m-Carer: Privacy-Aware Monitoring for People with Mild Cognitive Impairment and Dementia

Agusti Solanas, *Member, IEEE,* Antoni Martínez-Ballesté, *Member, IEEE,*
Pablo A. Pérez-Martínez, Albert Fernández de la Peña, and Javier Ramos

***Abstract*—Age-related diseases are becoming more prominent due to life expectancy increase in developed countries. Mild cognitive impairment and several types of dementia like Alzheimer's disease are gaining importance both socially and economically. Patients suffering from these diseases have different degrees of autonomy and, thus, different needs. Often, relatives or friends take care of those patients. However, during the first stages of the disease, they still have a high degree of autonomy and frown on the supervision of others.**

Despite their autonomy, patients could get lost and disoriented. Rapidly determining the location of a lost patient is paramount to reduce the risk of suffering serious injuries. Current solutions to this problem are based on the continuous monitoring of the patient. Such continuous control might be seen by most people as a privacy invasion, and it may discourage patients from using these solutions.

In this article we present the concept of *m-Carer* as a smart mobile device able to privately monitor the movements of patients having diverse degrees of mobility and autonomy. After justifying the need for privacy-aware m-carers due to social and economical reasons, we propose a complete architecture aimed at fulfilling the needs of patients, relatives and healthcare services. Moreover, we show a real implementation of our proposal so as to confirm that it is technically sound and feasible.

***Index Terms*—m-Health, privacy, location monitoring, mild cognitive impairment, dementia.**

I. Introduction

In the last decades the society of the so-called developed countries has changed significantly. Whilst fertility rates are reaching unprecedented low figures, life expectancy grows steadily. As a result, we are witnessing the dawn of an aged society that poses new social and economical challenges. This ageing of the population leads to an increase in the cases of cognitive disorders related to age like Mild Cognitive Impairment (MCI), Frontotemporal Dementia, Lewy Body Dementia, Parkinson's Disease and Alzheimer's Disease (AD).

We are specially interested in MCI because it can be seen as a precursor of the early stages of AD and other types of dementia that imply impaired memory function whilst the cognitive function is generally preserved [1]. People suffering from MCI and early stages of different types of dementia might experience a decrease in their cognitive capabilities but they still have considerably high degrees of autonomy (*i.e.* they can live alone, walk, do exercise). The most apparent impairment is related to their memory function: patients might become spatially and temporally disoriented, and might have problems in finding their way home.[1] Note that although patients with MCI and early stages of dementia are the ones that motivated this research, patients suffering from more advanced stages of dementia might benefit even more than the formers because they tend to become spatially and temporally disoriented more frequently.

With the promise of being helpful to address many medical situations, information and communication technologies (ICT) have attracted the attention of the medical community, from physicians and health scientists, to regulators and governments. In this regard, a collection of devices and complex systems such as computers, sensors and databases are used in the so-called electronic health (**e-health**). ICT might be used for a variety of health-related tasks, namely communication between patients, doctors and carers (mobile health support), remote provision of care (mobile telemedicine), remote support to diagnostic (mobile telediagnosis), electronic medical records, smartcard-based prescriptions, etc.

The use of ICT in the healthcare sector has significantly contributed to reduction of management costs and efficiency increase increase. In this line, e-health substantially reduces the displacements of professionals and patients, globally brings down the cost of medical resources, and makes treatments and health watchfulness more comfortable to patients. All in all, e-health might be considered a revolution in this area. However, the next and probably more important revolution is taking place due to the use of mobile devices (*e.g.* smartphones) with unprecedented processing and communication capabilities. These mobile devices have favoured the emergence of mobile health (**m-health**), understood as the discipline founded on the use of mobile communication devices in medicine, or more specifically the delivery of healthcare services via mobile communication devices.

The use of mobile devices simplifies and makes many tasks more efficient. Specially the remote monitoring of patients and the communication between professionals, relatives and patients will highly benefit from the use of m-health. Moreover, m-health allows rapid gathering of data from patients, thus, providing doctors and scientists with a large amount of information that can be used for a variety of purposes.

Manuscript received February 15, 2012; revised July 17, 2012.

The authors are with the UNESCO Chair in Data Privacy and the Department of Computer Engineering and Mathematics, Rovira i Virgili University, Av. Paisos Catalans 26, 43007, Tarragona, Spain (e-mail: {agusti.solanas, antoni.martinez, pabloalejandro.perez, albert.fernandezd, javier.ramos}@urv.cat).

Digital Object Identifier 10.1109/JSAC.2013.SUP.0513002

[1]When the disease advances these patients may become wanderers and might require special supervision.

Certainly, m-health fosters innovation in the healthcare system of industrialised countries. Nonetheless, it can be regarded as a way of providing quick and effective access to health services to large populations without nearby hospitals or medical centres. Hence, the rapid proliferation of affordable smartphones in rural areas or in developing countries [2] might clearly improve the overall efficiency and coverage of their healthcare systems. Despite all the advantages of e-health and m-health applications, they cannot be applied without considering fundamental issues like the privacy and security of the users [3] (*e.g.* data access control, data disclosure, data privacy, etc).

There is a real need for systems and methods allowing the private supervision of patients, specially when, due to their disorders, they can easily get lost. Under specified circumstances (*e.g.* when a fall is detected), these systems should permit authorised users to locate patients. Notwithstanding, if no special events happen, the system must prevent users from locating patients, thus, preserving their fundamental right to privacy.

