into a heterogeneous service architecture is still an open issue.

Contrary to these mechanisms developed through history, current trends in the Internet lead to implementation of security and trust by *ex-ante* automatic access controls and technical reliance on secrecy. However, history teaches us to consider setting emphasis on usage rules rather than access rules or collection rules, and rely on the principle of transparency, accountability and enforcement in order to build trust in our Internet society.

SMARTIE solutions will provide a set of innovations and enhancements to address the challenges imposed by the application domains.

References

[1] Seshadri, A., Luk, M., Perrig, A., van Doorn, L., and Khosla, P.SCUBA: Secure code update by attestation in sensor networks. InWiSe '06: Proceedings of the 5th ACM workshop on Wireless security (2006), ACM.

[2] Aurelien Francillon, Claudio Soriente, Daniele Perito and Claude Castelluccia: On the Difficulty of software based attestation of embedded devices. ACM Conference on Computer and Communications Security (CCS), November 2009

[3] Benjamin Vetter, Dirk Westhoff: Code Attestation with Compressed Instruction Code. IICS 2011: 170–181

[4] Trusted Computing Group (TCG) Specification. URL: http://www.trustedcomputinggroup.org/