6

Trusted IoT in the Complex Landscape of Governance, Security, Privacy, Availability and Safety

Elias Z. Tragos[1], Jorge Bernal Bernabe[2], Ralf C. Staudemeyer[3], Jose Luis Hernandez Ramos[2], Alexandros Fragkiadakis[1], Antonio Skarmeta[2], Michele Nati[4] and Alex Gluhak[4]

[1]FORTH-ICS, Greece
[2]Universidad de Murcia, Spain
[3]University of Passau, Germany
[4]Digital Catapult, United Kingdom

"Trust but verify". Ronald Reagan

6.1 Introduction

The Internet of Things (IoT) has attracted a lot of attention the last decade due to the unprecedented opportunities it provides for economic growth and for improving the quality of life of citizens. The advances in the IoT domain have been quite important and especially in the areas of IoT hardware, data and context extraction, service provisioning and service composition, cognition, interoperability and extensibility. Considering these advances, the IoT technologies are being considered quite mature for being deployed in real world environments and this has already been done in many cities around the world. Thousands of smart devices are now operating in cities, gathering information and providing smart applications for e.g. environmental monitoring, energy management, traffic management, smart buildings and smart parking [1, 2]. These devices are equipped with intelligence and are able to monitor and control physical objects, thus creating a new "Cyber-Physical" world [3].

The latest advances in the manufacturing engineering has allowed the minimization of the size of IoT devices so that they are not easily noticed.

Additionally, the humans are nowadays so familiar with computers and small devices that do not even pay attention to them, considering them as a part of their everyday lives. These two facts are proving how true for IoT was the projection from Marc Weiser back in 1991 when he described the "computer of the 21st century" using the phrase [4]:

> The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

It is easily understood that this phrase can characterize the IoT technology and its future inclusion within the everyday activities of the humans. The projection is that people will become so familiar with IoT that they will consider the technology as part of their lives. Although this shows the huge potential of IoT and its power, it raises significant concerns regarding security, privacy and safety. Imagine thousands and millions of small, unnoticeable devices spread around in city areas and within buildings monitoring and logging the everyday activities of people and controlling physical objects (doors, windows, cars, traffic lights, etc.) [5]. This can be quite worrying for the privacy of the people if the IoT systems are not designed to be secure and privacy preserving. However, IoT is also susceptible to attacks against the safety of the people, if the actuators are faulty or being hacked [6].

In this respect, there is increasing attention lately towards designing and developing fully secure and privacy preserving IoT systems. The main requirements for secure IoT systems are: (i) to exchange information from the devices to the applications in a secure way, (ii) to safeguard users' and citizens' private information, and (iii) to provide reliable information. To meet these requirements, IoT systems have to include from their design phase functionalities for secure device configuration, encryption, confidentiality, device and user authentication and access control, integrity protection, data minimization, etc. All these functionalities have to be included in the design phase of the IoT systems, because any post-mortem corrections will only cover some holes but won't provide full-scale security [7].

In the previous two versions of the IERC book [8, 9], we have extensively covered the areas of security and privacy in IoT. In this chapter we will focus on another very important area for ensuring the provision of reliable information and for maximizing the security, privacy and safety of IoT: "Trust". The remainder of this chapter is structured as follows: in Section 6.2 the basic concepts of trust in the IoT are described, together with the reasons for

evaluating trust in the IoT world. In Section 6.3 we provide the basic concepts of trust management in the IoT, while in Sections 6.4 and 6.5 we present ways to calculate the trustworthiness of IoT devices and services. In Section 6.6 we present an analysis of using Trust with regards to privacy and personal data sharing. In Section 6.7 we present the improvement of the authorization mechanism with the usage of trust and reputation. In Sections 6.8 and 6.9 we present two examples of use of trust evaluation for an indoor positioning system and for improving the routing mechanism for increased confidentiality. Section 6.10 concludes the chapter.

6.2 The Need for Evaluating Trust in IoT

Trust is a very important concept for IoT since it can affect the adoption of the IoT systems by the humans. It is reasonable to assume that if the humans do not trust an IoT system and its components, they will not be willing to use it. The same stands for the service providers, the municipalities, the companies, and all kinds of IoT stakeholders. If they are not convinced that the IoT systems are reliable, they will not be willing to invest in them. Trust is closely interconnected with reliability and reputation. In Information and Communication Technologies (ICT) the concept of trust has been considered crucial for any digital interaction between multiple entities.

The concept of Trust can be defined as the level of confidence that an entity has on another entity to behave certainly in a given situation [10]. Up to recently, the notion of Trust was only used for humans, but lately it is also associated with machines, devices and software. Here, we also have to make a distinction between Trust and Trustworthiness. Trust can be considered as subjective, because it is a belief of an entity (user, device, etc.) that another entity is functioning according to some predefined criteria, and these criteria are subjective to the former entity. On the contrary, Trustworthiness, which is an abstract concept, is considered as objective, because it is described as a metric of how much an entity deserves the trust of other entities [11]. This metric is built upon several criteria, i.e. evidence of current and past behaviour, availability, data reliability, security, etc. Trustworthiness can also be calculated as "absolute" or as "relative" to other entities. For example, we can say that a device is trustworthy in general or that it is more trustworthy than its neighbours [12].

Another very important concept is the "Reputation" of an entity [13]. Although sometimes it is used interchangeably with trustworthiness, reputation is considered as an estimator of the trustworthiness of an entity according

to the criteria of another entity. Since the trustworthiness of an entity is very difficult to be evaluated, the metric that is widely used instead is the reputation. In order to calculate the reputation of an entity, the metrics of multiple other entities are fused and compared according to certain criteria.

As mentioned above, IoT systems have to be trustworthy so that they are adopted by all stakeholders. The trust in the IoT domain can be considered at many scenarios which include information exchange between the various entities of the system. Since users and devices are exchanging information between each other, we can consider trust (i) from users to devices that send them information, (ii) from devices to users that send actuating commands, and (iii) between devices that exchange information and actuating commands.

For example, in Machine-to-Machine type communications (M2M) the devices that are exchanging information have to know the reputation of other devices so that only the devices that are trustworthy will handle sensitive or critical information. So, in a scenario where a temperature sensor sends commands to the air-conditioning system to turn on the heating because the temperature in the room is very low, the air-conditioning should be sure that the temperature sensor is trustworthy in order to execute the command.

Furthermore, only trusted users have to be allowed to manage critical data or actuators. This is quite important, because in a scenario involving controlling of physical objects, e.g. doors, windows or even fire-extinguishers, malicious (untrusted) users may create incidents against the safety of other users. However, since in the IoT devices are also able to control other devices, these incidents can also occur not only by user actions (i.e. hacking devices), but also by faulty or malfunctioning devices.

Another scenario can be assumed when users are receiving measurements from devices, i.e. measurements for traffic in the center of the city in order to identify the fastest route towards their work. If the system does not provide them reliable traffic information, the users will stop using this system, because they will not trust it.

Apart from the previous examples that are mostly related to providing reliable applications and services, trust in the IoT can also be related to the reliable configuration of the various system components. One such example will be given in Section 9.6. Trust can be included in all types of cooperative networking mechanisms, for example as described in [14] in cooperative spectrum sensing and assignment, where measurements from various devices are fused in a gateway for identifying spectrum opportunities and for deciding which is the best spectrum portion to operate on. Any measurements from

untrusted sources may affect the decision of the system and may result in degraded system performance.