A. Contribution and plan of the article

e-Health has demonstrated to improve many healthcare-related procedures and we believe that, thanks to the steady advances in mobile communications, m-health will lead to the next revolution in the healthcare sector.

In this article we propose the new concept of **m-Carer**, this is, an intelligent application that runs on smartphones and allows the private monitoring of people's location. By using the proper cryptographic primitives, our proposal guarantees the privacy of patients whilst, at the same time, they can be located if necessary (*e.g.* if an emergency arises). Our proposal is easy to use and it does not require patients to use annoying and indiscreet devices like necklaces or bracelets.

Although we focus on patients diagnosed with MCI and initial stages of dementia, our solution could be easily extended to deal with the monitoring of children, disabled people, etc. We realise that privacy is not always a priority, specially when a patient's well-being might depend on quick and easy access to information [4]. However, we deem confidentiality of information to be critical both to guarantee the fundamental right of individuals to privacy and to avert hindrance to the monitoring system.

With the m-Carer we do not aim at replacing human carers but to provide them with a powerful tool able to simplify their job, improve their efficiency, reduce costs, and keep the fundamental rights of patients fully guaranteed.

The rest of the article is organised as follows: Section II justifies the need for m-carers, provides an overview of their architecture, and the main actors of the systems and their roles. Next, Section III describes the main situations handled by the system and the different states of alarm that have been considered. With the aim to demonstrate the real applicability of the system, we have implemented a fully functional m-Carer and we describe it in Section IV. For the sake of completeness, we summarise the most relevant previous work related to location monitoring in Section V. Finally, the article ends with some concluding comments and remarks in Section VI.

II. The m-Carer Architecture

In this section we provide an overview of the concept of m-Carer and its fundamental architecture. First, we justify the need for this kind of system and explain its main functions in Section II-A. Second, in Section II-B we present a running example that is used throughout the article to support the explanation of different situations and concepts. Finally, in Section II-C we describe the main actors of the system, their roles, and their relations.

A. Rationale, concept and desiderata

As we have previously stated in the introduction, we observe two very important trends: (i) our society is getting older, thus increasing the number of cases of MCI and dementia, and (ii) mobile communications are experiencing a massive development that leads to the appearance of m-health.

m-Health redefines the healthcare services in three main aspects:

- m-Health allows **easy access** to an unprecedented number of services and knowledge. Thanks to the inherent **ubiquity** of mobile devices, services may be accessed everywhere, anytime. Moreover, data could be collected more easily regardless of the location of the user.
- m-Health is **user-oriented**. Users play a key role in an m-health service. Services should be where the user is.
- m-Health is **personalised**. Users receive customised services, that fit their needs properly.

With all these main trends and features in mind, we can define an m-Carer as follows:

> *A mobile carer **m-Carer** is a mobile device and an infrastructure that provides patients/users with healthcare monitoring services in a private, reliable, and personalised way.*

An m-Carer (in the context of an ageing society) is aimed at improving the quality of life of people suffering from MCI and early stages of dementia. To do so, an m-Carer privately monitors the location of patients and allows their safe recovery if they get lost or disoriented[2]. Also, the quality of life of their relatives and carers might be improved. Note that patients with MCI and initial stages of dementia have a significant degree of autonomy. In this regard, an m-Carer is designed as a non-invasive tool aimed at helping relatives and human carers to supervise the regular activities of patients whilst respecting their fundamental right to privacy.

An m-Carer should have the following features:

- **100% private:** The supervision should be private to avert any hindrance from the patient. Avoiding the "Big Brother" effect is paramount to guarantee the acceptance of patients with a high degree of autonomy. If alarm conditions are not met the location of patients should be kept secret.
- **Intelligent and reactive:** The m-Carer must be able to detect situations in which the safety of the patient is in danger. Some examples of those situations are the following:

[2]Note that patients with MCI and early stages of dementia are autonomous but might get lost, thus endangering their safety.

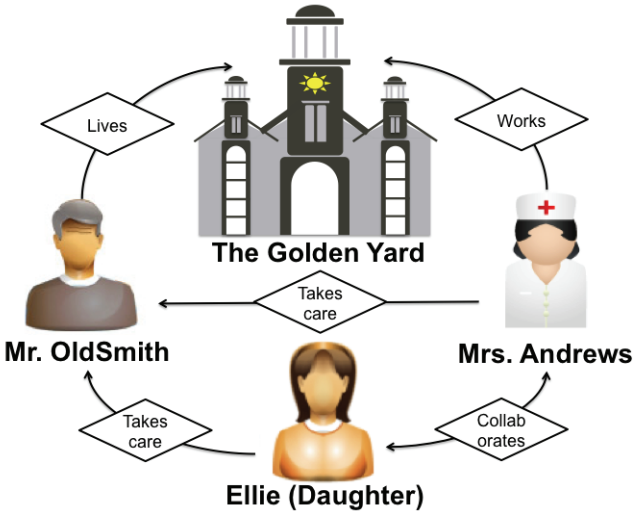

Fig. 1. Illustration of our running example. In the figure, the main actors of the systems are depicted along with their relations.

