Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 16 (2014) 1351 – 1360

Procedia Technology

CENTERIS 2014 - Conference on ENTERprise Information Systems / ProjMAN 2014 - International Conference on Project MANagement / HCIST 2014 - International Conference on Health and Social Care Information Systems and Technologies

Internet of Things and Smart Objects for M-Health Monitoring and Control

Alexandre Santos[a,*], Joaquim Macedo[a], António Costa[a], M. João Nicolau[b]

[a]*Centro ALGORITMI, Dep. Informatics, Eng. School, University of Minho, Campus Gualtar, 4710-057 Braga, Portugal*
[b]*Centro ALGORITMI, Dep. Information Systems, Eng. School, University of Minho, Campus Azurém, 4800-058 Guimarães, Portugal*

Abstract

Internet of Things combined with *Radio Frequency IDentification* technology enable a whole new context for smart objects that are able to combine their physical and virtual existences. *Radio Frequency IDentification*, putting an identification label into every object, enables a smart system to get information, either real-time or virtual-linked information, without any physical contact. Information retrieved from such an object, turns it into a potential smart object, certainly able to auto identify itself and, if security problems are suitably treated, most probably able to connect to the global Internet. This way, one can get an ubiquitous framework to access, monitor and control any of those smart objects over an Internet of connected *things*. RFID tags in medical context enable a rapid and precise identification of each smart entity, enabling a ubiquitous and quick access to Personal Health Records over an Internet of Things. The use of smart phones with Internet access, along with strong security concerns - such as authenticity, privacy, confidentiality, integrity, data origin authentication, entity authentication and non-repudiation - turn this whole context into a decentralized and mobile healthcare system. Using the simple IoT architecture presented, combining smart objects, the security solution and mobile communications, one may remotely take care of patients' well being, establishing an ubiquitous Ambient Assisted Living for Mobile Health applications. As an application example, a prototype m-health service, its security mechanisms and web based application, establish a use case scenario for the evaluation of the proposed architecture.

Peer-review under responsibility of the Organizing Committee of CENTERIS 2014.

Keywords: Internet of Things, RFID, Ambient Assisted Living, M-Health, ONS, PHR;

* Corresponding author. Tel.: +351-253-604474; fax: +351-253-604471.
E-mail address: alex@di.uminho.pt

Peer-review under responsibility of the Organizing Committee of CENTERIS 2014.
doi:10.1016/j.protcy.2014.10.152

1. Introduction

Internet of Things (IoT) [1][2] refers to a recent paradigm that has rapidly gaining ground in the area of modern wireless telecommunications. IoT is then a new technological trend joining new computing and communications paradigms. Within this new trend, there are intelligent devices that have a digital entity and are ubiquitously interconnected on a network and to the global Internet. Everyday objects may integrate intelligence and the ability to sense, interpret and react to their environment, combining the Internet with emerging technologies such as Radio-Frequency Identification (RFID) [3][4], real-time location and embedded sensors. The IoT concept is based on the idea of a universal presence of 'things' or 'objects', such as RFID tags, sensors, actuators, mobile phones, etc, with digital identification and addressing schemes that enable them to cooperate with neighbors in order to achieve some common goals. In the business sector, the most apparent consequences of IoT may arise in industrial automation and manufacturing, in logistics, in business or process management and in intelligent schemes for transporting people and goods.

Therefore, in general, the term Internet of Things refers to any type of devices that are interconnected by means of Machine-to-Machine Communications (M2M), each of which may be identified through a unique ID and defined through a virtual representation within the Internet.

The Radio-Frequency IDentification, commonly known as RFID, is used in many applications. The use of this technology is constantly evolving, expanding at exponential rate. There are several methods of identification, although the most common is a microchip able to store a serial number that identifies the person, object or thing. Using electronic devices that emit radio frequency signals, it is possible to perform an automatic capture of data, or a tag, from a reader. Although it depends on the type of tag, passive or active, RFID is an easy-to-use and versatile acquisition information technology, where a radio signal is used to get data from transponders (e.g. tags) into the target application. Apart from the tags there is also the need for procedures to read or interrogate these tags (e.g. readers, antennas) in order to transmit the data [4] to a host system where it is further processed. The main advantage of using RFID is the possibility of reading without physical contact, being that the production price of tags has been heavily declining over the years. One can put the tag inside a product and read it without unpacking [5] or even implant it under the skin of a patient [6] and read it from outside, even if it is moving.