It is evident that considering Trust in the design of an IoT system is of outmost importance for improving its reliability, its security and the safety of its users. In the next sections we will discuss the recent approaches within IERC for evaluating and managing trust in IoT systems.

6.3 Trust Management in IoT

The main objective of a Trust management system in IoT is to be able to evaluate the trustworthiness of various components of the system and to use these values in order to provide reputation information to users of the IoT services or to internal configuration services.

Trust management systems use trust and reputation models that are based on five generic steps, as described in [15] and also discussed in [12]. The main goal is to enable one entity (human or device user or a service) to identify the entity or group of entities that are more trustworthy for a certain transaction, based on specific criteria. As described in [16] any IoT trust model should be designed according to the following:

- **Observation**: This step is the most important step since it is responsible for monitoring the parameters of the system entities and their behaviour, allowing the extraction of results with regards to the trustworthiness of the entities. The monitoring of these parameters can be performed by the system devices or by specific entities that are called observers. The collected information can originate from standalone observers or from groups of observers, which then fuse the information for extracting more objective results.
- **Scoring**: When the observers gather the information for an entity they can give it a proper weight which will result in a reputation score. This will be done for all entities in the system (considering that adequate information has been gathered). This reputation score can be given by an interested agent or a centralized entity or by many entities collectively. Finally, the reputation scores can be used in order to rank the entities in terms of trustworthiness according to some criteria.
- **Selection**: Once the reputation scores and ranks are in place, the next step is to select the entity which is more appropriate for a specific transaction, i.e. that provides a specific IoT service. Of course this service might be provided by more than one entity, thus the user has to select the most appropriate according to some criteria.

- **Transaction**: When a service has been selected, the transaction takes place and more information regarding the entity (that provides the service) is being gathered by the system components, as a feedback.
- **Rewarding and punishing entities**: Trust management systems should also include functionalities for rewarding the entities that are performing according to the criteria and have high reputation. At the same time, the system must punish malicious or untrustworthy entities that may negatively affect system decisions or the systems' overall reliability and trustworthiness.

Based on the above and as described in [16], a trust model for the IoT can be split in two main sub-models: (i) a trust evaluation model and (ii) a reaction model. The Trust evaluation model is responsible for gathering trust metrics and trust ratings for the system entities and evaluating them for extracting their reputation, while the reaction model is responsible for reacting to these reputation evaluations, either by rewarding or by punishing the entities.

The trust evaluation model has to be lightweight, keeping a small state that is updated regularly, so that it can also run on constrained devices. For the trust evaluation model, as proposed in RERUM [16], the main idea is that there is a set of observers that are providing trust ratings for a specific entity in mind (be it software, hardware, user or object). These trust ratings are trust values that relate to the confidence that this observer has on this entity according to some criteria. Trust ratings can also be provided by the administrator of the system or by other users that have had past interactions with this entity. These trust ratings are then fused into a centralized component (i.e. reputation manager) that extracts the reputation of this entity. Then, when a user, a service or another entity wants to interact with the entity under evaluation, it queries this centralised component to get the reputation and decide according to its own rules if it can trust this entity or not.

A reacting model can be considered as another set of rules that describe the actions of the system when a reputation for an entity is evaluated. Any reputation change may trigger reactions by the system [16]. For example, when a reputation of a trusted entity is being decreased, an alert may be triggered so that the system will search to find what is the cause of this reputation decrease. On the contrary, when a reputation of an untrusted entity is increased, another alert may be triggered so that this entity will be closely monitored to identify if it has become trusted or not. The reactions are based on specific rules that are mainly being defined by the system administrator. Various reactions can be

defined, i.e. logging alerts, warning administrators, disabling or re-enabling services, stopping/starting gathering data from devices, initiating networking or system configuration mechanisms, warning users, etc.

In the following subsections, we present details for the trust evaluation model, as described in the RERUM [17] and Sociotal [18] projects. The focus is on devices and services, which are of outmost importance for the IoT. Although the end users are also very important when interacting with IoT systems, the trust evaluation for users is not discussed within this chapter since existing schemes for user reputation in the Internet can be applied [17, 20, 21].

6.4 Trust for Devices

The trust model for IoT devices aims to improve the reliability and trustworthiness in IoT scenarios where disparate and unknown devices interact each other and provide data to IoT applications. The device-based trust model follows a multidimensional or multi-layered approach to calculate the overall trustworthiness of an IoT device. The model describes the procedure employed to quantify several trust dimensions (or trust metrics). Then, the dimension's values are aggregated to come up with a final score of trust i.e. by means of fuzzy logic or data fusion techniques such as the Dempster Shafer theory of evidence to avoid outliers or malicious nodes [22].

The trust dimensions correspond to different properties that have to be taken into account in the IoT paradigm. Contrary to past approaches that considered only reputation between different devices and data reliability, lately other parameters such as communication reliability, security aspects and social relationships between the devices are being considered. In the end, this approach leads to a more accurate and reliable value of trustworthiness about a given IoT device, which can be exploited either for improving the reliability of the provided services or for increasing the overall security of the IoT system.

The trust model follows a hierarchical and a layered approach in which the different dimensions are split in categories and subcategories, which in turn are composed by measurable properties. This hierarchical approach enables the trust model to be extensible, allowing users to consider and include new properties to the model. Nonetheless, the trust quantification procedure is the same regardless of the amount of properties taken into account. In fact, some of the trust properties explained below could be optional in case the

implementation of the IoT system is unable to measure these properties. Of course in that case the resulting trustworthiness value of the device will be sub-optimal, but it will give a good indication [23].

The trust dimensions can be measured in different layers within an IoT network. Some of them can be measured on the devices themselves and the values will be exchanged between the devices and fused in order to extract the reputation of each of their neighbour devices. Other dimensions may be calculated at cluster heads or gateways, which will do the fusion of the reports of the devices and then they will feed back the results to the devices. This approach may save enough computational resources on the devices in case the trustworthiness evaluation is complex.

Finally, some dimensions may also be calculated at the backbone cloud servers or the IoT middleware, where centralized trust management schemes may be employed, which will allow the fusion of measurements from more devices connected to different gateways to have a more accurate reputation evaluation for the devices.

In IoT the evaluation of the trustworthiness of a device can be generally based on multiple criteria that can be grouped into 5 categories: (i) communication criteria, (ii) security criteria, (iii) data-based criteria, (iv) social relationship criteria, and (v) reputation criteria.

6.4.1 Communication-based Trust

The communication based criteria correspond to the quality of the communication links between the devices. Although someone may think that the communication link quality is not directly related with the trustworthiness of the devices, this is not entirely true because the link quality may affect significantly the performance of the device's transmissions. This will in turn affect the Quality of Service provided by this device (in terms of throughput, delay, jitter, etc.) and its availability.

Within RERUM, the communication based trust criteria are mainly used for evaluating the networking related trustworthiness of the devices which is then used to consider the trusted devices within network-related cooperative mechanisms such as cooperative routing, spectrum or channel allocation, network monitoring, etc. In this respect, the main criterion considered is the link quality statistics based on a link quality metric. In RERUM, the chosen metric is the *Expected Transmission Count* (ETX) metric which has been proved in the literature that is quite accurate in evaluating the reliability of the link between any two nodes.