  - The patient is approaching risky areas (*e.g.* highways, cliffs, rivers, etc).
  - The patient is not in a usual place and he or she is probably lost.
  - The patient has fallen and might be injured.
- **Autonomous:** Collaboration of the patient should not be required. The m-Carer might respond by its own to the possible situations in which the safety of the patient could be in danger. In those cases, the m-Carer should automatically warn the patient, their relatives or carers, and even the emergency services (if necessary).
- **Easy-to-use and accessible:** The m-Carer must be simple and easy to use (even to those patients that are not familiar with information and communication technologies). Alarms and warnings should be easy to configure by patients, relatives or human carers by means of off-the-shelf technology (*e.g.* a regular website). Also, if there is an emergency, the location of the patient might be easily accessible (*e.g.* through SMS messages, or using a secure website).
- **Discreet:** The embodiment of the m-Carer should be simple and usual. If so, patients will have no reason to reject it. It should not be seen as something strange nor intrusive.

B. Running example

Throughout the article we will refer to the following example so as to show the specific functioning of our proposal. The main aim of this fiction is to help us show that although the architecture is quite abstract it has a clear and direct application to real life situations. Note that any resemblance to real people is purely coincidental.

John Oldsmith' case: *John Oldsmith (70) was diagnosed with Alzheimer disease a year ago. All began by forgetting simple things, such as the name of his daughter Ellie or the name of the company in which he had worked for 35 years. Being a widower for three years, Mr Oldsmith decided to retire in a renowned old people's house – The Golden Yard. He wanted to live his life autonomously, together with some of his best friends who also had chosen to retire in The Golden Yard. Having large promenades and enjoying interesting after-meal talks became his everyday activities.*

Mr. Oldsmith is aware that his cognitive capabilities are going to decrease with each passing day. However, he feels strong and healthy enough to carry on with his daily walks. Notwithstanding, Mrs. Andrews, the head of The Golden Yard carers, asks John to carry a GPS-enabled necklace that allows her to know the location of Mr. Oldsmith at any moment – "just in case", she always says. Mr. Oldsmith feels that his privacy is being invaded, and he has to choose between his promenades and his privacy.

C. Structure, actors and roles

The m-Carer (an essential actor of the system) is an application that runs on a smartphone able to locate itself by means of GPS, WiFi, or fixed antennas trilateration. It is able to encrypt information and to send it to a server or a set of servers that store it. The m-Carer uses the telecommunications infrastructure that already exists and does not require any additional device (apart from the smartphone).

In addition to the smartphone (with the m-Carer) and the servers, the system considers a number of human actors, namely patients, official users and unofficial users. Figure 2 depicts a general scheme of the structure of the m-Carer system with all the actors and their relations.

Next, we describe those actors in detail and the role they play within the whole logical structure of the m-Carer system.

1) Patients: Patients are people that are able to move autonomously (*e.g.* have a walk, go shopping, etc.) that due to their cognitive impairments might get lost and require assistance. In order to guarantee their fundamental right to privacy and to avert the "Big Brother" effect, the m-Carer encrypts their information. Patients are equipped with a GPS-enabled smartphone connected to the Internet. We refer to this device as *Patient's Device* in which the m-Carer application runs.

In our example *John Oldsmith* is the patient. Mr. Oldsmith owns a simple smartphone, equipped with GPS and a 3G data connection. He has installed our m-Carer application in his smartphone and he has signed in the system.

2) Users: Users are people ethically or legally responsible for the supervision of patients (*e.g.* human carers, relatives, friends, etc). Although the privacy of the patients is one of our main priorities, for the sake of safety, users are allowed to know the location of patients in some specific situations[3]. Similarly to patients, users are equipped with a smartphone running a *User application*. By using this device, users can interact with the system and receive notifications. We distinguish two different types of users:

- **Official users** are people that are legally responsible for the well-being and safety of patients (*e.g.* civil servants such as social workers, doctors, nurses, or public human carers).

[3]In the next section we will discuss the details about the operation of the system and which procedures the users have to follow in order to obtain the location of patients.