Whenever we make use of RFID-enabled items, we may face privacy loss [7] as users or items may be identified and linked together by means of tag identification. So, when using this type of technology special security concerns must be brought into place. In health care contexts, these security and privacy concerns are imperative, so any m-health solution must deal with this threat; if personal or private information is to be accessed, all the necessary security mechanisms must be in place, protecting direct data access and or information inference.

The Internet of Things enables to virtually establish links from the information residing in smart objects, for instance in tags, to any Internet connected system. This way, when working in intelligent spaces, we may establish interfaces to connect smart objects to this ”Internet of Things”, thus fostering mobile solutions for Ambient Assisted Living. RFID technologies are of special interest in such scenarios because it does not need any physical contact, or even awareness, of established communications in this Internet of Things; being this the case, of course there is a need and special concern on privacy and security issues.

This paper discusses these technologies and presents a new m-health service architecture, using RFID tags and structured around the Internet of Things, to establish a remote medication control system for Ambient Assisted Living, specially aimed at elderly people care in outpatient clinic. The main objective of this m-health service architecture is to allow elderly patients to self-manage their health in mobility, outside any special health care giving unit, either by monitoring their disease or by helping them to control the timely and correct intake of their medication.

After the technological context discussion and review of related work in section 2, the general IoT architecture we propose is presented in section 3. Section 4 describes the prototype m-health service we have implemented and the testing of its main components, focused on RFID identification and Object Name System resolution, but also dealing with security and indoor localization aspects. Section 5 presents some concluding remarks and future work.

2. Internet of Things Technologies and Related Work

2.1. RFID

Although different RFID tags may operate, as defined in ISO/IEC 18000 standardization documents, Part 1 - Part 7, at several radio frequency bands - bellow 135 KHz for Low-Frequency, at 13.56 MHz for High Frequency, at 433 MHz or at 860 MHz to 960 MHz for Ultra High Frequency (UHF), at 2.45 GHz for Super High Frequency - we will focus on UHF band tags, mainly on account of the envisaged distance between readers and tags. There are different types of RFID tags, operating at different radio frequency bands, and those frequency bands determine, almost directly, the feasible reading distances, that is the distance range between readers and tags that ensure tag reading. Those distances may vary, and for passive RFID tags, from a few centimeters (when Low Frequency bands are used) to several meters, for UHF band, as Table 1 presents. Also, tags may be classified as Read Only (RO), Write Once Read Many (WORM) and Write Many Read Many (WMRM) corresponding the type of the access to information that is kept in its memory structure. Furthermore, tags may be characterized as active, passive and semi-passive, when dealing with the existence (or not) of any internal power source: active tags do have an internal power source, used for processing and communications; passive tags have no internal power source and derive their power, needed for communication purposes, directly from the energy transmitted by the reader antenna, by means of power harvesting; semi-passive tags normally have a very small internal power source, used essentially for internal processing (e.g. sensing, data logging). Semi-active tags are only active when programmed to send a signal at previously predetermined intervals or when interrogated by the readers antenna, from which they derive power for data transmissions.

Table 1. Comparison of some Characteristics of RFID Tags

Characteristics	Passive RFID	Active RFID
Frequency	860-960MHz	860-960MHz & 2.4 GHz
Internal Power	No	Yes
Memory	WORM	WMRM
Read Range	Up to 12 m (36 feet)	Up to 100 m (325 feet)

Indeed there are tags specially suited to be used for medical staff and patients in health environments (e.g. UHF Medical Wrist Bands and Straps (Gen-2)), especially those that are passively coupled, where there is only a magnetic field coupling. So, tags are not constantly emitting any radio signals; when they are stimulated by the magnetic field that the reader is emitting, they harvest power and modulate the answer. So, passive tags become completely safe for usage, for wearing or even implanting, in healthcare or in health sensitive environments.

2.2. Towards an Internet of Things for M-Health

Automatic and easily serialized identifiers became the main driver for an Internet of Things. With the aid of a global and generic identification system, such the Electronic Product Code (EPC), together with EPC-compatible RFID tags and access to a global and distributed Directory system (to resolve those unique EPC identifiers to database locations), one gets all the necessary building blocks for establishing a real Internet of Things: automatic identification, automatic and somehow powerless data capture techniques, access to a distributed data indexing system, together with wireless communications capabilities.

All Gen-2 tags (and all other after Class I Gen-2, as seen on Table 2) have equal basic memory features that encompass a 96 bit Electronic Product Code, EPC, a number identification that can be used also for other purposes, a kill password (32 bit) to permanently disable the tag, an access password (also 32 bit) to lock the read/write characteristics of the tag and also set the tag for disabling, apart from a tag identifier (32 - 64 bit) that identifies the tag manufacturer, but may differ in user memory characteristics (ranging from several bits up to some Kbit or even some tenths of Kbit).

The Electronic Product Code (EPC) [9], which is an open standard, is a code number that gives the unique identification of a given physical object. RFID Tags, directly referenced in the EPC open standard, are the main data carrier that most applications use for accessing the Electronic Product Code. Information read from RFID Tags may then be automatically entered into digital medical records.

Table 2. RFID: EPC Class structure

EPC Class	**Characteristics**	Programming
Class 0 Gen-1	Read Only, Passive ID	Factory programmed
Class I Gen-1	Passive Tags, Write Once Read Many	User programmed, once, then locked
Class I Gen-2	Passive Tags, Write Many Read Many (WMRM)	User programmed
Class II	Passive Tags, WMRM, with additional functionalities (memory, encryption)	Re-Programmable
Class III	Semi-Passive Tags, may support broadband communications	Re-Programmable
Class IV	Active Tags, may support broadband peer-to-peer communications (readers, other tags, same frequency band)	Re-Programmable
Class V	Readers. Can power other tags (Class I-III), can communicate wirelessly with other Class V or Class IV tags	Reader, Not Applicable
Class III	Semi-Passive Tags, may support broadband communications	Re-Programmable

There are three main types of digital medical records: i) Electronic Medical Record (EMR), which are healthcare providers centered; ii) Electronic Health Record (EHR), when patient health information is to be shared across different health providers; iii) Personal Health Record (PHR), whose set up, access and management is carried out by patients.

According to the definition from the Healthcare Information and Management Systems Society an electronic Personal Health Record (ePHR or simply PHR) [10] is a ”[...] lifelong tool for managing relevant health information, promoting health maintenance and assisting with chronic disease management via an interactive, common data set of electronic health information and e-health tools. [...] The ePHR is owned, managed, and shared by the individual or his or her legal proxy(s) and must be secure to protect the privacy and confidentiality of the health information it contains”. PHR emanated to fulfill the need for patients to control and access their own personal medical data, enabling them to keep record of their own medical data. There are several solutions for PHR management, such as Microsoft HealthVault and Dossia [11]. PHRs enable patient-entered information, such as medication plans or data from home monitoring devices, and its access control is totally managed by the patient.

When dealing with mobility one can not use EMRs because they are provider centered; although EHRs enable access to trusted medical records it is difficult to share information as it depends on agreements across different institutional health providers, difficult to accomplish. That is the main reason why we rely on PHRs, as they are patient managed and patient controlled; of course that there must be some information transfer from EHRs, determined with trust by medical staff, into the PHRs that hold all the needed patients' information when in mobility.

2.3. Security and M-Health

Health context is very sensitive, and so it has some very specific security requirements. It is necessary to prevent any unauthorized access attempt to private information and it is also important to keep an updated log that records system failures [12].

In m-health context, several security threats must be taken into account, especially wireless communications and radio security, Internet of Things security and Radio Frequency IDentification security.

Wireless communications and radio security - wireless communications, a must for m-health applications context, have even more security problems [13]: data is transmitted through radio frequencies, available to any intruder unless protected; if unprotected, data may be destroyed, modified or stolen, and can also be subject to various other attacks (eg Denial of Service).

Internet of Things security - Internet of Things devices are being used in healthcare systems [14] and new security measures for IoT have been proposed [15], as this IoT context has already exhibited special interoperability and security problems [16].

Radio Frequency IDentification security [17][18] - Most of the Radio Frequency Identification solutions for e-health are using tags that comply with the standard EPC Gen2 [9] because they are passive and low cost. Furthermore, their use enables building an average cost system able to offer a suitable level of security, especially regarding the protection of privacy [19].

According to [20] security attacks on RFID may be classified into three main categories: privacy and authentication attacks, attacks on data integrity and the network availability attack (Denial of Service (DOS) attacks). The most relevant protocols to be used with RFID found in literature were RFID Grouping Proofs [21] and Cryptographic Puzzles [22].

In a health environment system it is important to balance system security with availability. A non-authorized access may be harmful to the system or patients. But in case of emergency, if medical personal can't reach the needed information it can be even more dangerous, mainly to the patients. The necessary security balance is crucial as adding or modifying any important medical information may be catastrophic.

2.4. Indoor Location Awareness

One possible application of RFID is Indoor Real-Time Localization Systems (RTLS). Although several solutions exist for outdoor localization, mainly GPS based, indoor localization still remains a challenge. In indoor environments the line-of-sight transmission between devices and satellites is not possible and the satellites signals are heavily attenuated and reflected by the building materials. On the other hand, many technologies can be used for indoor localization, such as infrared, computer vision, ultrasound and Radio Frequency (RF). In turn, the use of RF may include RFID (Radio Frequency Identification), Bluetooth, UWD (Ultra-WideBand) and Wireless Local Area Networks (WLAN). The use of WLANs to locate devices has been subject of research in recent times and has increasing importance because it is already widely deployed for other services [23]. However, WLAN devices are more expensive and larger than RFID tags. For small objects, RFID tags can provide a good and less expensive alternative.

Indoor environments are complex because the propagation of electromagnetic signals may be influenced by the existence of obstacles like walls, equipment, and even human beings, which causes multi-path effects. There are various different strategies to perform Indoor Localization using RFID [24] and they may be classified based on the strategy used to compute location, using various types of signal measurements (Received Signal Strength (RSS), Angle Of Arrival (AOA) and Time Of Arrival (TOA)). When used this criterion to classify RFID Indoor Localization Systems, they fall into these different categories: Proximity, Triangulation and Scene Analysis.

Proximity is the easiest approach. When the object we intend to locate enters in the radio range of a Reference Point their location is assumed to be the same. Typically when using this approach the Reference Point is a RFID Reader and the object to locate is carrying a RFID tag. Triangulation approach, on the other hand, uses the geometric properties of triangles to determine the location of an object and has two variants: lateration and angulation. Lateration estimates the location of an object by measuring its distance from multiple reference points. Angulation locates an object by computing angles relative to multiple reference points. Finally Scene Analysis uses a completely different approach. It can be divided into two phases: an offline phase and an online phase. In the first phase, called the offline phase, information concerning the localization area is collected and stored in a fingerprinting map. Then in the online phase, online measurements are taken and compared with those previously observed in the offline phase in order to infer the object position. Due to the very limited capabilities of RFID tags the Proximity approach is widely used, however it may present low accuracy.

RFID Localization can also be classified depending on the different roles assumed by RFID tags and readers. When using Reader localization scheme, the RFID reader is attached to the object that is intended to locate and RFID tags are scattered in the localization area (typically the floor) [25]. In the Tag localization scheme, the opposite is proposed: the object to locate carries the RFID tag and the Reference Points are implemented by RFID readers installed in the localization area [26]. Both Reader and Tag localization may present the same accuracy, however

since the tag price is cheaper than the reader, Tag Localization may be suitable for application with many objects to locate, like tracking patients in Hospitals.

3. Service Architecture for M-Health in IoT

In order to illustrate the service architecture let us first introduce a possible m-health complete scenario where patient mobility, automatic identification of things and the Internet of Things are combined together into a real problem solving solution.

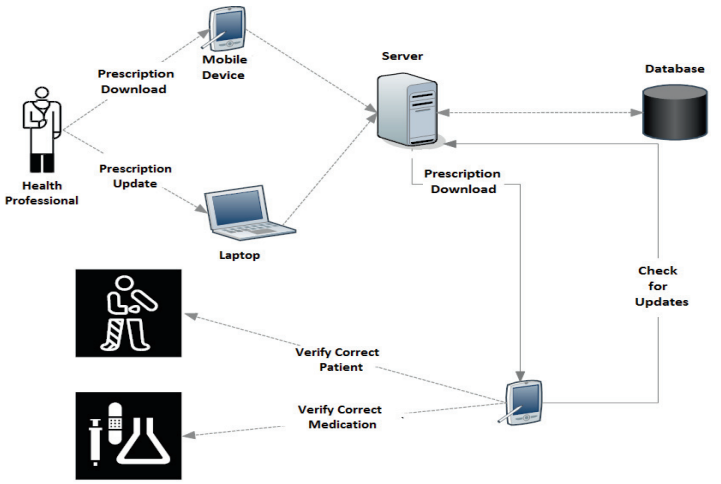

Figure 1. Smart objects and Internet of Things for M-Health

Figure 1 presents a global Internet of Things architecture, able to support ubiquitous Health care service delivery and service control in an Assisted Ambient Living, encompassing mobility of any of the health players: health professionals, patients, care givers, pharmacists. Doctors, using their own personal or institutional devices (either mobile or fixed) will issue prescriptions that will be immediately updated in the database. Patients, or caregivers, in mobility will have access to a smartphone (or a tablet) running the m-health application. Mobile devices, using RFID technology, enables pharmacists to deliver the right medication and users to verify that they are sure to take/deliver the right medication at right time. Along this whole process, the security is a major concern: data confidentiality and integrity has to be granted, all users and even applications must be accredited and authenticated.

3.1. M-Health Context

A study carried out in Portugal on ”Adherence to Medication Regimen in the Elderly” [27] (PhD thesis, in Portuguese) showed that a large majority of the elderly people need external help for managing medication. Having carried out a study with a population of elderly people, the study stated that ”interventions (giving advise on pharmaceutical drugs, pharmaceutical drugs control and pharmaceutical drug education) are effective in increasing adherence” to medication. Looking at the summary of the type of help that Portuguese elderly patients (older than 65 years, as published in [27]) said to be needing in order to adhere to medication, one can notice that a large majority of the elderly need help in medication control, being that more than 80% present reasons that can be almost completely overcome by Ambient Assisted Living systems.

3.2. IoT Service Architecture

The Internet of Things Service Architecture for AAL, specially targeted for M-Health solutions, satisfies the requirements described bellow. All health-related items should have auto-identification capabilities, in order to leverage its use as smart objects. This auto-identification corresponds to a unique and global identifier, based upon the Electronic Product Code standards.

Auto-identification capabilities apply not only to every health items but also to all other health stakeholders in the system, as persons are also identified using the same principle. Auto-identification may also be applied to health instruments, health goods and public spaces. All the above auto-identification principles may also be used for indoor location awareness and guidance, as well as for safety location purposes (eg, restricting baby displacements in nurseries). In this architecture, all items and health stakeholders identifiers may be easily serialized and read without direct contact, namely by means of RFID readers (accessing mainly passive RFID tags).

There is a standard, although tunable and adaptable, distributed Directory system, whose implementation is done by means of an Object Naming System. There are mobile smart devices that can connect to the Internet, although not necessarily depending on online only operations. Users are able to create, use and manage their Personal Health Records using their mobile devices.

In this architecture, security issues are based on a Public Key Infrastructure (PKI) and PKI certificates. Security concerns extend from users to devices, from devices to applications and from applications to services. The Object Name Service prototype system, firstly presented in [28], assumes that physicians, patients and medicines are to be identified by means of RFID tags and that the entire process, from drug prescription until its intake, is controlled by an information system completely based on IoT.

For that, both stakeholders (doctor, pharmaceutical, nurse, patient) and medicines have an RFID-tag assigned. Additionally, electronic equipment used by them, such as tablets or smartphones, include a RFID reader

4. Prototype Service Implementation

4.1. Object Name Service Prototype

The Object Name Service prototype system, firstly presented in [28], assumes that physicians, patients and medicines are to be identified by means of RFID tags.

The entire process, from drug prescription until it is taken, is controlled by an information system based on IoT.

For that, both stakeholders (doctor, pharmaceutical, nurse, patient) and medicines have an RFID-tag assigned. Additionally, electronic equipment used by them, such as tablets or smartphones, include a RFID reader.

The prescription issued by the doctor (with RFID) with the indication of the type of drugs (each having an associated RFID-tag), dosage and associated time of take, is written into the Electronic Health Record of patient and passed into his/hers' Personal Health Record. If a pharmaceutical intervenes in the preparation and delivery of the drug, he will also have his RFID associated with the event.

To support this IoT based AAL system a prototype Object Name Service, whose block diagram is presented in Figure 2, was developed. The prototype enables the registration and retrieval of information about several entities (doctors, nurses, patients, pharmacists) and objects (drugs, prescriptions) of interest. This information, after enforced verifications are performed by the security mechanisms, is accessible in a ubiquitous manner for the existing AAL applications.

The service provided by ONS is given a URI (for example urn:epc:id:sgtin:0614141.000024.400) in a standardized format (in this case, for instance 000024.0614141.sgtin.id.onsepc.com) and returns a set of Resource Records (taking the form of NAPTR records, for the prototype in Figure 2) that link the item with its Internet related pointers. The URI is obtained automatically from the EPC that is read from the RFID tag. The prototype is using format SGTIN, with a length of 96 bits, for the EPC. The operation to be performed on the EPC may be simply a query for information but may also record information about a related event.

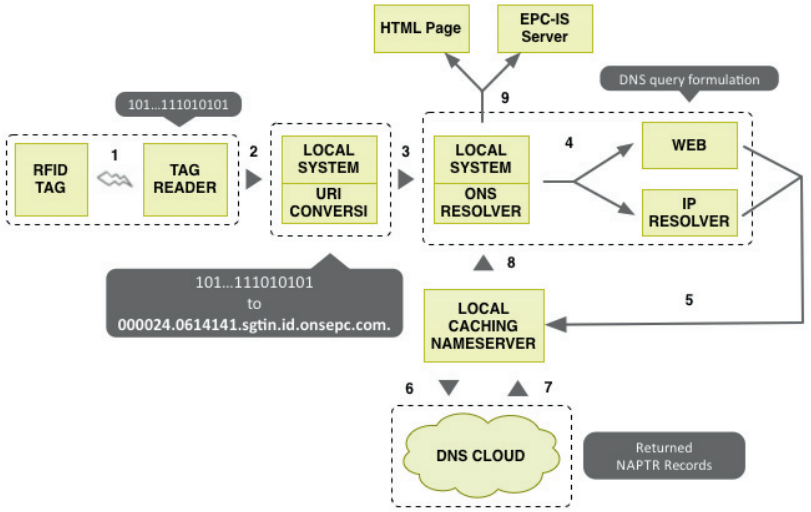

Figure 2. ONS support for M-health applications (adapted from [12])

4.2. *Security Protocols for M-Health*

In [14] we have presented an application layer security context for m-health and its protocol definition.

To achieve all the fundamentals of cryptography, one need tools such as hash functions, digital signatures, symmetric and asymmetric keys and Public Key Certificates [29]. These Public Key Certificates are digital documents, owned and held by a single entity, that prevent any other entity to impersonate another. Certificates are issued by an Certification Authority, CA, a trusted central infrastructure known as a Public Key Infrastructure (PKI) that testifies the validity of the certificates.

In order to bring strong authentication, encryption and privacy in e-Health context for medication control, authors [14] proposed a secure architecture and new M-Health Security Protocols that provide an application level secure channel for (mobile) client-server interactions. Additionally, the whole secure architecture discussed in [14] enable strong authentication from both users but also for mobile devices. The use of RFID tags to identify entities, combined with an RFID Grouping Protocol, and with the M-Health Security Protocol, provide a complete and common security framework to implement Mobile E-Health Applications for Medication Control.

4.3. *RFID for Indoor Location Awareness and Guidance*

RFID tags are also used for indoor localization procedures, to locate all types of entities (doctors, nurses, patients and helpers) or objects (medication, equipment, etc) that carry them. A simple proximity-based positioning methodology is easier and cheaper to deploy, yet it allows for the implementation of monitoring and alert systems of great added value. In this technique, tag location is considered to be the same of the RFID reader that was able to read it in its antenna range. Accuracy is very low and conditioned by the reading range of each reader. The number and position of RFID readers must be previously planned and registered for each building and system costs depend on this planning.

In our work we have done a simulation example in java. The program works on a building floor plan. In first stage special access areas or zones must be identified, either rooms or corridors or mixed aggregates of corridors and rooms. These areas are named using user-friendly common names and, for each name, access control rules are enumerated. Simple rules include the definition of who (patients, visitors, medical staff) or what (equipments, etc) can or cannot enter or leave the zone. This access control rules can be specified by selection, mapping entities, zones and actions. In second stage, RFID readers are positioned only in enter and exit points of those areas. Third phase is

a validation phase, done by simulating the movement of a simple tag in the plan. This type of tool is required and must be improved for effective planning.

A centralized system collects tag ids read by each RFID-reader and registers the tag position in the system. Public buildings, like hospitals and clinics, or even patient's home facilities, are required to have a set of RFID-readers pre-registered in the system, at known positions and with network access. Location data is stored and updated in real time on the server. When a RFID-tag changes its position to a new zone, a stored procedure runs a check on all access control rules associated with that zone. An event is generated on each broken rule and a pre-configured associated set of actions is immediately executed. There are three types of actions, while more can be defined: security alerts, simple notification and system updates. Security alerts are signaled (sound or visual) and require other entities (staff, for instance) to be notified. An example is when a visitor enters on a staff-only zone. A sound alert is originated and security staff is alerted. Notifications require only appropriate signaling. In our example, the building is also populated with information screens and this type of information is presented in the nearest screen. As an example, consider a visitor or a patient that previously checked in at reception with a well-known destination zone. If the RFID-tag associated with him is located out of the best path, a notification is issued as a simple signal or navigation indication (go back, go left, etc) in the nearest screen. The third type of action requires system state updates. If two entities are detected in the same zone, that meeting can be automatically registered. If the two entities are a patient and his doctor and the time frame is adequate, that can be registered as potential medical consultation; a patient and an equipment may be registered as a potential medical exam; a patient and its medication as a potential medication taking action, etc. This type of events can further be used on other security alerts. If a patient meets no doctor for a long period of time, he may be missing, voluntarily or not, his periodic consultation. In the same way, if patient and medication were not identified in the same zone for long time, medication was not taken as expected.

Experiments conducted on hypothetical facilities show that a reduced amount of RFID-readers is required for potential large security benefits.

5. Conclusions and Future Work

This paper presents a simple and secure Internet of Things architecture aimed at establishing a generic and ubiquitous Ambient Assisted Living framework to be used by Mobile Health applications. The global solution presented is based on Radio Frequency Identification technology (RFID) and Electronic Product Code (EPC) normalization for the establishment of a unique identifier for each m-health related item (an object, a medicine, pharmaceutical drug, physician, patient, caregiver, drug, hospital, pharmacy, etc). Any of such identifier may be read without direct contact and is to be used as a primary access key to a service indexer, via an Object Name Service (ONS), that enables linking any of such physical items to its virtual correspondents in a global Internet of Things.

In order to ensure the necessary privacy and security levels of any m-health Ambient Assisted Living applications within this architecture, the paper also presents the security context that has been defined, applied both to devices, users and software applications. The paper also argues that the broad development of RFID technology has the potential to increase patient safety in medical services and to reduce costs. As most health services can be enhanced with the location, tracking and monitoring, specially in mobile and ubiquitous environments, an IoT system for monitoring and position referral of any of health-related entities - people (such as patients, nurses, doctors visits, auxiliary) and goods (such as medicines, clinical analyzes, wheelchairs, beds, medical equipment) - has been presented and discussed.

As future work, authors are extending the system and its mobile applications in order to test this AAL architecture in corporate health facilities. This would enable testing entities/objects location in real scenarios, also testing the systems' usability by the elderly, personnel adherence to secure authentication mechanisms, encrypted communications and the other global security levels.

Acknowledgements

This work has been partially supported by FCT - Fundação para a Ciência e Tecnologia, in the scope of the project: PEst-OE/EEI/UI0319/2014.

References

[1] Tan L, Wang N. Future Internet: The Internet of Things. Adv. Comput. Theory Eng. (ICACTE), 2010 3rd Int. Conf., vol. 5, 2010, p. V5–376 –V5–380.

[2] Wu M, Lu T-J, Ling F-Y, Sun J, Du H-Y. Research on the architecture of Internet of Things. Adv. Comput. Theory Eng. (ICACTE), 2010 3rd Int. Conf., vol. 5, 2010, p. V5–484 –V5–487.

[3] Sharma M, Siddiqui A. RFID based mobiles: Next generation applications. Inf. Manag. Eng. (ICIME), 2010 2nd IEEE Int. Conf., 2010, p. 523–6.

[4] Ziegler J, Urbas L. Advanced interaction metaphors for RFID-tagged physical artefacts. RFID-Technologies Appl. (RFID-TA), 2011 IEEE Int. Conf., 2011, p. 73–80.

[5] Viret J, Bindel A, Conway P, Justham L, Lugo H, West A. Embedded RFID TAG inside PCB board to improve supply chain management. Microelectron. Packag. Conf. (EMPC), 2011 18th Eur., 2011, p. 1–5.

[6] Rajagopalan H, Rahmat-Samii Y. On-body RFID tag design for human monitoring applications. Antennas Propag. Soc. Int. Symp. (APSURSI), 2010 IEEE, 2010, p. 1–4.

[7] He W, Zhang N, Tan PS, Lee EW, Li TY, Lim TL. A secure RFID-based track and trace solution in supply chains. Ind. Informatics, 2008. INDIN 2008. 6th IEEE Int. Conf., 2008, p. 1364–9.

[8] Katayama M, Nakada H, Hayashi H, Shimizu M. Survey of RFID and Its Application to International Ocean/Air Container Tracking. IEICE Trans 2012;95-B:773–93.

[9] GS1 AISBL (GS1). EPC Tag Data Standard - GS1 Standard Version 1.8 2014.

[10] HiMSS. HIMSS Electronic Personal Health Record Definition Fact Sheet 2008.

[11] Eysenbach G. Medicine 2.0: Social Networking, Collaboration, Participation, Apomediation, and Openness. J Med Internet Res 2008;10.

[12] Laranjo I, Macedo J, Santos A. Internet of Things for Medication Control: E-Health Architecture and Service Implementation. Int J Reliab Qual E-Healthcare 2013;2:1–15.

[13] Mueck M, Ivanov V, Choi S, Kim J, Ahn C, Yang H, et al. Future of wireless communication: RadioApps and related security and radio computer framework. Wirel Commun IEEE 2012;19:9–16.

[14] Goncalves F, Macedo J, Nicolau MJ, Santos A. Security architecture for mobile e-health applications in medication control. 21st Int. Conf. Software, Telecommun. Comput. Networks (SoftCOM), 2013, 2013.

[15] Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Meghanathan N, Boumerdassi S, Chaki N, Nagamalai D, editors. Recent Trends Netw. Secur. Appl., vol. 89, Springer Berlin Heidelberg; 2010, p. 420–9.

[16] Tarouco LMR, Bertholdo LM, Granville LZ, Arbiza LMR, Carbone F, Marotta M, et al. Internet of Things in healthcare: Interoperatibility and security issues. Commun. (ICC), 2012 IEEE Int. Conf., 2012, p. 6121–5.

[17] Martin H, San Millan E, Peris-Lopez P, Tapiador JE. Efficient ASIC Implementation and Analysis of Two EPC-C1G2 RFID Authentication Protocols. Sensors Journal, IEEE 2013;13:3537–47.

[18] Khoo B. RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. Internet Things (iThings/CPSCom), 2011 Int. Conf. 4th Int. Conf. Cyber, Phys. Soc. Comput., 2011, p. 709–12.

[19] Peris-Lopez P, Orfila A, Mitrokotsa A, van der Lubbe JCA. A comprehensive RFID solution to enhance inpatient medication safety. Int J Med Inform 2011;80:13–24.

[20] Hadda Ben Elhadj Nourchene Bradai LC, Kamoun L. A survey of security proposals and issues in wireless body area networks for healthcare applications. 2012 Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2012, 2012.

[21] Pedro Peris-Lopez AO, Hernandez-Castro JC, van der Lubbe JCA. Flaws on RFID grouping-proofs. Guidelines for future sound protocols. J Netw Comput Appl 2011;34:833–45.

[22] Peris-Lopez P, Hernandez-Castro JC, Tapiador JME, Palomar E, van der Lubbe JCA. Cryptographic puzzles and distance-bounding protocols: Practical tools for RFID security. RFID, 2010 IEEE Int. Conf., 2010, p. 45–52.

[23] Silva JA, Nicolau MJ, Costa A. WiFi Localization as a Network Service. Proc. 2011 Int. Conf. Indoor Position. Indoor Navig., Guimaraes: 2011.

[24] Bouet M, dos Santos AL. RFID tags: Positioning principles and localization techniques. Wirel. Days, 2008. WD '08. 1st IFIP, 2008, p. 1–5.

[25] Han S, Lim H, Lee J. An Efficient Localization Scheme for a Differential-Driving Mobile Robot Based on RFID System. Ind Electron IEEE Trans 2007;54:3362–9.

[26] Ni LM, Liu Y, Lau YC, Patil AP. LANDMARC: indoor location sensing using active RFID. Pervasive Comput. Commun. 2003. (PerCom 2003). Proc. First IEEE Int. Conf., 2003, p. 407–15.

[27] Henriques MAP. Adesão ao regime medicamentoso em idosos na comunidade: eficácia das intervenções de enfermagem (in Portuguese). Universidade de Lisboa, 2011.

[28] Laranjo I, Macedo J, Santos A. Internet of Things for Medication Control: Service Implementation and Testing. Procedia Technol 2012;5:777–86.

[29] Robling Denning DE. Cryptography and data security. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.; 1982.