The ETX is very widely used for routing mechanisms because apart from providing good reliability results it is also quite simple and computationally efficient, so that it can be easily calculated even in the very constrained IoT devices.

As described in [25], the ETX calculated for node *i* by node *j* is defined as:

$$ETX_{i,j} = \frac{1}{f_{i,j} \cdot r_{i,j}},$$

where $f_{i,j}$ is the metric for the forward delivery ratio, namely the probability that a packet sent from node *i* is received by node *j*, and $r_{i,j}$ is the reverse delivery ratio, namely the probability that the acknowledgement packet from node *j* will be received by node i.

It is easily anticipated that the ETX is a metric of the retransmissions that a device is performing in order to successfully transmit a packet to the destination.

Basically, the ETX expresses the average number of transmissions that are required for a successful delivery of a packet to its destination when there are transmission failures due to degradation of link quality (e.g. interference, collisions, etc.).

6.4.2 Security-based Trust

The security trust criteria are mainly related with the behaviour of a device as this is anticipated by its neighbours. In the literature, these criteria are also described as behavioural trust metrics.

These metrics correspond to specific types of attacks as described in [26] and presented in Table 6.1.

By evaluating and fusing these metrics, the security-based trust of the devices can be calculated, which will show how susceptible this device is in these types of attacks, affecting it overall trustworthiness and the way the rest of the neighbours behave towards this device.

These metrics can be calculated mainly at the device level or at the cluster head/gateway level, when the devices are incapable (in terms of resources) to do these calculations. In order to calculate these metrics at the device level, the devices have to be able to go into promiscuous mode [16].

If one wants to measure some of the metrics of the table (i.e. data/control packets forwarded, metric No. 1 in the table), every time a device sends a packet to one of its neighbours (in a multihop network) it should enter into promiscuous mode so that it monitors if the destination neighbour forwards the

Table 6.1 Neighbour behaviour monitoring [26]

No	Trust Metric	Monitored Behaviour	Attack Addressed
1	Data/control packets forwarded	Data/control message/packet forwarding	Black-hole, sinkhole, selective forwarding, denial of service, selfish behaviour, Control/routing message dropping
2	Data/control packet precision	Data integrity	Data message modification, Sybil and any attack based on routing protocol message modification
3	Availability based on beacon/hello messages	Timely transmission of periodic routing information reporting link/node availability	Passive eavesdropping, selfish node
4	Packet address modified	Address of forwarded packets	Sybil, wormhole
5	Cryptography	Capability to perform encryption	Authentication attacks
6	Routing protocol execution	Routing protocol specific actions (reaction to specific routing messages)	Misbehaviours related to specific routing protocol actions
7	Battery/lifetime	Remaining power resources	Node availability
8	Sensing communication	Reporting of events (application specific)	Selfish node behaviour at application level

correct packet, if it forwards a modified packet or if it drops the packet. Then, it can change the respective trust rating for this neighbour device accordingly.

In RERUM's view, it can be assumed that the metrics (1), (2), (3), (4), (5) and (8) are the most important ones, while the others can be used in specific cases.

The metrics can be used either "as is" or by assigning different weights to each one for giving larger weight values to the most "important" metrics according to the application what will use the trustworthiness value of the device. One such example is given in [26]:

$$BR_{i,j} = \sum w^s \times BC^s_{i,j}, \text{with} \sum_{s=1}^{n} w^s = 1.$$

In RERUM [27], we have used formulas for the metrics No. 1 and No. 2 in the table above, namely for packet delivery and packet integrity. These are

assumed to be the most commonly used in this type of trust criteria because they represent the most common attacks for malicious users in IoT networks.

All devices within an IoT network are assumed to be monitoring the behaviour of their neighbours when they are interacting with them.

For these two metrics, the following statistics can be used: (i) *Packet Drop Rate* (PDR), as the ratio of the number of dropped packets divided by the total number of received packets and (ii) *Packet Modification Rate* (PMR), as the ratio of the number of modified packets divided by the total number of forwarded packets.

However, these metrics correspond to the values observed by one device for one of its neighbours. Assume that a receiver device '*j*' receives a packet, each neighbour '*i*' overhears the forwarding behaviour of '*j*' and updates accordingly the values of $PDR_{i,j}$ and $PMR_{i,j}$. Then, we can use a combined metric called aggregate *Misbehaviour Rate* (MBR) for the device '*j*' as perceived by device *i* is calculated as:

$$MBR_{i,j} = w \times PDR_{i,j} + (1 - w) \times PMR_{i,j}$$

where $w \in [0,1]$ is a user-defined weight controlling the balance between the behavioural statistics.

6.4.3 Data-Reliability based Trust

One of the most important trust metrics for IoT devices is related to the reliability of the data they produce. By using the term "data" we refer to the measurements the IoT devices are producing from their onboard sensors, i.e. environmental, location, energy, etc. These measurements are being used by the services of the system and if they are unreliable they may severely degrade the trustworthiness of the overall system. Consider for example a weather station producing wrong values for the temperature and the rain level in the centre of the city and the citizens are falsely informed and are not properly dressed. Another example may be regarding the alerts for fire or hazardous gases. It is evident thus that the data reliability is very important because it can even affect the safety of the users/citizens.

The data reliability based trust metric is also described in the literature as "service-based metric" [16]. Its evaluation is done by comparing the measurements with known measurement patterns, past measurements or measurements of other devices at the same area, monitoring the same physical object and the same property of the object. This means that we should only compare temperature measurements from different sensors monitoring the same room

and not different rooms or measurements of temperature with humidity. The goal is to identify inaccuracies in the measurements observed by the devices. In this direction, a statistical analysis of the measurements' time series can be done (i.e. the deviation from the average value reported in X previous timeslots) and/or compared to the measurements reported by another similar device. For this type of calculation, there have been proposed many techniques in the literature for i.e. outlier detection in WSNs, see the references in [28].

What is different in the IoT world, as described in RERUM, is that the IoT devices may have various sensors of different types onboard and may be providing multiple services. As a result, when the system needs to evaluate the data-based trust metric, this evaluation must be done separately for each one of these services and then it can be combined, if needed, to calculate the overall data-based trustworthiness of the device. In most cases, the applications or the functions that will use the data-based trust rating will only need the rating for one service and the overall trust rating may not be of importance for them. However, for self-monitoring purposes, the overall trust rating might also be important.

Let's assume that each device can provide 'N' services, then N data-based trust ratings, one for each service it provides can be calculated. A low trust rating for one service does not mean that other services provided by different sensors will also be unreliable. However, combining the trust ratings for services provided by a specific sensor can provide results about the malfunctioning of that sensor or its driver being hacked. Furthermore, the fusion of the trust ratings of all services can only give a hint if the node is tampered with/hacked so that it reports intentionally false measurements.

So, we can have trust metrics as below:

$$OSTM_i = \sum_{S_x=1}^{N} w^{S_x} \times STM^{S_x} i,$$

where OSTM is the overall service based trust metric and the STM is the trust metric for each one of the provided services Sx.