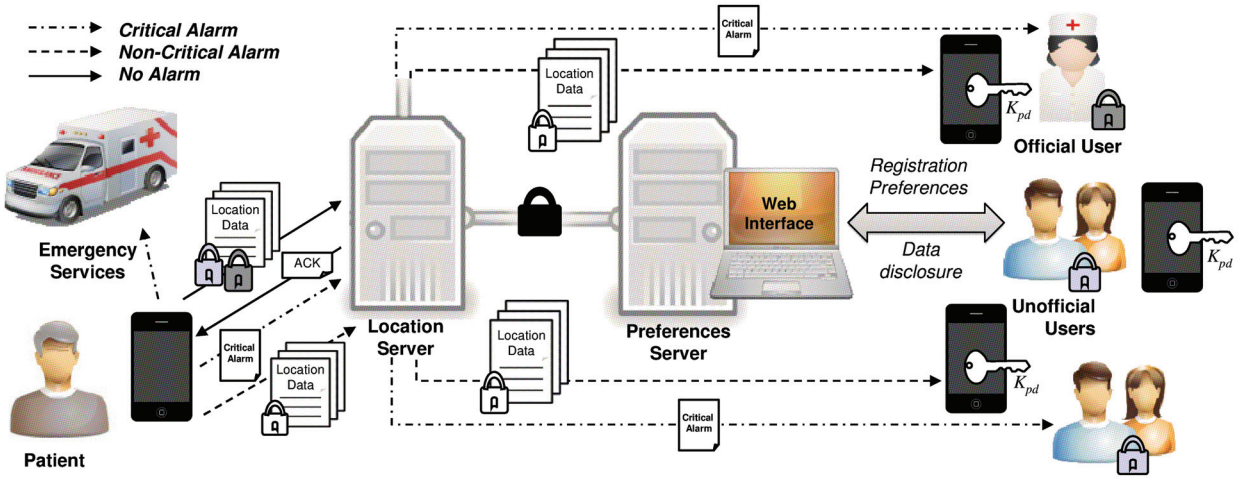

Fig. 2. General scheme of the m-Carer system with all the actors (*i.e.* the m-Carer, the patient, the official and unofficial users, the servers and the emergency services), and their relation under different alarm states.

In our example, *Mrs. Andrews* is the official user for all the patients living in The Golden Yard.

- **Unofficial users** are other people related to the patient, namely relatives, friends and private human carers. Those people might be in charge of patients and would need to know where they are, specially if they tend to get lost. In our example, *Ellie* (Mr. Oldsmith's daughter), is the unofficial user responsible for the safety of Mr. Oldsmith.

3) Emergency services: These are actors that ensure public safety by addressing emergencies (*e.g.* firemen and rescue services, medical emergencies, etc.). In normal conditions, these emergency services do not play an active role in the system (*i.e.* they do not directly interact with the system). However, their help is required when an emergency situation arises. The m-Carer is responsible for informing emergency services and for asking for their help when a critical emergency is detected. We give more details about this procedure in the next section.

4) Servers of the system: In addition to the applications that run over smartphones (*i.e.* the *m-Carer* in the patient's device, and the *User application* in the device of the users), the system comprises a set of servers that support its operation and provide additional functions. Mobile applications interact with these servers by using the already present infrastructure of the telephony company and the Internet service provider. We distinguish two different types of servers in the system:

- **Servers of preferences**, that allow the registration of patients and users into the system. They are responsible for the generation of the cryptographic keys to be used by the *m-Carer* and the *User applications*. Also, they allow users and patients to tune several parameters of the system that controls its behaviour. By doing so, users and patients can customise the service provided by the m-Carer and make it to better suit their needs. Figure 3 shows an illustration of the surroundings of The Golden Yard in our example and the customised areas defined by *Mr. Oldsmith* and his daughter *Ellie*. The information about these areas along with a number of other parameters are stored in the *Server of preferences*.
- **Location servers** receive encrypted location information from the m-Carer of the patients and store it. These servers could receive other data (*e.g.* heartbeat rate, body temperature, etc.). Note that all this information is encrypted and the server does not have access to the cryptographic keys to decrypt it. In this regard, location servers can be understood as log servers that store information of the whole system. The frequency at which m-Carers send information to the servers can be customised by the patients and the users of the system (*e.g.* Usual values range from one to ten minutes).

III. m-Carer Operation and Alarm States

From an operational perspective we can distinguish two main kinds of tasks: (i) administrative tasks, and (ii) monitoring tasks.

Administrative tasks are mainly related to the registration of users and patients into the system, the management of cryptographic keys, and the disclosure of information that requires the intervention of multiple parties. On the other hand, monitoring tasks are essentially focussed on the analysis of location information (and possibly some additional variables) with the aim to detect situations that could endanger the safety of the patients. In general, administrative tasks involve several actors (patients, users, servers, etc.) whilst monitoring tasks are essentially performed by the m-Carer running on the patients' devices.

In this section we describe two fundamental administrative tasks: the registration of patients and unofficial users (Section III-A), and the disclosure of information (Section III-E). Furthermore, we describe the three basic states of alarm (*i.e.* no alarm in Section III-B, non-critical alarm in Section III-C, and critical alarm in Section III-D) and the operations performed to guarantee the privacy and safety of patients in each state.

A. Registration of patients and unofficial users

To illustrate the registration operation of our system, let us suppose that an old people's home is offering the service (*e.g.* in our running example this is The Golden Yard). A patient (*e.g.* Mr. Oldsmith) and an unofficial user (*e.g.* Ellie) agree with an official user (*e.g.* Mrs Andrews) that the patient

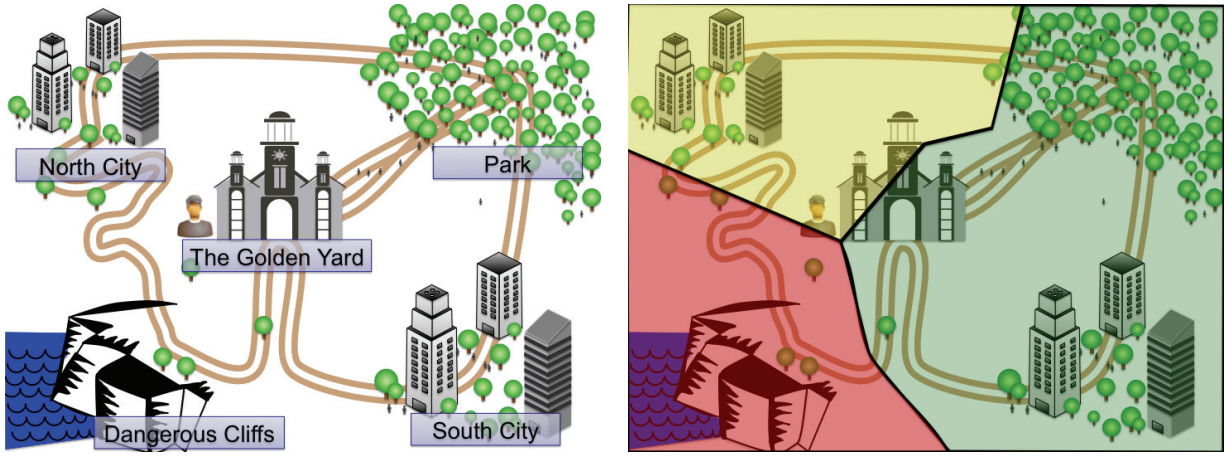

Fig. 3. **Left:** Illustration of the area surrounding The Golden Yard in our running example. **Right:** Areas defined by patients or users (in this case *Mr. Oldsmith* and his daughter *Ellie*). Green areas indicate allowed zones without risk, yellow areas indicate non-allowed zones (possibly risky), and red areas indicate dangerous zones that must be avoided.

is going to be under surveillance. Hence, the official user accesses the *Server of preferences* to register the new patient as well as one or more unofficial users related to the patient. During this procedure, the following actions take place:

1) The Server of preferences generates the cryptographic keys required by the system's protocols: a public/private key pair for the unofficial users $\{PK_{uu}, SK_{uu}\}$, a public/private key pair for the m-Carer running in the *Patient's Device* $\{PK_{pd}, SK_{pd}\}$ and a random encryption key K_{pd}. We assume that official users already have a public/private key pair $\{PK_{ou}, SK_{ou}\}$.
2) The initial conditions that lead to different alarm states are defined during this procedure (note that these conditions can be modified by the patient or the users at any time), as well as some other preferences. The following are the most significant parameters:
   - *Secure areas.* As long as the patients remain in these secure/allowed areas no alarm will be raised regarding the location of the patient.
   - *Non-allowed and dangerous areas.* When the patients enter those areas, the system raises an alarm. The type of alarm depends on the kind of area and it is fully customisable by the users.
   - *Health parameters.* A number of gadgets could be attached to the Patient's Device (*e.g.* via Bluethooth) so as to measure, for instance, the heartbeat frequency or the body temperature. Users might assign different states of alarm for different values of these measures.
   - *Frequency of messages.* This parameter defines how often a message containing location information (an possibly other) is sent to the *Location server*. Increasing this frequency benefits the resolution of the system at the cost of bandwidth usage.
3) Keys $\{SK_{pd}, PK_{uu}, PK_{ou}, K_{pd}\}$ and the m-Carer application are installed into the patient's device (*e.g.* the smartphone of Mr. Oldsmith).
4) Key PK_{pd} is sent to the *Location server* and it is associated to the *patient's device*.
5) Keys SK_{uu} and SK_{ou} are stored in the *Server of preferences*, protected by a password that is known only by the owners of the keys. Key K_{pd} is also stored in this server, and it is protected by a password known by all users related to the patient.

B. State of No Alarm (NA)

If the m-Carer running in the patient's device does not detect any of the alarm conditions defined, it periodically sends encrypted data to the *Location server*:

1) First, these data are encrypted with the public key of the *Unofficial user*, and the result is encrypted again this time with the public key of the *Official user*. In addition to these doubly encrypted data, the message contains a message authentication code (MAC):

$$\{\mathcal{ENC}_{PK_{ou}}(\mathcal{ENC}_{PK_{uu}}(data)), \mathcal{MAC}_{SK_{pd}}\}$$

2) The *Location server* stores the encrypted data and acknowledges the reception.

In our example, consider the locations 1 and 2 of the route of Mr. Oldsmith shown in Figure 4. In these points the m-Carer does not detect any alarm because Mr. Oldsmith is located in an allowed area that does not mean any risk to his safety. Hence, the m-Carer will take the current location of Mr. Oldsmith and will encrypt it first with the public key of Ellie and the result will be encrypted again with the public key of Mrs. Andrews. As shown in Figure 5, in this situation our system encrypts the location by using the RSA public key cryptosystem. However any other algorithm with the same security properties might be used.

C. State of Non-Critical Alarm (NCA)

If the m-Carer detects a *Non-Critical* alarm condition, it sends an encrypted alert to the *Location server*:

1) The location along with other data are sent from the patient's device to the *Location server* using a *Non-Critical Alarm* message that contains the data encrypted

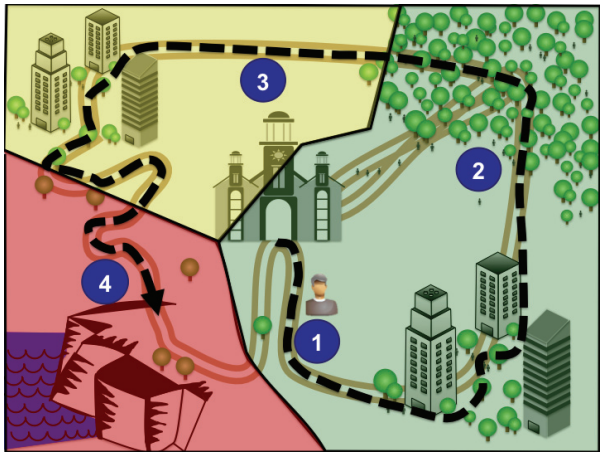

Fig. 4. Route followed by Mr. Oldsmith in our example. Circled numbers indicate different moments in the promenade of Mr. Oldsmith that are used to illustrate different alarm states.

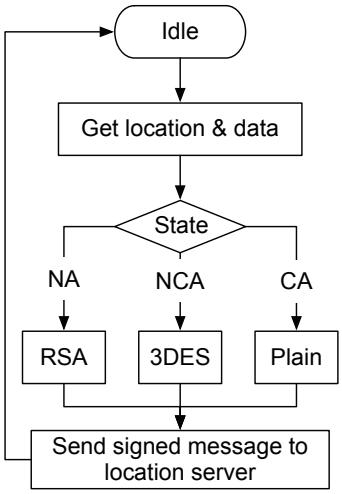

Fig. 5. Simplified task flow of the m-Carer. Initially the m-Carer determines the location of the patient. With this information and the one from other sensors, it determines the state of alarm and sends the messages encrypted accordingly.

with a symmetric key K_{pd}. A MAC is also added to the message to guarantee authenticity:

$$\{\mathcal{ENC}_{K_{pd}}(data), \mathcal{MAC}_{SK_{pd}}\}$$

2) Upon reception, the *Location server* forwards the message to all users related to the patient. Then, users can decrypt the message, since they know the symmetric key K_{pd}.

In our example, consider the location 3 in the route of Mr. Oldsmith shown in Figure 4. When the m-Carer analyses the location of Mr. Oldsmith at that point, it detects that he is located in a non-allowed area (marked in yellow). These areas do not represent a direct risk to the safety of the patient, but the fact that the patient is there might indicate that he is lost. In this situation the m-Carer sends the message described above to the *Location server* that forwards it to Ellie and Mrs. Andrews (*e.g.* they receive a warning message in their mobile phones). They can decrypt the message because they know the secret symmetric key K_{pd}. After decrypting the message Ellie and/or Mrs. Andrews may act accordingly. As shown in Figure 5, in this situation our system encrypts the location by using the 3DES symmetric key cryptosystem, however any other algorithm with, at least, the same security properties might be used (*e.g.* the Advanced Encryption Standard (AES) algorithm is an alternative).

D. State of Critical Alarm (CA)

If the m-Carer detects a critical situation (*e.g.* the patient is in a dangerous area, a fall has been detected, attached biosensors indicate a critical situation, etc.) it sends an unencrypted message to the *Location server* that forwards it to all users related to the patient. In addition, in parallel, the m-Carer sends a warning message to the *Emergency Services* informing about the location of the patient in clear text (*i.e.* no encryption is used).

In our example, consider the location number four of the route of Mr. Oldsmith shown in Figure 4. In this point, the m-Carer detects that Mr. Oldsmith is in a dangerous area (*i.e.* he is very close to a cliff). In this situation the safety of the patient is more important than his privacy, thus, the m-Carer automatically sends a warning message to the *Emergency services* (*e.g.* these can be public services or private services paid by The Golden Yard). Also, the m-Carer sends an unencrypted message with the location of Mr. Oldsmith to the *Location server* that immediately forwards it to Ellie and Mrs. Andrews. They will receive the warning in their mobile phones. In addition, the system can automatically make a distress voice call to warn them more reliably.

E. Obtaining information

As shown in the previous sections, depending on the alarm state, the m-Carer encrypts the location information differently. Thus, users have to use different procedures to decrypt the messages and obtain the information.

- If the message is sent under the *Critical Alarm* state, no encryption is used. Consequently, users receive the information in plain text and no further action is required on their side.
- In a *Non-Critical Alarm* state, messages are encrypted with a single symmetric key known by official and unofficial users related to the patient. Thus, they can individually decrypt the message by using the key K_{pd} as follows:

$$\mathcal{DEC}_{K_{pd}}\{\mathcal{ENC}_{K_{pd}}(data)\} = data$$

  Note that only these users will be able to decrypt the message. The *Location server* that stores and forwards the messages is not able to decrypt them. In this regard, the privacy of the patient is fully guaranteed.
- For messages encrypted during normal operation (*i.e.* in a *No Alarm* state), official and unofficial users **have to collaborate** to decrypt the information. First, an official user partially decrypts the message using SK_{ou} and sends the result (partially decrypted) to an unofficial user that uses SK_{uu} to obtain the fully decrypted information.

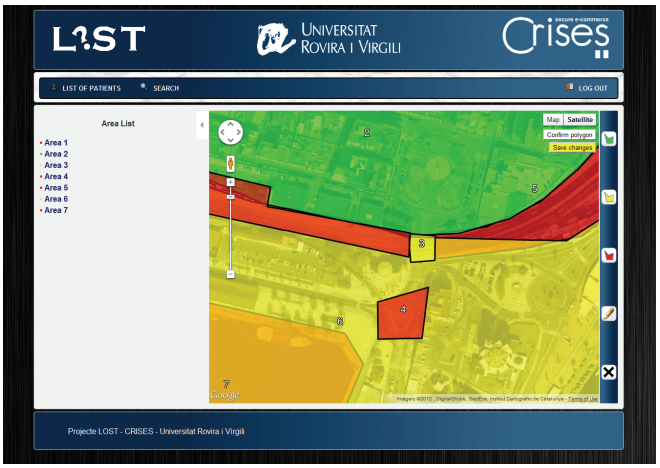

Fig. 6. Screenshot of the website used by users to define their preferences

$$\mathcal{DEC}_{SK_{ou}}\{\mathcal{ENC}_{PK_{ou}}(\mathcal{ENC}_{PK_{uu}}(data))\} = \mathcal{ENC}_{PK_{uu}}(data)$$
$$\mathcal{DEC}_{SK_{uu}}\{\mathcal{ENC}_{PK_{uu}}(data)\} = data$$

Note that neither official users nor unofficial users are able to obtain the information individually. Thus, the privacy of patients is guaranteed.

In our example, consider the location number two in the route of Mr. Oldsmith shown in Figure 4. Imagine that Ellie has to meet with this father but (for any reason) he has forgotten about the meeting. The m-Carer does not detect any risky situation because Mr. Oldsmith is located in an allowed safe area. Hence, it encrypts the location under the NA condition and sends it to the *Location server*. Ellie is worried and wants to know the location of her father. To do so, she contacts Mrs. Andrews and asks for her help to determine the location of Mr. Oldsmith. If they agree (let us assume that they do), Mrs. Andrews starts the decryption procedure by using her private key and sends the partially decrypted message to Ellie. Ellie receives this message and finalises the decryption using her private key and obtaining the location of his father.

Note that in this case in which no alarm is detected Mrs. Andrews (the official user) acts as a regulator to avoid the inappropriate use of the system. As a result the privacy of the Mr. Oldsmith is guaranteed.

IV. Real Implementation

In the previous sections we have described our m-Carer proposal from a theoretical perspective. In this section we provide a brief overview of a real implementation details of the system that is fully functional. This implementation has been done within the framework of "The LOST project" by a team of cryptographers and programmers of the CRISES Research Group at the Rovira i Virgili University in Spain. Note that this implementation is only a possibility. Several other options, based on the theoretical description given above, are also possible. Thus, the main goal of this section is not to deeply analyse the efficiency of the implementation but to show the feasibility of the proposal in the real world.

The communication protocols between users, patients and servers have been implemented in Java using a RESTful approach over HTTP. The web interface of the *Server of preferences* (shown in Figure 6) uses PHP, HTML and the Google Maps JavaScript API.

We have developed the m-Carer application that runs on the patient's device for the three main smartphones platforms, namely iOS, Android and Windows Mobile.

Regarding cryptography, we have used 3DES (Triple Data Encryption Standard) with 192-bit keys for the symmetric encryption and RSA with 1024-bit keys for the asymmetric/public-key encryption. Messages authentication codes (MAC) are obtained by using SHA-1 (Secure Hash Algorithm-1) and its RSA digital signature.

In addition, the battery life of the patients' devices has been tested in real life situations. For instance, using our m-Carer running on a Samsung Galaxy S with Android, the battery lasts for up to 62.5 hours (sending an encrypted location message every 5 minutes). Note that this result is only approximate and might vary depending on the operating system, the GPS chipset, the data network, and the smartphone used.

Currently, we are planning and realising several trials in Tarragona and Barcelona (Catalonia) with the collaboration of the City Council, the University and local associations of relatives of patients with Alzheimer. The trials will last for, at least, six months and we expect to collect data that will allow us to improve the system and to better understand the wandering behaviour of patients with dementia.

V. Previous Related Work

When patients with cognitive impairments wander away and get lost, they may have serious or even fatal accidents. This usual behaviour, known as *wandering*, is a common problem related to people with dementia, from which over 40% get lost outside their homes. To avert this situation carers supervise patients and keep them safe. However, this often requires to lock doors or preventing the patient from leaving in other ways such as constant surveillance or putting them on drugs [5] [6]. Unfortunately, these methods limit the sense of freedom of patients and could have negative effects on their well-being. To mitigate these undesired effects, imaginative solutions, like installing a fake bus stop [7] have been proposed. However, these solutions are only applicable to very specific situations and patients.

With the aim to provide patients with more freedom and autonomy, Miskelly proposed in [8] the use of mobile phones equipped with GPS to continuously track patients, so that it was possible to locate and assist them if necessary. Before using the system, each patient gave written informed consent. However, the main problem encountered by the researchers was user compliance. The system proposed by Miskelly introduces the promising idea of using mobile technology but the lack of privacy related to the "Big Brother" effect [9] prevents this proposal from being fully accepted. Nevertheless, some commercial applications like the Columba bracelet [10] use this idea.

Instead of tracking patients constantly, Casas et al. [11] suggested the idea of using "alarms". A system of alarms only informs about the location of patients when something goes wrong. The alarm can be raised by patients (active

alarm) or by wearable light devices when certain conditions are met (passive alarm). These conditions can be based on the location of patients (*i.e.* the alarm is triggered when a patient leaves a predefined perimeter, is near a dangerous area or is moving too fast) or based on the data of sensors, namely accelerometers [12], thermometers or heartbeat detectors [13]. Several commercial applications based on tracking and alarms are Urgentys [14], Simap [15] and GPS trackers [16]. These proposals, use both alarms and constant tracking. Note that although they use security and privacy methods such as deleting information, using Transport Layer Security (TLS), encrypting databases or using pseudonyms, none of them guarantee the privacy of the patients because users can ask for their location anytime, thus, deliberately invading their privacy.

Collaboration is paramount for many architectures that involve human beings. In [17], Ray et al. introduced the concept of awareness level as a measure of cooperation in the context of cooperative management and m-health. Other interesting examples of collaboration in the context of location-based services and tracking can be found in [18], [19], [20] and [21].

VI. Conclusions and Further Work

The number of people with mild cognitive impairment grows and it will keep growing in the future due to the ageing of our society. Most of these people are able to carry a normal life, however, they can get lost or disoriented in some occasions. In these situations, they could be injured and finding them rapidly is very important. Although there exist some proposals to locate people, none of them fully considers the privacy of the user. Thus, this lack of privacy protection might prevent patients from using these systems. There is a clear need for new proposals able to balance the right of patients to be properly treated and controlled and their fundamental right to privacy.

In this article, we have proposed the new concept of m-Carer. We have described a comprehensive architecture aimed at tracking people whilst guaranteeing their right to privacy. By using a set of personalised alarm states, relatives and human carers can easily find and help lost patients if necessary. With the aim to demonstrate the feasibility of our proposal we have implemented a fully functional solution, and we have shown that our proposal is practical and useful. Although our proposal will help patients, human carers and relatives, we recognise that nowadays it is impossible to substitute a human carer and there is still much work to do. The following are research lines that are going to be studied in the future so as to improve the m-Carer proposed in this article:

- Wandering detection: Patients can get lost within allowed areas, in this situation, the system would not detect any alarm. It is desirable to develop methods to determine whether a patient is wandering even within safe areas.
- Incremental learning of mobility patterns: The development of intelligent systems able to learn the movement patterns of patients might help to automatically adapt the allowed areas in which patients move.
- Integration with indoor systems: The concept of m-Carer is basically designed for outdoors (due to the constraints of GPS receivers). Thus, integrating m-Carers with indoor monitoring systems would lead to a comprehensive solution.
- Cellphone loss: Depending on the stage of the illness, patients might lose their cellphones. Determining the best way of carrying the cellphone to avoid its loss is still an open issue.
- Data integration: Cellphones are capable of gathering data from other devices via bluetooth or the like. However, the lack of well-known standards and the non-trivial nature of multiple sources data integration make this task very challenging and requires further consideration.

Acknowledgments

This work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-0004 ARES, project TSI2007-65406-C03-01 E-AEGIS, project TIN2011-27076-C03-01 CO-PRIVACY, project INNPACTO 2010 PT-430000-2010-31, project AVANZA I+D 2009 TSI-020100-2009-720, project AVANZA I+D 2010 TSI-020302-2010-153, and by the Government of Catalonia under grant 2009 SGR 1135, and by the Rovira i Virgili University through project 2010R2B-02 LOST?, and by La Caixa trough the program RECERCAIXA 2012. The authors are with the UNESCO Chair in Data Privacy, but the views expressed in this paper are their own and do not commit UNESCO. The authors would like to thank Jorge Carranza Vélez for the implementation of valuable parts of the system.

References

[1] R. Petersen, R. Doody, A. Kurz, R. Mohs, J. Morris, P. Rabins, K. Ritchie, M. Rossor, L. Thal, and B. Winblad, "Current concepts in mild cognitive impairment." *Archives Neurology*, vol. 58, no. 12, pp. 1985–1992, 2001.

[2] Vital Wave Consulting, "mhealth for development: The opportunity of mobile technology for healthcare in the developing world," UN Foundation-Vodafone Foundation Partnership, Tech. Rep., 2009.

[3] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *Eng. Medicine Biology Society, 2006. EMBS '06. 28th Annual International Conf. IEEE*, 30 2006-Sept. 3 2006, pp. 5453–5458.

[4] R. Heckle, "Security dilemma: Healthcare clinicians at work," *Security Privacy, IEEE*, vol. 9, no. 6, pp. 14–19, Nov.-Dec. 2011.

[5] R. McShane, K. Gedling, J. Keene, C. Fairburn, R. Jacoby, and T. Hope, "Getting lost in dementia: A longitudinal study of a behavioral symptom," *International Psychogeriatrics*, vol. 10, no. 3, pp. 253–260, 1998.

[6] J. C. Hughes and S. J. Louw, "Electronic tagging of people with dementia who wander," *British Medical J.*, vol. 325, pp. 847–848, 2002.

[7] Expatica Communications BV. (2008, June) Waiting for the bus that will never come. http://www.expatica.com/de/health_fitness/healthcare/Waiting-for-the-bus-that-will-never-come.html.

[8] F. Miskelly, "Electronic tracking of patients with dementia and wandering using mobile phone technology," *Age Ageing*, vol. 34, pp. 497–518, 2005.

[9] E. Kaasinen, "User needs for location-aware mobile services," *Personal Ubiquitous Compu.*, vol. 7, no. 1, pp. 70–79, 2003.

[10] Medical-Intelligence. Columba bracelet. http://www.medicalintelligence.ca/en/products/hardwares/prima/tech.html.

[11] R. Casas, A. Marco, J. L. Falco, H. Gracia, and A. Marco, "DALMA - Location Aware Alarm System for People with Disabilities," in *Comput. Helping People Special Needs*, ser. Lecture Notes in Comput. