10.1 Introduction

Throughout the world and particularly in Europe, the average life expectancy of the population has dramatically increased in the last few decades [1]. European citizens are now living longer than ever before. According to the European Commission, it is expected that the percentage of older adults (65+ years old) will increase from 18% to 28% of the European Union (EU) population by the year 2060 [2]. This will indeed have a strong impact on the health and social care systems, as nations must find efficient ways to provide services to an increasing population of older people. The latter can be realized with the exploitation of new information and communication technologies (ICTs) such as the Internet of things (IoT).

The IoT has emerged over the last decade as a promising set of enabling technologies that will support the concept of the hyperconnected society. In our future, we now expect that everything around humans will be connected to the Internet, forming an enormous global network of digital, virtual, physical, and cyberobjects, with the goal of improving the peoples’ quality of life [3,4]. IoT is providing unprecedented opportunities for businesses to improve their products and develop new “smarter” products and services in

10.1  Introduction........................................................................................................................ 191
10.2  Security, privacy, and trust issues in IoT-based AAL scenarios ........................................ 193
  10.2.1  Overview and methodology .................................................................................. 193
  10.2.2  Risk sources ........................................................................................................... 194
  10.2.3  Elements to be protected....................................................................................... 194
  10.2.4  Attacks against AAL elements ............................................................................. 196
  10.2.5  Assessment of the identified risks ....................................................................... 198
10.3  Decentralized trust management for robust and secure AAL scenarios using blockchains ................................................................. 199
10.4  Blockchain and smart contracts for AAL scenarios in smart building management ... 202
10.5  Trust challenges in AAL systems: Testimonials from EU projects ................................ 203
  10.5.1  ACTIVAGE ............................................................................................................... 203
  10.5.2  SOrBet: Smart objects for intelligent building management........................... 204
10.6  Conclusions and recommendations ................................................................................ 205
Acknowledgment ......................................................................................................................... 206
References ..................................................................................................................................... 206
domains such as manufacturing, environment, agriculture, maritime, food, city services, home automation, and health [5]. The foundations of an IoT system are the physical devices that are either sensors, spread around an area gathering information about physical entities (such as the environment, the air, the users, the doors, and any other real-world objects), or actuators that are controlling physical entities with actions (such as closing a window, switching on the radiator, raising alarms, and moving objects). One main objective of IoT is to interconnect billions of devices in an efficient, scalable, and secure way so that they are able to provide the requested services with the highest quality of service [3,4].

Until recently, IoT systems were only providing sensing services, while the actuation was mostly performed with manual interaction from the users. However, lately, there are many attempts toward automating the actuation procedures, giving the devices the ability to learn and act themselves in an autonomous way. Despite the many benefits that automation provides, it also raises significant concerns with respect to the security and safety of those systems, especially in applications that directly involve human users [6].

The term ambient assisted living (AAL) has been extensively used lately with various similar (but many times ambiguous) meanings. Here, we adopt the definition given by IGI Global with regard to independent living: “It’s a relatively new ICT trend to embed intelligent objects in the environment to support people (mostly elderly) in living independently and monitored” [7]. AAL applications can be considered as an integration of e-health and home automation applications, with the goal of supporting the independent everyday life of disabled people, patients, and the elderly. AAL applications support the execution of advanced user services for monitoring the health and vital signs of a user. They incorporate various sensors for temperature and air quality, and possibly cameras. Wearable on-body sensors can be integrated with various sensors in the surroundings of the user to monitor the ambience, the air quality, the room, and the appliances that are in the same area as the user. Moreover, actuators can be used for assisting users to open doors, set the temperature of the room, open windows for better air ventilation, inform the user to take their medication, move objects to avoid obstructing the movement of the user, and other similar activities [8,9].

Consequently, it is evident that AAL applications can greatly benefit from IoT technologies since they are the enabling technologies that support the gathering, analysis, and exploitation of measurements from the devices. They also allow the execution of smart applications for acting upon the physical environment using the actuators. The fact that IoT merges the digital with the physical worlds, allowing remote control of physical entities, raises concerns with respect to the safety of such AAL applications. Additionally, the fact that AAL applications may gather sensitive user information in centralized servers raises concerns for the privacy of the users of such systems, especially now with the effect of the EU General Data Protection Regulation (GDPR) [16].

We will now present a basic example as the basis of the discussions of the rest of the chapter. We will refer to this as the Basic_example. Following the concept described by Neisse et al. [10], AAL systems need to have strong security and trust systems, which should also be at the same time dynamic and adaptive to the context of the situations. Imagine a situation when an AAL system is installed in a household, restricting access to the front door only to inhabitants. When there is an emergency at home, with an inhabitant having a heart attack not being able to react, the AAL system will be able to correctly identify the situation (using the trust mechanisms to ensure the reliability of the data of various sensors that indicate the emergency). Then, since the context of the home situation will be changed to “health emergency,” the access policies for the front door can change so that the police and the doctors or the nurses (with the necessary identification that the trust manager can use to identify that they are indeed members of the emergency response teams) will be
allowed to enter, while otherwise, they would not be able to get in the house and help
the user. This example shows the importance of trust in AAL systems, because all actions
have to be certified that they are “trusted.” In this scenario, an unknown user will not be
allowed access since he/she is not considered as trusted. Similarly, when the situation is not
an emergency, the police and the doctors will not be allowed to enter the house, even if they
are trusted users. Nevertheless, for an AAL system to maintain its high levels of security
and trustworthiness, it has to be first protected against a number of risks and attacks [11].

In this chapter, we analyze the risks of IoT-based AAL applications, focusing on the
elements that need to be protected, the types of attacks that can be launched by malicious
attackers, and how such attacks may be mitigated. Additionally, a proposal for a distrib-
uted framework for improving the trustworthiness of IoT-based AAL systems using block-
chain technology is presented.

10.2 Security, privacy, and trust issues in IoT-based AAL scenarios

10.2.1 Overview and methodology

AAL applications using IoT technologies are becoming mainstream lately due to the
inherent advantages they can provide for remotely monitoring the health of patients in
prehospital or posthospital scenarios. However, as with all systems that are based on
information technologies, the AAL applications do not come without security, privacy and
trust issues, and threats. AAL applications are vulnerable to many threats and attacks
that can be potentially very harmful for the end users. For example, malfunctioning or
hacked patient-monitoring devices may not be able to signal alarms for the health of the
patient or may disclose false information to the doctors. Since AAL applications are criti-
cal applications that have immediate impact on the health of humans, they must be care-
fully designed, tested, and evaluated through a rigorous process. Additionally, IoT-based
AAL applications must be protected against a number of IoT-originating attacks, and they
have to follow the recommendations of well-acknowledged projects and initiatives (i.e., IoT
European Research Cluster [12], IoT architecture (IoT-A) [13], RERUM [14]).

In this section, we present an overview of the security, privacy, and trust issues in
IoT-based AAL scenarios, building on a thorough vulnerability analysis of AAL applica-
tions. It is not the goal of the chapter to analyze the vulnerabilities of specific commercial
products; thus, the analysis here will be more generic, aiming to provide an overview of
the threats and assets of AAL applications.

The first step toward a vulnerability and threat analysis is to identify which approach
will be followed. The most commonly used approaches are analyses for confidentiality,
integrity, and availability and authentication, authorization, and accounting (CIA/AAA)
or the STRIDE/DREAD analysis that originated from Microsoft. In this chapter, we will
follow the STRIDE/DREAD methodology [15] as it was adapted for IoT by the IoT-A project [13]
in combination with the methodology used in RERUM [16].

The STRIDE methodology splits the threats into six major categories: (i) spoofing iden-
tity, (ii) tampering with data, (iii) repudiation, (iv) information disclosure, (v) denial of
service, and (vi) elevation of privilege. After the analysis of the threats, the assessment of
the risks is usually done, following the DREAD methodology, which helps evaluate the
criticality of an identified threat. Each risk/threat is evaluated against (i) damage potential,
(ii) reproducibility, (iii) exploitability, (iv) affected users, and (v) discoverability. For the
DREAD methodology, usually, each risk/threat is being rated against the preceding five
metrics, and the ratings can be either numbers (1–5) or low, medium, and high [15].
10.2.2 Risk sources

To conduct a threat analysis, the identification of the risk sources and the assets or elements that should be protected is the mandatory initial step. In IoT-based AAL scenarios, the risk sources for potential attacks or threats in the system can be originating from either humans or other phenomena. Human-based threats can be either malicious or due to faults, but from a security point of view, what matters is the result of the attacks on the AAL applications and users. Human-originated risk sources can be related to stealing information, hacking devices, or identities device loss, accidents, and errors. Nonhuman risk sources can be related to natural phenomena such as lightning, fire, heat, or device failures [15,16].

In AAL applications, human-based threats can be related to attackers that want to take control of AAL platforms, sensing devices, and communication channels. Malicious users may be stealing information regarding the health status of the patients that are being monitored, intercepting the measurements and identifying when the user is at home or is absent. This information can be stolen in multiple ways, such as monitoring the wireless channel and intercepting packets that are being transmitted, hacking applications, and accessing databases or hacking devices themselves.

A critical issue in AAL scenarios is also the potential of attackers to access actuator devices that are used for acting on the physical environment, simplifying the everyday activities of the elderly. This means that using some specific rules, doors and windows can open automatically (when the user is nearby), the air-conditioning will set the correct temperature by combining information for the outdoor temperature and the user preferences, and the alarms will notify the user when he/she has some health condition and should take a pill (for example, in low blood sugar or in high blood pressure). It is evident that malicious users that take control of such devices can create harmful effects on the human health.

Nonhuman threats can also have harmful effects on AAL applications, since they can affect the measurements and decisions of the overall system. For example, heat or fire can affect the measurements of health sensors and water and humidity can cause device malfunction, which in turn can affect the integrity of the measurements. Malfunctioning or hacked devices sending false measurements with respect to the health status of the users can decrease the reliability of the overall AAL platform, which in turn lowers the trust that humans put on the system.