6.4.4 Social Relationship based Trust

In IoT, social parameters can also be used for evaluating the trust rating of IoT devices. These social parameters are based on the emerging Social IoT (SioT) paradigm, which assumes that devices can establish social relationships with each other. In such a case, devices are assumed to be grouped into trust

bubbles or communities based on their social relationships, i.e. if they belong to the same owner, if their owners are friends, are working together, if they are located at the same area, if they have the same manufacturer, etc. The Community of the devices is formed when the devices that share common interests are interacting and the more they interact the stronger becomes the trust relationship between them [23].

An IoT trust model has to consider the social relationship between a device *'i'* when assessing the trust of a device *'j'*. Different weights can be given to the relationship between the devices considering the links among them. The weights assigned by the trust model to the social relationships should be configurable by the user in the interval [0..1] and should satisfy:

$$W_{B_p} > W_{B_f} > W_{B_o} > W_C$$

Where B_p is the Personal Bubble, B_f is the Family Bubble, B_o is the Owner Bubble and C is the Community Bubble. Apart from this, when the devices do not belog in one of these bubbles, the trust model can calculate the degree of *Interest-In-Common* or the *Friends-In-Common*. The Interest-In-Common I_j^i can be calculated as the ratio between the interest that both devices share over the total amount of interests of the evaluator device

$$I_j^i = \frac{interest(i) \cap interest(j)}{interest(i)}.$$

Similarly, the Friends-In-Common F_j^i can be calculated as the ratio between the number of friends that both devices have in common, and the total amount of friends of the evaluator device

$$F_j^i = \frac{friends(i) \cap friends(j)}{friends(i)}.$$

It should be noticed that to quantify the interests and friends in common the devices should be able to exchange, in a common way, their list of interests (e.g. services and capabilities) as well as the lists of friends.

6.4.5 Reputation based Trust

As mentioned before, an IoT trust model should consider recommendations from multiple devices about a particular device *j*. Let O_j^i be the Opinion score about device *j* given by device *i*. It is also reasonable to assume that the opinions of different devices may have different impact on the opinion

score of other devices, that's why there can be weights for each one of the "recommender" devices. This weight can be calculated based on the past behaviour of this device in the opinion scores or also on the trustworthiness of the device [23]. Thus, the opinions are subject to a credibility process where each reputation evidence coming from a device *i* is subject to credibility factor Cr_i in the interval [0..1], where 1 represents the highest credibility. Therefore, the Reputation property in our trust model is given by $R_j^i = O_j^i * Cr_i$.

Since the opinion scores are calculated by the trust ratings provided by the devices for their neighbours, the results can be biased leading to uncertainty. For this type of reputation evaluation, other techniques for trust fusion can be used, i.e. the Dempster Shafer theory of evidence, which is a powerful mathematical framework able to handle uncertainty of the complete probabilistic model describing the system under consideration.

The calculation of the reputation metric can be done either at the device level, at the gateways, or even at a centralized or cloud based IoT middleware [16]. If calculated at the device level, each device should store the direct evidences and recommendations provided by other devices to quantify trust of each neighbour. However, this can be quite demanding in terms of computational and storage resources and might not be appropriate for constrained IoT devices. Thus, either evidences about devices which they do not interact for a long period of time should be discarded or the evaluation of the reputation trust should be escalated to the cluster heads, gateways or the middleware.

6.5 Trust for IoT Services

The IoT Services provide streams of information towards the end users. Thus when evaluating the reputation of a service, the goal is to provide enough information so that a user can have an answer to the question if he can rely on a specific service or if the service provides reliable measurements. As mentioned in the beginning of Section 9.3, a user has to query the reputation manager for getting the reputation value of that service. We can assume that for privacy reasons only authorized users are allowed to query the reputation manager for specific services.

IoT services can be either simple services provided by a single device or composed services that combine data from many devices. Of course, behind the provision of the service lies a business logic that also has some rules for managing the data from the devices. The reputation of a service is directly related with the reliability of the data of this service. As a result, for evaluating

the reputation of a service, the trust rating of its data stream has to be evaluated. Thus, an observer has to be allocated to monitor this data stream. The observer should basically extract statistics for the data stream, in order to be able to identify changes in the pattern of the data stream, i.e. to identify when there are jumps or values that are outside the "normal" limits of the data stream [16].

For the statistics of the data stream, the first calculation that has to be done is the average value, that can be calculated as an overall average or as a moving average on a sliding window (according to the criteria of the administrator and the properties of the data stream). Here the challenge is to be able to calculate the average without using too much storage, so that even constrained devices will be able to calculate it. Then, the observer has to calculate also the limits and the thresholds of the data stream (in terms of minimum and maximum value) so that an alert will be fired if a value outside these thresholds is measured [16]. For example, when measuring the temperature in a room, it might have been noticed that in the past the minimum value was around 5 degrees and the maximum around 35 degrees. If the temperature monitoring service provides values of around 50 degrees, an alert has to be fired for a possible fire in the apartment or for a possible tampering with the service's data (i.e. a hacked device or a n intermediate entity altering the measurements). In the latter case, the reputation of the service has to be lowered.

Apart from the values outside the thresholds, sudden jumps in the data stream might cause change in the reputation of the service [16]. For example, in the previous scenario of a temperature monitoring service, if the current temperature of the room is around 10 degrees and suddenly the service starts providing values around 25 degrees this might fire an alarm despite the fact that the values are within the thresholds. Such a sudden jump has to be evaluated because it might mean that the service might be providing false values and its reputation has to be decreased. For this reason, the alarm might to be a warning to the administrator of the system to check what is happening in that room. Another type of an alert, may cause the cross-evaluation of the values of the temperature service with the values of other services, i.e. of a smoke detector service to see if there is indeed a fire in that room, etc.

It can be easily understood from the latter scenario that in order to evaluate the reputation of a service, the calculation of the statistics of its data stream might not be enough. Thus, there needs to be a mechanism to allow the cross-evaluation of the statistics of different data streams (assuming that some data streams are known to be trustworthy).

For the usage of the statistics of the data streams, the definition of the thresholds and the identification of the jumps, specific rules have to be defined either by the administrator of the system or by the users that want to receive a service [16]. Within RERUM, the expert system CLIPS [29] has been selected for the implementation of the rules in a simple but powerful way.

6.6 Consent and Trust in Personal Data Sharing

The volume of data is doubling every two years, of which two thirds is generated by individuals, in particular with adoption of new wearable devices [30]. This growth has been driven by the increasing of both the number of connected devices in our lives as well as their capabilities. This trend looks set to continue with data traffic from IoT devices rising from 2% share of the total in 2013 to 17% in 2020. Only considering the Public Health sector, sharing of personal data is estimated to generate 100Bn EUR value per year. This derives from the creation of new services such as those providing holistic approach to healthcare, where prevention and caring of long-term conditions can be made more effective by combining information beyond those included only in medical records, but including also any related life style information (such as shopping and dietary habits, fitness/exercise information etc).

In the current IoT service model, personal data are mostly collected by a multiplicity of Service Providers, each one offering a dedicated service, most of the time provided through a freemium model [31], whose main revenues stream is generated by third party exploitation of generated data for target advertisement.

This currently undermines individuals' trust in sharing IoT personal data, thus hindering its associated value. A recent Digital Catapult report on Personal Data and Trust [32] highlighted that 60% of consumers are uncomfortable about sharing their data, with a further 14% feeling so uncomfortable that they do not want to share their data at all. Individuals' reluctance to share personal data becomes higher when commercial purpose is foreseen while more confidence is put in sharing data for research purposes. However, people feel uncomfortable with their information being used for secondary purposes if not enough trust is put in the organization originally collecting the data and re-distributing them to third parties [33]. Preparedness of individuals to share their data varies considerably by sector, with more than a third of individuals trusting banks and the public sector, but less than 5% trusting mobile network operators, utilities, retail and media companies. In general 80% of consumers

feel organisations hold their data solely for economic gain. Even for public sector organisations, only 45% of consumers believe they hold data for their benefit.

There is a need to regain individuals' trust by increasing transparency on how data are collected, managed and shared. *Control* is the key and to support this change in the current trend, the new General Data Protection Regulation [34] (aka GDPR), recently approved and in force by early 2018, is putting the end-user (aka *the individual*) at the center of this process, while promising expensive sanctions for those businesses big and small failing to comply to its principles (e.g., up to 100 Mio or 4% of their annual turnover fines for big corporates and up to 100K or 2% of annual turnover for SMEs).

Figure 6.1 shows what are the elements required to develop a personal data sharing ecosystem, where trust should be maintained by giving individual control on how their personal data are collected and further used.

Attribute Providers collect personal data through the provisioning of a service as part of their day-to-day operations (e.g., banks, utility suppliers, IoT service providers, etc.). To avoid to lock such data in silo'ed systems, and to allow further access, reuse and combination of them for creation of new services by a growing ecosystem of SMEs, data need to be brokered according to well-defined rules (aka *the Scheme*), enforced by *certified* Scheme Operators.

For ensuring compliance to GDRP, while increasing individuals' trust, the envisioned Scheme should set, among others, the following principles:

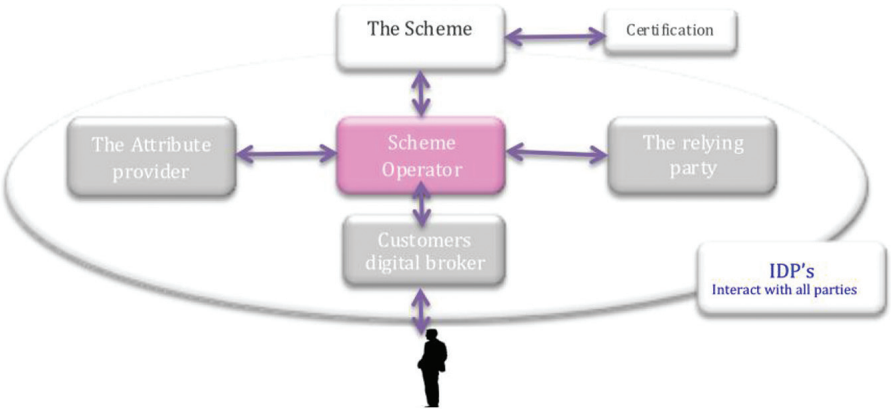

Figure 6.1 Personal data sharing ecosystem.

- *Transparency*: Privacy Notices for data sharing should be easy to access and to understand, explaining how data are processed, what are the individuals' rights and how they can be enforced;
- *Consent*: Valid consent must be explicit for data collected and the purpose for the data collection should be stated. Data controllers must be able to collect "consent" form end-users (opt-in) and consent might be withdrawn;
- *Erasure*: Attribute Providers (e.g., the data controllers) are the entry point for the erasure requests and need to inform third parties (e.g., the Relying Parties).

If control means trust for individuals [35], to exercise this control, hence the consent to sharing cross-domain personal data, there is the need for tools and open standards. Consent Receipt [36] represents one of such tools.

The Consent Receipt inherently, *by being a record of consent given at the point of consent (e.g., when first accessing a service)*, provides proof of consent and delivers contact information to communicate about consent directly to the end user. According to GDPR and in order to guarantee individuals' trust, consent should be: *freely given* (opt-in); *informed*, i.e., 'no legitimate interest' in using collected data should be allowed; *specific*, i.e., bound to the purpose the data are collected for; *unambiguous* and *transparent*, i.e., additional personal data cannot be vaguely collected while offering a service; *dynamic*, i.e., it can change over time and be revoked at any time.

The Consent Receipt provides the evidence that the consent for personal data sharing is properly collected and guarantee individual control over it, thus maintaining trust in the created ecosystem.

Figure 6.2 provides a summary of a Minimum Viable Consent Receipt standard's elements, currently under development by the Kantara Initiative through its Consent and Information Sharing Working Group and the support of the Digital Catapult Personal Data Network (https://pdtn.org).

In particular:

- *Header*: The purpose of which is to set out administrative fields for the consent transaction, including a unique Consent ID;
- *PI (Personal Information) Controller Information*: This section identifies the individual and company that is accountable for data protection and the privacy policy (included in the receipt or linked to otherwise) to which the consent is bound;
- *Purpose Specification*: This section clearly specifies the purpose(s) for which Controller is collecting additional Personally Identifiable Information [37];

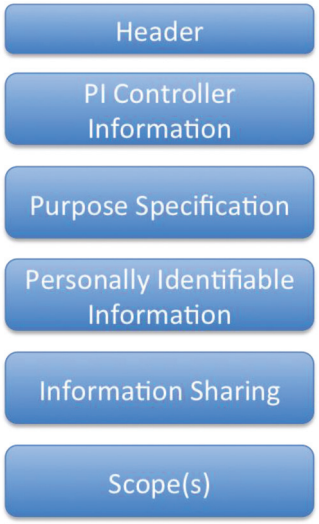

Figure 6.2 Consent receipt structure.

- *Personally Identifiable Information*: This section specifies the personal information categories and related attribute collect by the PI Controller;
- *Information Sharing*: When applicable and stated in the Privacy Policy, the purpose of this section is to provide the individual with information about how their information is shared with third parties;
- *Scope*: This section specifies the technical and policy scope within which the collected data are used.

Like a paper receipt for any purchased good, it is clear how issuing end users with Consent Receipts, adequately certified by a Scheme Operator, for each digital service developed by a Service Provider using personal data collected by Attribute Providers, gives them a trusted tool to clearly understand how their data are used and to control how they are eventually shared. The same tool allows also to easily revoking access to such data with possibility to backward notify all the third parties accessing the same data, thus guaranteeing *the right for erasure*.

To ensure use of such trust tool, some additional elements are requested to create the Trust Framework encapsulated in the "Scheme" overarching the personal data sharing and operationalized by the certified Scheme Operators. Figure 6.3 shows the elements of the so defined Open Consent Framework [38].

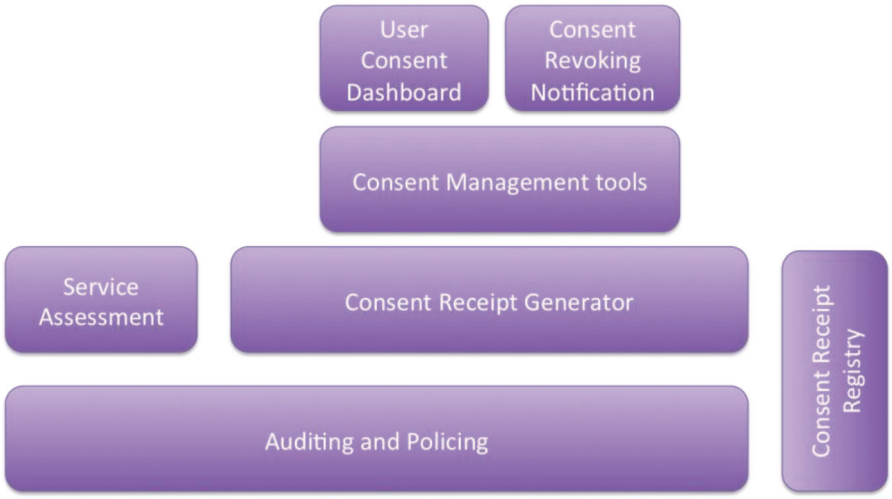

Figure 6.3 Open consent framework.

First of all, certified authorities perform a Service Assessment of Relying Parties that develop services using personal data, in order to provide a *data protection impact assessment* and to collect the information required to pre-fill the Consent Receipt fields, specifying what data and how they are collected, used and shared according to stated privacy policies. The result of such assessment is used to pre-configure a Consent Receipt Generator, the access to which is provided to the given Relying Party as Service (Consent Receipt As A Service, CRaaS). Unique Consent Receipt IDs, useful for auditing purposes, are created by the Scheme Operator and assigned to each generated receipt. Along with the Consent Receipt ID, the remaining Consent Receipt fields are filled at run time.

A first implementation and the related open APIs of a Consent Receipt Generator can be found at: http://api.consentreceipt.org. For easiness of management a JSON Web Token conversion of a Consent Receipt generated by the Consent Receipt Generator is returned.

With this minimum set of services in place, third parties can develop Auditing and Policing functionalities (e.g., similar to EuroPriSe [39] is doing for website) aiming to verify that data are processed and used by Relying Parties according to what stated in the given Consent Receipt. The result of such auditing can enforce policing actions towards organization failing to comply with the agreed principles and to build a Consent Receipt Registry providing a transparent Kitemark [40] of *compliant organizations*. This will

allow end-users to monitor *reputation* of the organizations they give consent to access to their own data.

On the other end, a set of end-users facing tools allow, among others, individuals to manage consent, collect and group receipts, as well as visualize and track shared personal data, through a *User Consent Dashboard* [41]. Currently more UX research is undergoing in order to understand, from an end-user perspective, how to better visualize in the Consent Receipt and associated Dashboard information about the type of data collected and how they are used. The British Standard Institute (BSI) and Digital Catapult are currently developing a new Publicly Available Specification (PAS) [42] defining a number of icons providing such information, using traffic light colour codes similar to those used to classify food composition [43].

To support Consent revocation, achieved by handing over a given receipt to the Relying Party providing the subscribed service, and to notify involved third parties to remove collected data, an additional set of Consent Revoking Notification tools need to be developed.

By achieving end users trust through the above presented Open Consent Framework, the Personal Data Sharing of IoT Services ecosystem (Figure 6.4)

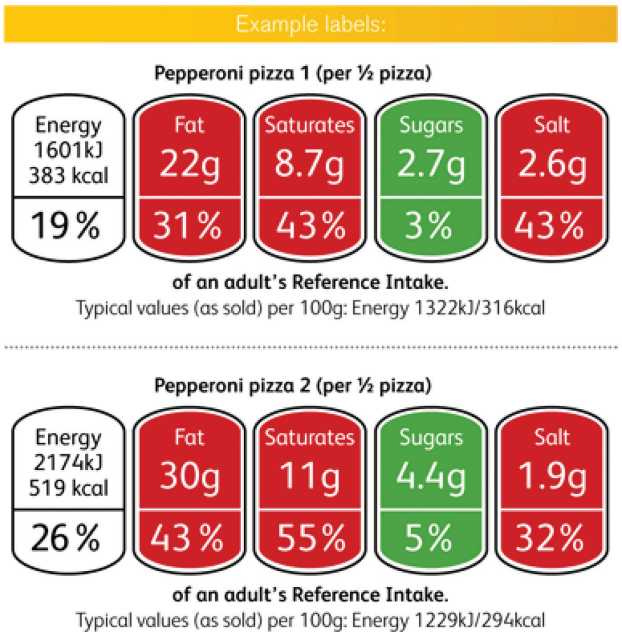

Figure 6.4 Example of food labels inspiring the data labels.

can be further grown with the future development and deployment of Customer Digital Agent (CDA), e.g., organizations, autonomous agents, robo advisors, or ultimately blockchain-based smart contracts (https://www.ethereum.org) that offer and manage service subscription requests on behalf of end-users and based on context and on user preferences as learned by previously accepted services and their issued receipts. This will open up potential for a new personal data market for IoT services, where data are shared with individual trust.

6.7 Using Trust in Authorization

The IoT Access control system can implement a Trust Model in order to enable secure and reliable interactions between granted and trustworthy entities. This mechanism can be deployed on IoT scenarios where smart objects can maintain social relationships, composing different kinds of groups of entities called "bubbles" (e.g. Personal, Family, Office or Community). According to Figure 6.5, each bubble is made up of a set of smart objects, along with an Authorization Manager, which is responsible for generating authorization credentials for smart objects. Furthermore, each smart object have a Trust Manager, which is in charge of assessing the trustworthiness of the other involved entities [23].

The main entities involved in the trust-based access control process are the following:

- **Smart object**. It is a device (e.g. a smartphone, printer, camera, sensor, etc.) that can act both as a CoAP client and a CoAP server offering services (e.g. temperature, location, etc.) in an IoT environment.

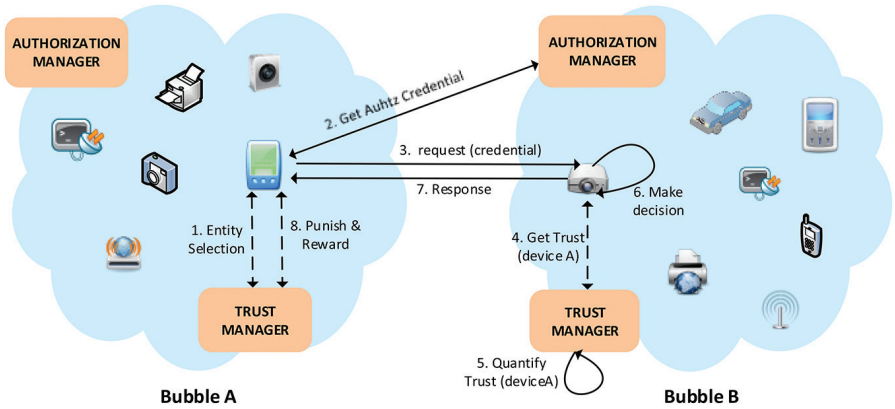

Figure 6.5 Sample scenario for Trust-based authorization in IoT.

- **Trust Manager**. It is the component implementing the proposed trust model. In the case of a smart object with tight resource constraints (i.e., class 0 or class 1 device), the Trust Manager is deployed as separate network element, such as a gateway. In the case of more powerful smart objects (at least class 2 devices), the Trust Manager is a part of the devices.
- **Authorization Manager**. It is responsible for generating and sending authorization tokens to smart objects. Additionally, it is composed of two subcomponents; the Policy Decision Point (PDP), which is in charge of making authorization decisions based on a XACML engine, and the Token Manager, which generates authorization credentials according to the authorization decisions.

In a trust-aware access control system, an **intra-bubble** communication happens when a smart object attempts to access another smart object that is part of the same bubble. Figure 6.5 shows the interactions at high level in the case of an **inter-bubble** communication between smart objects from different bubbles. Under this scenario, the purpose of the Trust Manager (TM) is twofold. On the one hand, it is used by the **requester** smart object to know the most trustworthy target among a set of devices providing the same service. On the other hand, it is employed by the **target** smart object in order to get the trust value associated with the requester under a specific transaction. This value is used, along with the authorization credential that is previously obtained from the Authorization Manager, in order to make the access control decision.

The process carried out during the trust-based access control, depicted in Figure 6.5, is summarized as follows. Firstly, the smart object A accesses its TM in order to know the most trustworthy smart object providing a specific resource in bubble B. The TM calculates the trust of the set of available devices in bubble B (a prior discovery of devices is assumed). Then, in step 2 device A obtains an authorization token for accessing to devices in B. The decision is made based on XACML policies evaluated by the policy engine. This stage is optional and it is supposed to be done not so often, as tokens are reusable. Afterwards, in step 3, the subject smart object A uses the authorization credential (authz token) for access to a service/resource being hosted on the target smart object B. The target acts as PEP (Policy Enforcement Point) that enforces the authorization rights defined in the token, taking into account as well actual context conditions. During this interaction the target device also considers the trust value associated to the requester device (i.e. smart object A). To this aim, it contacts its TM in bubble B, which quantifies in real time the trust based on previous evidences within A as well as actual conditions.

Then, in step 6, device B verifies that the obtained trust value is greater than a threshold value, which was specified as a condition in the token. If that condition is fulfilled, the request is accepted and the service is provided to the smart object A. Finally, in steps 7 and 8 (reward stage), the smart object A sends to its TM evidences feedback about the reliability of the interaction, in order to update the trust value associated to the smart object B, which is useful for future interactions.

6.8 Using Trust in an Indoor Positioning Solution

Smart buildings are comprised of devices integrated into the Internet infrastructure with network and processing abilities, which make them vulnerable to attacks and abuse. The associated services and resources can be accessed through mobile devices anytime and anywhere by common users, which may interact each other according to their levels of trust and reputation. In the smart buildings context, location-aware mechanisms for trust evaluation, can allow a user located at a certain room to share his data only with users located in his same location. In this way, a specific level of trust can be automatically established among people located in the same room, because all of them can be seen as belonging to the same ecosystem [44].

The effectiveness of location-aware security mechanisms is closely related to the accuracy of the location information and the definition of security zones, that is, the area where security aspects like access control, trust, reputation, etc. may be established. However, in the context of smart buildings, how this location information is obtained is a challenging task since traditional mechanisms such as GPS are not useful. The indoor localization mechanism for smart buildings is able to provide accurate location data to be included in security aspects of smart services. The proposed system is based on the use of sensors which are integrated in common smartphones built-in magnetic sensors to make security mechanisms totally independent on the type of devices and available signals in buildings. The sensed magnetic field is a combination of the effects of the Earth's magnetic field and that of surrounding objects. A methodological approach is used to generate the buildings maps containing the magnetic field distribution used as map of fingerprints. Then, based on such maps, location estimations are calculated using a combination of Radial Basis Functions Networks and Particles Filters [45].

The Access Control system can rely on the Indoor location enabler to make authorization decisions accordingly. In this way, devices can ask this service in order to get the distance where a requester user is placed when trying to

access to their services; consequently, certain services can be only provided when users are placed inside the authorization zone of some smart objects. Figure 6.6 below depicts the proposed scenario to perform location-aware access control in indoor environments. The smartphone, acting as a subject, requests to get access a resource being provided by the target smart device. Before allowing it to access to his resource, the target device evaluates both the capability token as well as the subject's position, which must be located inside target's security zone. The context that determines the smart object B position comes from the indoor localization enabler.

Firstly, the use case requires an offline stage where the smartphone of user A contacts with the Authorization Manager in order to get an authorization credential to get access to smart objects. Notice that this phase requires the authentication process. Once the subject is successfully authenticated, the Authorization Manager evaluates the policies and generates (if allowed) a token with the set of privileges associated to the smart object. Then, the subject device wants to make use of a resource hosted by target device, and it uses the obtained token to present it against the target, which validates the token, see it the quantified trust value is over a threshold, and checks subject's position against a localization service, since only those devices located nearby are allowed to get access.

6.9 Using Trust in Routing

A different scenario for the application of trust management in IoT systems is related to improving the security, the privacy and the performance of a network of IoT devices. Assume that there is an IoT deployment with a

Figure 6.6 Location-aware access control for indoor environments.

large number of IoT devices that are forming a multi-hop sensor network. In such a network, the information from the leaf devices or any device has to pass through a number of intermediate devices before it reaches the gateway that will forward the measurements to the backbone middleware and the applications. If there are intermediate devices that are either tampered with, malicious or faulty, this may result to loss of information or to the provision of faulty/tampered information. Moreover, malicious devices may be able to get access to sensitive user information that is passed through them.

To avoid such scenarios, the evaluation of the trustworthiness of the devices can be used in the routing mechanism of the network, so that malicious or malfunctioning devices will be quickly identified and sensitive information to be passed only through trustworthy devices. As described in [27], the reputation evaluation of a network of IoT devices can be done very easily. Assuming that the devices are able to monitor the transmissions of their neighbours, the trust evaluation system can identify very quickly which devices are providing erroneous information. The main idea is that before the start of the trust evaluation all devices have a trust-rating of "unknown", which is then changed as the devices start to exchange data and observing the behaviour of their neighbour devices. Generally, the rules that can be applied are that the trust-belief for a device (i.e. how much we trust a device) should increase slowly, in order to be sure after many interactions that the device is trusted, but it should decrease faster, so that malicious or suspicious devices should be avoided.

When the reputations of the devices have been calculated, then these have to be included in the definition of the routing metric, to ensure that the nodes will be able to identify the routes to the gateway by avoiding suspicious or malicious devices. As shown in [46], including the device reputation in the routing mechanism can significantly improve the performance of the IoT network in terms of improved packet delivery ratio and throughput. This is justified because by avoiding malicious nodes, the percentage of packet losses or packet integrity fails will be minimized.

6.10 Conclusions

The IoT requires new adapted trust models able to overcome the drawbacks of traditional complex models that have not been tailored for the pervasive nature of such global ecosystem. The IoT trust management aims to improve the reliability and trustworthiness in IoT scenarios where disparate and unknown devices interact with each other. It is known that trust is closely inter-related

with security and privacy. However, the inter-relationship is not purely bi-directional. If an entity is neither secure nor privacy preserving, then it should not be trusted. On the contrary, if an entity is secure and privacy preserving, this does not necessarily make it trustworthy for all users.

In this sense, this chapter has shown a trust model that follows a multidimensional approach to calculate the overall trustworthiness of an IoT device. It defines different criteria for the evaluation of the trustworthiness, such as communication, security, data-based criteria, social relationships, and reputation.

Moreover, the trust model provides means for detecting malfunctioning devices by checking if the provided values are inside a static range of values. To this aim, it relies on a rule based approach and fuzzy logic techniques for assessing the trustworthiness, which considers the plausibly, that is, whether the devices are generating correct values.

In addition, this chapter has shown the way the IoT trust management can leverage the access control by making authorization decisions based on quantified trust values as well as indoor localization context. In this sense, magnetic field techniques have shown its feasibility for providing accurate indoor localization positions with the aim of helping to make reliable authorization decisions.

Acknowledgment

This work is partially funded by the EU FP7 projects RERUM (GA no 609094), SOCIOTAL (GA no 609112) and UNIFY-IoT (GA no 688369).

Bibliography

[1] D. Evans. *The internet of things. How the Next Evolution of the Internet is Changing Everything*, Whitepaper, Cisco Internet Business Solutions Group (IBSG) 2011.

[2] A. Zanella, et al. Internet of things for smart cities. *Internet of Things Journal*, IEEE 1.1 (2014): 22–32.

[3] L. Gurgen, et al. Self-aware cyber-physical systems and applications in smart buildings and cities. *Proceedings of the Conference on Design, Automation and Test in Europe*. EDA Consortium, 2013.

[4] M. Weiser. *The computer for the 21st century*. Scientific american 265.3 (1991): 94–104.

[5] N. Petroulakis, et al. A lightweight framework for secure life-logging in smart environments. *Information Security Technical Report* 17.3 (2013): 58–70.

[6] E. Z. Tragos. et al. Enabling reliable and secure IoT-based smart city applications. *Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops* (PERCOM Workshops), 2014.

[7] H. C. Pohls, et al. RERUM: Building a reliable IoT upon privacy- and security-enabled smart objects. *Wireless Communications and Networking Conference Workshops* (WCNCW), 2014 IEEE. IEEE, 2014.

[8] O. Vermesan, and P. Friess (Eds). *Internet of Things-From research and innovation to Market Deployment.* River Publishers, 2014.

[9] O. Vermesan, and P. Friess (Eds). *Building the Hyperconnected Society: IoT Research and Innovation Value Chains, Ecosystems and Markets*, River Publishers, 2015.

[10] M. Ion, A. Danzi, H. Koshutanski, L. Telesca, A peer-to-peer multidimensional trust model for digital ecosystems, 2nd IEEE International Conference on Digital Ecosystems and Technologies, vol., no., pp. 461, 469, 26–29 Feb. 2008.

[11] G. Baldini, et. al., IoT Governance, Privacy and Security Issues, IERC whitepaper, 2015.

[12] N. Gruschka, D. Gessner (eds), Concepts and Solutions for Privacy and Security in the Resolution Infrastructure, IoT-A Deliverable D4.2, February 2012.

[13] Z. Yan, P. Zhang, and A. Vasilakos. A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, (42):120. March 2014.

[14] E. Z. Tragos, and V. Angelakis. Cognitive radio inspired m2m communications. Proceedings of 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), IEEE, 2013.

[15] S. Marti, H. Garcia-Molina, Taxonomy of trust: categorizing P2P reputation systems, *Computer Networks* 50 (4) pp. 472–484. Elsevier Science. Available via http://zoo.cs.yale.edu/classes/cs457/fall13/TaxonomyOfTrust.pdf. 2006

[16] D. Ruiz (Ed) et. al., Modelling the trustworthiness of the IoT, RERUM Deliverable D3.3, April 2016.

[17] RERUM, Reliable Resilient and Secure IoT for smart city applications, www.ict-rerum.eu.

[18] SOCIOTAL, Creating a socially aware and citizen-centric Internet of Things, www.sociotal.eu

[19] G. Zacharia, A. Moukas, and P. Maes. Collaborative reputation mechanisms for electronic marketplaces, *Decision Support Systems* 29.4 (2000): 371–388.

[20] J. D. Work, A. Blue, and R. Hoffman. Method and system for reputation evaluation of online users in a social networking scheme. U.S. Patent No. 8,010,460. 30 Aug. 2011.

[21] Z. Malik, and A. Bouguettaya. Reputation bootstrapping for trust establishment among web services. *Internet Computing*, IEEE 13.1 (2009): 40–47.

[22] A. P. Dempster, The Dempster-Shafer calculus for statisticians. *International Journal of Approximate Reasoning* 48.2 (2008): 365–377.

[23] P. N. Karamolegkos, et al. User-profile based communities assessment using clustering methods. Proceedings of 18th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC IEEE, 2007.

[24] J. B. Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez. TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Computing* (2015): 1–17.

[25] S. Biswas, and R. Morris. ExOR: opportunistic multi-hop routing for wireless networks. *ACM SIGCOMM Computer Communication Review*. Vol. 35. No. 4. ACM, 2005.

[26] T. Zahariadis, et al. Trust management in wireless sensor networks. *European Transactions on Telecommunications* 21.4. pp. 386–395. 2010.

[27] E. Tragos (Ed) et. al., Introducing CR elements into smart objects towards enhanced interconnectivity for Smart City applications, RERUM Deliverable D4.1, March 2015.

[28] M. Gupta, J. Gao, C. Aggarwal, and J. Han. Outlier detection for temporal data. *Synthesis Lectures on Data Mining and Knowledge Discovery*, Vol. 5, No. 1, pp. 1–129. March 2014.

[29] CLIPS Reference Manual. CLIPS Basic Programming Guide version 6.30. (http://clipsrules.sourceforge.net/documentation/v630/bpg.pdf). last accessed: March 17th 2015.

[30] https://www.idc.com/getdoc.jsp?containerId=prUS40846515

[31] https://en.wikipedia.org/wiki/Freemium

[32] http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf

[33] https://script-ed.org/article/share-and-share-alike-an-examination-of-trust-anonymisation-and-data-sharing-with-particular-reference-to-an-exploratory-research-project-investigating-attitudes-to-sharing-personal-data-with-the-pu/
[34] http://ec.europa.eu/justice/data-protection/
[35] https://kantarainitiative.org/confluence/display/infosharing/Home
[36] https://github.com/KantaraInitiative/CISWG/blob/master/MVCR-Spec/MVCR-v0.8/MVCR%20v0.7.9.md
[37] https://en.wikipedia.org/wiki/Personally_identifiable_information
[38] http://smartspecies.com/open-consent-framework/
[39] https://www.european-privacy-seal.eu/EPS-en/Home
[40] https://en.wikipedia.org/wiki/Kitemark
[41] https://eu-smartcities.eu/sites/all/files/Addressing%20Privacy%20in%20Smart%20Cities%20-%20Chris%20Cooper%20-%20Consentua%20API.pdf
[42] http://shop.bsigroup.com/navigate-by/pas/
[43] https://iapp.org/news/a/europes-privacy-seal-schemes-gradually-taking-shape/
[44] M. Moreno, and A. F. Skarmeta. An indoor localization system based on 3D magnetic fingerprints for smart buildings. *Proceedings of International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for the Future* (RIVF), RIVF IEEE, 2015.
[45] M. Nati, et. al., Device centric enablers for privacy and trust, SOCIOTAL Deliverable D3.1.2, February 2015.
[46] E. Tragos, et. el., Improving the Trustworthiness of Ambient Assisted Living Applications, *Proceedings. Of WPMC* 2015, Hyderabad, India, 13–16 December 2015.