10.2.3 Elements to be protected

In AAL scenarios, the elements to be protected via ICTs can be split into several categories and are a mixture between the physical and the digital world. Of course, the most important element is the human user, who is the end user of the AAL system that either monitors the user’s health status or acts using actuators to provide everyday assistance. In the Basic_Example, the human user is the inhabitant of the house who is in either a critical or a normal state. Tampering with sensors or actuators can have devastating effects for the human, because sending false information and commands on an insecure system results in bad system decisions. In the Basic_Example, when the user is in a critical state, an attacker may stop the system from sending alarm to the ambulance or reject access to the house to the emergency teams. These attack scenarios are mainly considered as “safety” and not security, and there is a research domain that tackles functional safety and tries to identify solutions so that IoT or cyberphysical systems ensure the safety of the
With the upcoming implementation of the EU GDPR [17], AAL systems and applications will have to comply with very strict privacy requirements, with respect to data gathering and processing. GDPR requires that the user’s privacy has to be protected at the highest level. Users have to be informed about the type of data that are gathered and how these are processed and stored. All private user information, such as health status, phone number, name, social security number, and credit card number, have to be protected from unauthorized access, and the user should have full control over their usage.

The second physical element that has to be protected is the IoT devices that are sensors, actuators, or even gateways. In the Basic Example, these devices can be the actuator controlling the door, a motion sensor to identify the user movement, or a wearable measuring the blood pressure or the pulse of the user. These devices are mainly the generators of AAL data and can include any type of sensors such as on-body sensors, ambient conditions sensors (temperature, humidity, and light levels), and air quality sensors that may affect the user (gases and dust). Gateways have to be protected too, since they are critical parts of the IoT network, gathering all data from the end sensors and sending them to the backbone servers and applications. Getting access to those devices will open up a Pandora’s box for an AAL system. These devices are ICT devices, and their software, firmware, and applications and their communication with other devices or gateways have to be protected.

Another element to be protected are various types of data that can be application (sensing) data, actuation commands, or signaling data (for example, networking measurements for routing or channel assignment). Examples of data that have to be protected are user’s heartbeat, blood pressure, temperature, blood sugar levels, status (walking, standing, and laying down), location, room conditions, air pollution, door/window status (open/closed), actuator’s state, and actuator request and response.

Device and server software also has to be protected against tampering and hacking. This includes the operating system, the firmware, the drivers for the sensors/actuators, the implementation of the network stack, and any services that are running on devices or gateways. The software also includes AAL services and applications, such as end user applications (rule based for executing control loops as well as home automation), data collection, service discovery and lookup, identity management, as well as trust and reputation.

Authentication credentials and user policies are also critical for the secure operation of an AAL system. Credentials and policies are used by security and privacy mechanisms to identify users and grant them access to the AAL system. False or altered credentials and policies may provide access to malicious users, who can steal personal user information or send malicious commands to actuators. In the Basic Example, the home user has the role of the owner and manager of the system and has access to everything. The AAL system should also have a role for the emergency response teams, which should be able to grant access to the front door “only in emergency situations.” To be able to distinguish emergency response members, the AAL system, when sending an alarm to the emergency response teams, could also send an access code for the front door. In this respect, different response teams could also have different codes, which change dynamically.

The wireless channel in the IoT network has to be protected against a number of attacks, because common threats can affect the integrity and the confidentiality of the data. Eavesdroppers can monitor the wireless channel and intercept messages; masquerading attacks can allow the attacker to get access to sensitive information, and authentication; credentials and intermediate malicious nodes can alter measurements and actuation commands, i.e., opening doors and setting offalarms.

Finally, since IoT systems can have an impact on the physical environment, the actual physical entities, such as the house and the furniture have to be protected from the actions
of the actuators. Toward this, examples of malicious commands to actuators for, e.g., flooding the apartment (in case of a false fire event) or overheating appliances and causing explosions, have to be avoided.

### 10.2.4 Attacks against AAL elements

The STRIDE analysis can be used to identify potential attacks against elements that need to be protected in an AAL system (see also Table 10.1). For the human user in the Basic Example (discussed in the introduction), attackers tampering with the monitored user’s data can alter them, sending false measurements to the AAL system, so that emergencies are not identified or false health status is noticed and wrong medical treatment is provided. Falsifying the user’s health data can have devastating effects on the safety of a user, which is of utmost importance for AAL systems. Similar results can take place when there is a denial of service attack on an AAL system, so that services that are critical for the user’s safety are disabled.

Attacking IoT devices is relatively easy because most of the current commercial products have very limited on-board security features. Especially due to the fact that these devices are lightweight, they can be an easy target for hacking, blocking, or altering their communication, changing their configuration, or sending them false commands. Apart from that, physical attacks such as destruction, theft, or reprogramming/controlling the devices through their universal serial bus interfaces are usual types of attacks [18]. Masquerading attacks on devices is also quite common in IoT or wireless sensor networks. In this attack, an attacker plays the role of a “gateway” so that all measurements go to

<table>
<thead>
<tr>
<th>Element to be protected</th>
<th>Attacks</th>
<th>Impact</th>
<th>Mitigation procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human user</td>
<td>Data tampering, repudiation, and user safety</td>
<td>User’s health and private data</td>
<td>Access control, safety procedures, and user trustworthiness</td>
</tr>
<tr>
<td>IoT devices (sensors, actuators, and gateways)</td>
<td>Denial of service, data manipulation, device hacking, and spoofing identity</td>
<td>Access to sensitive information, access to the IoT system, and sending false information</td>
<td>Encryption, access control, physical protection, and device trustworthiness</td>
</tr>
<tr>
<td>Data</td>
<td>Data tampering and eavesdropping</td>
<td>Unauthorized access to data and breach of privacy</td>
<td>Encryption, integrity protection, and service trustworthiness</td>
</tr>
<tr>
<td>Software</td>
<td>Data tampering, device hacking, and denial of service</td>
<td>Loss of data and no access to services</td>
<td>Encryption, access control, and security management</td>
</tr>
<tr>
<td>Credentials</td>
<td>Elevation of privilege and identity spoofing</td>
<td>Breach of privacy and unauthorized access to the IoT services</td>
<td>Strong access control and identity management</td>
</tr>
<tr>
<td>Wireless channel</td>
<td>Eavesdropping, masquerade attacks, and man-in-the-middle attack</td>
<td>Loss of data, loss of communications, and breach of privacy</td>
<td>Communication encryption, integrity protection, and antijamming</td>
</tr>
</tbody>
</table>
his/her device instead of the proper AAL gateway. These attacks can be quite severe, resulting in the loss of communication so that AAL devices cannot send crucial monitoring data (or send false data) to the AAL application. Moreover, sending false commands to actuators can also have an effect on the physical environment. For example, opening doors/windows to intruders or even closing doors when the user is passing creating physical harm to the user.

Attacks against various types of data are also very common. Especially in an AAL system where measurements from various sensors are mostly sensitive carrying critical health information, attacks, such as tampering with data, false measurements reporting, or denial of service, can raise issues with regard to the trust of the overall system. Loss of the integrity of the data in an AAL system can occur both when the data are at rest (stored on a device) or in transit (when they are exchanged). When at rest, an attacker can modify the data by launching a malicious code on the device or by gaining remote control. When in transit, an attacker can modify the data by attacking the networking infrastructure using a man-in-the-middle attack. Loss of data availability can also take place either at rest or in transit. In the former case, an attacker might delete the data stored on a device, while in the latter case, an attacker can perform radio jamming, denial of service attacks, or sinkhole attacks. Similar attacks can also target command and control data, such as routing or wireless channel assignment data, which can have an effect on the overall performance of the system and the communication between the devices and the applications.

The software of both devices and the backbone servers is also a point of attack in AAL systems. Services and applications for monitoring the health of the users and acting for either assisting them in their everyday activities or notifying their doctors in cases of emergency can be attacked by malicious users so that they gain access to unauthorized data, perform denial of service, change measurements and data in databases, or impersonate services and applications. This will result in hacked user accounts, devices becoming unable to communicate with applications, or users denied access to their own applications.

Loss of confidentiality of credentials and policies can take place when an attacker specifically gets access to the security servers of an AAL system or if he/she spoofs the identity of devices and gains access to the applications. The access to credentials or policies can be achieved by executing malicious code on a gateway/server or at a device or by eavesdropping and performing a man-in-the-middle attack. In the Basic_Example, when an attacker gets credentials and access policies, then he/she can launch more attacks by getting unauthorized access to the servers, applications, and user data, not allowing the alarms to be sent, sending false alarms or even taking control of devices and harming the user with injection of medicines at wrong times.

Most of the preceding attacks take place when an attacker tampers with the communication channel. In most AAL scenarios, the communication channel is wireless, and it is easy for an attacker to perform man-in-the-middle, eavesdropping, or jamming attacks [19]. That way, the attacker can listen to transmissions gaining unauthorized access to data, can perform identity spoofing and pretend to be an authorized device/user or can disrupt the communication by degrading the link quality of the wireless connection between the devices and the gateways. Considering an AAL system in a home, if the communication link is not secured, a neighbor who is listening to the wireless transmissions of the devices will be able to identify the measurements and even pretend to be an authorized user and send commands to the actuators. Moreover, even if the transmissions are encrypted and the attacker is not able to extract the content of the transmissions, just the simple monitoring of the transmissions allows the extraction of information about which devices are operating, when the user is at home, or when there are emergencies.
10.2.5 Assessment of the identified risks

After analyzing what the risks against critical elements of an AAL system are, the important step is to see what the impact of these risks on such a system is and what can be done to mitigate this impact. The attacks against a human user have a high damage potential, cannot be easily reproduced, and can be very exploitable (even with financial gains for the attacker). Moreover, these AAL attacks are mostly targeted per person, so they cannot affect many users and they cannot be discovered very easily. These attacks can be mitigated with a security, privacy, and trust framework that employs strong security with cryptographic protocol, access control, and privacy-enhancing techniques. Such a system is also critical for emergency situations, as the one described in the Basic Example. The main target will be to minimize the possibility for an attacker to gain access to the private information of the user or to send any type of malicious commands to the actuators that can harm the human or his/her surroundings.

Attacks against an IoT device may also cause significant damage, especially if the device has stored private user information or credentials that would provide access to the system to an attacker, if the device is used to gather real-time health-related information or raise alarms for emergency situations. These attacks cannot be easily reproduced or discovered, but can be exploitable by the attacker. They can be sometimes avoided with the physical protection of devices, such as installing the devices in unreachable locations, hiding the devices, or covering them. Additionally, these attacks can be mitigated with secure storage functionalities to prevent an attacker to gain to the filesystem of the device to read the files. Additionally, proper authentication can contribute to avoid device identity spoofing and masquerading. Moreover, software security updates when any vulnerabilities are identified are very critical to ensure the proper protection of the device.

Attacks against data and services normally have high damage potential due to the fact that in AAL systems, the data gathered by the devices are sensitive user health data that can be exploited by malicious attackers for knowing the medical history and possible diseases of the user. These attacks can be easily reproduced when launched at both the devices at the local level and at backbone servers, targeting services and applications. They can be easily discovered when they target services that actively use and transmit user data, but cannot be easily discovered when they are passive and only capture user data. To avoid these types of attacks, proper security management with a strong authentication and authorization framework should exist, together with a trust management framework to identify the trustworthiness of users and the data that are gathered by the devices. Moreover, the encryption of data and secure communications are of high importance to minimize the possibility for an attacker to eavesdrop or to decrypt the data that it gathers from the devices. Additionally, accountability mechanisms should exist so that when such an attack is launched, the system should be able to identify and isolate the attacker. A proper identity management scheme will also provide secure identities to the devices and the components of the system, so that they cannot be replicated or stolen by an attacker to be used for impersonation.

Attacks against communication channels, especially in AAL scenarios where most of the communications are based on wireless links, can have severe effects on the performance of the system, on the privacy of the user data, and on the safety of the system. The attacks can be easily reproduced, regardless of the number of the devices or of the type of wireless links, and they cannot be easily discovered, especially considering the specificities of the eavesdropping attack. An attacker who listens to a wireless channel can only intercept personal data, but cannot affect the system performance or
the trustworthiness of the system. However, wireless jamming can be quite harmful since it affects data availability, which can cause issues such as missed emergencies or actuating commands not received by the devices. These attacks can be mitigated by end-to-end integrity protection on the measurements from the devices, to increase their trustworthiness. Additionally, secure communications with data encryption to avoid eavesdropping and anonymous communications to protect user data can also be used, in combination with privacy-enhanced techniques for improving the privacy of the user data. Antijamming techniques with automatic channel or spectrum reassignment using cognitive radio devices can be used, so that denial of service attacks have minimum to zero effect on the system performance. Finally, authorization mechanisms on the devices can be used to ensure that only authorized users send actuation commands.

Most AAL systems, as also described earlier, are mostly centralized (i.e., Sánchez-Pi and Molina [20]) with all the decision-making processes handled by a central server. However, this creates new threats such as a single point of failure or a single point of attack, which means that if an attacker wants to exploit such a system, he/she can only target to hack or jam this central point. To avoid this, lately, there is a shift toward more decentralized or distributed systems, to allow the devices and gateways to take cooperative decisions and enable the distributed storage of data. This approach increases the scalability, the security, and the trustworthiness of the system, but only when strong and efficient trust management mechanisms are employed. In the following section, such a framework for the decentralized management of AAL systems using the new technology of blockchains is introduced, aiming to set the foundations for improving the trustworthiness of AAL systems.

10.3 Decentralized trust management for robust and secure AAL scenarios using blockchains

Trust management and trust computation (computation of nodes’ trust based on metrics such as average packet drop ratio and forwarding delay) are not trivial issues in an IoT ecosystem for several reasons: (i) the presence of resource-constrained devices, (ii) the lack of standardization, (iii) the presence of heterogeneous devices, (iv) protocol inefficiencies, (v) the lack of interoperability, and (vi) an unattended operating environment. In the special case of the AAL, IoT devices perform several specialized operations such as monitoring, alerting, on-demand data provisioning, and actuating. Moreover, wireless sensors are mainly used in related scenarios as more flexibility is provided [13]. For these reasons, the IoT networks for such scenarios are susceptible to several attacks launched by adversaries with various motives, as also presented in detail in Section 10.2.4. Countermeasures against such attacks can include cryptographic means in several layers (e.g., symmetric-based encryption on advanced encryption standard). However, given the broadcast nature of the wireless medium, countermeasures such as these cannot protect against several types of attacks such as routing attacks (black hole, gray hole, selfish behavior, etc. [21]). For tackling these issues, several trust management and computation schemes have been proposed by the research community. The main idea is that all nodes observe their neighbors by collecting various pieces of information such as the packet drop rate and the packet modification rate [13]. Related research contributions (e.g., Fragkiadakis and Tragos [22]) combine physical-layer measurements such as the signal-to-interference-plus-noise ratio to adjust the reliability of an observation based on the amount of interference when the specific observation takes place. Based on nodes’ observations, a level of trust computation is performed aiming to assign a trust value for each node. In general, trust-based models are classified...
into three categories [22]: (i) **centralized**, where all nodes send their evaluation reports to a single node that has more advanced capabilities (in terms of processing), and performs the fusion of the reports, inferring about a potential attacker; (ii) **distributed**, where each node fuses the individual reports and estimates the reputation of its neighbours; and (iii) **hybrid**, where large portions of the wireless network are split into multiple clusters such that the elected cluster heads are responsible for the fusion. Each model has its pros and cons, and the design choice depends on several factors such as: (i) the network size, (ii) the hardware capabilities of the nodes, and (iii) security mechanisms to be deployed. With centralized schemes, processing can be performed by advanced devices (servers and gateways), but these single points of failure exist that can make the network collapse in case of failures or attacks against these advanced devices. Distributed models assume that all processing regarding the trust management and computation are performed by the nodes exclusively, something that cannot be always feasible considering the resource-constrained nature of IoT nodes (sensors). The hybrid schemes try to compare the benefits of the centralized and distributed ones; however, the consensus algorithms used may not be robust in case of failures or deliberate attacks (e.g., Sybil and Byzantine attacks).

In this section, we investigate the feasibility of trustless distributed schemes in the IoT domain for defending against three types of attacks: (i) black hole routing attack, (ii) gray hole routing attack, and (iii) integrity attack. We will consider the use of the so-called **blockchain**, a distributed data structure replicated and shared among all nodes in a network. The blockchain is used in Bitcoin, the famous cryptocurrency [23], and consists of a series of interrelated blocks as shown in Figure 10.1.

Each block can have several fields, depending on the implementation:

- The previous hash that contains the hash value of the previous block.
- The list of transactions (Transactions []) that will be executed within this block. Usually, this list is organized as a Merkle tree that is a binary tree using hash pointers. A transaction is used to describe a specific type of operation based on a specific asset.
- The nonce that is a one-time random value is used as one of the hash function arguments.
- The hash function H() that receives data of arbitrary length and produces a fixed-size output. For the transactions’ list case, the hash function is used multiple times, depending on the level of the Merkle tree. Initially (Level-0), and for each transaction, a hash value is computed taking as input the body of the transaction. Next, in Level-1, pairs of the hash values are formed, and their concatenated values are used as input to the hash function. This continues to all upper levels, until a single hash value is computed.
- The hash value of the block is computed using the data of the block as input (depending on the implementation). A typical input can include the concatenated values of the nonce, the mrkl_root hash value, and the hash value of the previous block.

![Figure 10.1 Blockchain structure.](image-url)
The blockchain data structure is maintained by all nodes in the network. Its size is proportional to the number of blocks and the number of the transactions for each of the blocks. As this is a distributed system, the nodes are free to generate new transactions and blocks. However, certain rules have be and respected by all nodes; otherwise, chaos will rise:

- Strong cryptographic means are used, and each node that generates a transaction signs it with its private key; therefore, a public key cryptography system is required.
- Nodes forward only valid transactions that belong to other nodes. As each transaction is signed by its owner, it is easy to verify that a specific transaction belongs to a specific node by using its public key.
- Block creation can be potentially performed by any node; however, strict rules can apply on the requirements for building such blocks. When a new block is successfully added into the long-term blockchain, this is broadcasted to all nodes so as to refresh their local copies, and the miner who created this block is rewarded.

The question now is how robust this mechanism is against various types of attackers considering that no central authority exists. Suppose that an attacker (Bob) modifies a transaction created by Alice, while this transaction is on transit. Alice, who is a legitimate user, has properly signed this transaction with her private key. If Bob modifies this transaction, the modified transaction is not valid anymore, as he does not know Alice’s private key, and hence, all other legitimate nodes will discard it. Therefore, the modified transaction will never reach the miners, so there are no chances for it to be included in a successful block. Moreover, by altering a single bit of a transaction, Bob must re-compute all hash values of the Merkle tree that is computationally difficult, with the difficulty increasing with the number of transactions.

In a different attack, Bob tries to drop or discard all packets created by Alice that carry valid transactions. This could happen if Bob acts as an intermediary in a wireless network, and instead of routing Alice’s packets, he drops or discards them. This will not create any problems, given that the number of the legitimate nodes is high enough, so Alice’s transactions can reach the miners as transactions are broadcasted to all users. Similarly, if Bob drops packets that notify about new valid blocks, the broadcast nature of the network guarantees that a fraction of the legitimate nodes will still be able to receive these packets.

In the special case of Bob being a miner, but still acting maliciously, he could manage to create a block in the long-term blockchain that contains an invalid transaction. Again, this attack cannot be finally successful because legitimate users will detect that the specific block contains an invalid transaction, and legitimate miners will continue the mining process based on the last valid block.

Next, we will discuss how the blockchain concept can protect an IoT network against black hole and gray hole routing attacks. Very often, IoT ecosystems are based on wireless sensor networks (WSNs) with many nodes (sensors) to provide data to backbone servers. The network topology can employ multihop links where data are forwarded from the source nodes to the ultimate destination (e.g., server) over multiple links. In this case, other nodes operate as routers by following an appropriate routing protocol (e.g., the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [24]). A malicious user can take advantage of this mechanism and do the following:

- Discard all packets he/she has to forward (black hole attack [21])
- Selectively drop packets based on several criteria such as type of information and data owner (gray hole attack [25])
For detecting these types of attacks, several schemes (e.g., Zahariadis et al. [26] and Liu et al. [27]) have been proposed that attempt to compute a node’s trust based on observations from other nodes. Therefore, a trust management and computation mechanism is required. Referring to the WSN shown in Figure 10.2, a schematic representation of a number of honest nodes (HNs), one adversary (AD), and a sink is displayed. The aim of the adversary is to drop either all or selective packets. To maximize the effect of his/her malicious action, and prior to packet dropping, he/she takes advantage of the routing protocol used and broadcasts an attractive routing metric (e.g., minimum number of hops from the sink and minimum delay) aiming to appear as the ideal neighbor to the rest of the nodes for forwarding their packets. This is usually referred as sinkhole attack [28], and if successful, the adversary can start dropping packets.

We now consider the use of blockchain in such a network. All nodes, based on the data they have to transmit, create transactions and sign them with their public key. All transactions are broadcasted into the network, and the miners (all nodes or a fraction of them) try to create a successful block. Despite the presence of the adversary who is dropping packets, at least one miner will manage to create a block and add it in the long-term blockchain.

If the adversary instead of dropping packets tries to modify their content, this will lead to invalid transactions as he/she is not aware of the public keys of the HNs. The invalid transactions will be rejected by all users, so they will not be included in their blockchain (each user maintains a copy of the blockchain).

10.4 Blockchain and smart contracts for AAL scenarios in smart building management

As described in the previous section, a blockchain, which is an immutable ledger, can be efficiently used to provide a decentralized trustworthy system with nontrusting peers. Along with the blockchain ledger, research groups around the globe work on smart contracts (SCs), which are scripts that are stored in the blockchain and used for multistep process automation [29]. An SC is a “computerized transaction protocol that executes the terms of a contract” and usually describes a list of conditions and the actions to be performed when one or more of such conditions occur. For example, if a user’s device battery drops below a threshold, then do not use it in future blockchain transactions. Specific languages are used for the creation of the SCs, as for, example, the Solidity language used in Ethereum [30].
Next, we describe how SCs and blockchains can be used in smart building management (SBM) for AAL scenarios. SBM systems can provide efficient frameworks for data collection, monitoring, and actuation based on IoT architectures. SOrBet is an IoT architecture designed to securely interconnect smart devices that are equipped with intelligence, able to support AAL scenarios [31]. SOrBet functional architecture (Figure 2 in Tragos et al. [31]) consists of modules such as the service manager, communication manager, event manager, context manager, quality of service (QoS) manager, and security and trust manager. Given this architecture, SCs can be created by the communicating peers in several layers.

SCs are digitally signed and stored in the blockchain, and they execute automatically if certain conditions are met. For example, an SC can bind to the QoS and communication managers, stating that if a packet delay exceeds a threshold, then give priority to the specific flow. For this action, some reward can be defined through the exchange of digital assets (e.g., Ether or Bitcoin).

In another example, if strong privacy is required, then data must be encrypted before storing them to the blockchain. An SC can assign encryption duties to more advanced peers that will encrypt the data of less advanced ones (in terms of processing memory and storage), and they will be rewarded after encryption is completed.

As many AAL applications are heavily based on SBM systems, the use of SCs can in general automate several of their processes, enable the exchange of digital assets, and create a marketplace for the AAL ecosystem.

10.5 Trust challenges in AAL systems: Testimonials from EU projects

AAL applications have also been the focus of many EU research and innovation projects, aiming to improve the functionalities of the systems and the services they can provide to the end users. Since AAL systems also have inherent challenges with respect to security and privacy, most relevant EU projects are also considering components for improving the trustworthiness of AAL in their functional architectures. Since every project has its own objectives, we provide here example testimonials of trust challenges that two EU-funded research projects have identified with respect to their AAL systems and how they addressed these challenges.

10.5.1 ACTIVAGE

One part of the AAL community is the new active and healthy aging (AHA) community, which is wide and heterogeneous in terms of needs, demands, and living environments, which will use IoT-based services to address many of the challenges of everyday living of the elderly. ACTivating InnoVative IoT smart living environments for AGEing well (ACTIVAGE) is a European multicentric large-scale pilot on smart living environments [32], which aims to develop methodologies, while responding to the real needs of caregiver, services providers, and public authorities, to prolong and support the independent living of older adults in their preferred living environments. This will be achieved and validated through the real-world deployment of innovative and user-led large-scale pilots across nine IoT-enabled deployment sites, in seven European countries, involving up to 7000 users.

ACTIVAGE aims to build the first European AHA-IoT ecosystem, which is modeled as a technological infrastructure of hardware and software services and standard protocols and a constellation of stakeholders interacting with each other within a governance
framework toward the achievement of common goals. ACTIVAGE will utilize IoT solutions through nine different use cases that address specific end user needs to improve their quality of life and autonomy. These use cases include daily activity monitoring, integrated care, monitoring assisted persons outside home, emergency triggering, exercise promotion, cognitive stimulation, prevention of social isolation, safety and comfort at home, and support for transportation and mobility.

In the conceptual model for AHA-IoT ecosystem, the components for trust, security, and privacy are core components. Data streams are the core asset of the ecosystem, which belongs to either private or public sources. As in all AAL applications, private data are produced by wearable and medical devices as well as smart sensors and devices in older adults’ living environments. Public data, not necessarily linked to user interactions, are harnessed from public sources, including weather data, public transport timetables, and traffic situations. Both private and public data are processed at the edge and/or at cloud level. These data streams are then passed through different processes, such as anonymization, aggregation, and analysis that aim to increase the security and privacy of the overall system and thus its trustworthiness.

The sources of the ACTIVAGE AAL system introduce many issues related to the security of medical data and the protection of user privacy, which can be separated into several fundamental data management concepts, namely, trustworthiness of data sources, integrity of aggregated data, data privacy, anonymization of the data provider, location privacy, as well as the confidentiality of the network packets. As in many other areas, privacy and security are critical aspects of the general IoT environment, where multiple concerns are constantly being raised and compared to the privacy issues of traditional ICT systems.

ACTIVAGE proposes that AAL systems require inherent security, trustworthiness, and privacy by design. To this end, a modular framework will provide placeholders for incorporating security and privacy preserving algorithms, along with protocols ensuring that only trusted entities (i.e., “things”) can become part of the deployment. The project suggests to investigate the economics of privacy and security in a cloud environment, with a view of associating them with the researched utility metrics of the cloud infrastructure. So privacy and security by design methodology and tools should be used for system design and risk management. The main novelty of ACTIVAGE in this area is the incorporation of utility-based schemes for negotiating and enforcing privacy and security.

10.5.2 SOrBet: Smart objects for intelligent building management

The SOrBet project [33] develops an IoT-enhanced intelligent building management system (BMS) based on the concept of reliability by design, and one of the main application scenarios considered is the provision of AAL applications. SOrBet built its system architecture considering various requirements that should be met to improve the reliability of AAL applications, especially in terms of security, privacy, and trust. SOrBet addresses the issues of security and privacy in AAL environments by considering heterogeneous wireless devices that are communicating in a trustworthy manner to ensure that only trusted devices are involved in the decision-making processes of the system and sensitive user data from the devices are sent only to authorized and trusted end users.

The requirements set by the project for the security, privacy, and trust of AAL systems are considered as key factors to ensure the overall reliability of the system. SOrBet considers that data encryption, strong authentication and access control framework, reputation management, and privacy-enhancing techniques are key requirements to protect AAL applications from attacks. In this respect, the SOrBet project has defined a dedicated functional
entity called “security and trust manager” in its functional architecture (Figure 10.3), which is responsible for (i) secure communications between devices and the system, (ii) the secure configuration of devices, (iii) the access control, and (iv) the trust management of the system.

It can be seen from Figure 10.3 that security and trust components are critical for AAL systems since they should be protecting all components: communications between the various sensors and devices, services that are provided by the system, the virtualization of the components, as well as the automation layer that handles the automated actions of the actuators, according to rules defined using case-based reasoning and business management processes.

It is important to note that as SOrBet proposes, the security and trust actions can be affected by the context of the situation. This can be of great importance to provide important assistance to people in need. In cases of nontrustworthy or insecure systems, a malicious user might be able to send false data to change the context of the system and then gain access to the house by tampering with the door access policies. Another scenario would be when a malicious user blocks the communication of the devices with the AAL application so that they cannot send the data about the emergency scenario and the emergency response teams are not notified about the user’s health, which will have devastating results.

10.6 Conclusions and recommendations

AAL applications for supporting the aging and well-being of human users at their homes have attracted a high interest lately due to the explosion in the usage of IoT technologies. Although technology can greatly help monitor users’ health status at home, it also introduces various risks for the security, privacy, and safety of users. In this chapter, building on the requirements and the testimonials of two EU-funded projects, we analyzed in detail the trustworthiness of AAL systems, focusing on the threats and risks of IoT-based AAL systems and discussing what has to be protected in these systems and how. As a summary of this discussion, we can briefly mention the fact that protecting

Figure 10.3 SOrBet functional architecture. (Reprinted from Tragos, Elias et al., D1.1: System requirements and architecture definition, SOrBet Deliverable D1.1, Dec. 2014.)
users’ safety is the most important goal. In the past, physically harming users using standard computer attacks was not at all possible. However, with the introduction of IoT technologies that allow the remote control of actuators that are controlling physical objects, the convergence of the cyberworld and physical world is creating new threats for the humans. Such safety risks can arise from attacks on various elements of an AAL system, which raises the importance of a strong trust management framework that will be combining strong aspects of security and privacy. Since the centralized control and management of such systems imposes significant security risks, we also discussed the use of blockchains for distributed management.

The use of blockchain can provide solutions to many security- and trust-related aspects of the IoT due to the inherent distributed nature and trust assurance. The blockchain can provide user and device trustworthiness ratings, so that only trusted users/devices are part of the system. Additionally, the decentralized nature of a blockchain-based AAL system will mitigate issues of a single point of failure and overloading. However, this new technology also introduces new issues and risks and has to be carefully adopted. A blockchain-based scheme requires nodes with advanced memory capabilities as the blockchain is replicated and maintained from all nodes. Blockchain is maintained by all nodes, so broadcast messages are transmitted by the nodes. If not carefully designed, packet collisions and network delay will decrease the performance of a network. Furthermore, extensive packet broadcasting can exhaust nodes with limited energy.

Overall, AAL systems are critical systems that are directly affecting the everyday lives of people in need. These systems are handling extremely private user information and should be designed to be reliable, secure, and trusted so that people can be reassured that they are safe to be used.

Acknowledgment

The authors acknowledge support from the ACTIVAGE project, cofunded by the European Union’s Horizon 2020 research and innovation program under grant agreement number 732679. The research leading to these results has also received funding from the People Programme (Marie Curie Actions) of the European Union’s Seventh Framework Programme FP7/2007-2013/under Research Executive Agency (REA) grant agreement number 612361.

References

Chapter ten: Trusted IoT in ambient assisted living scenarios


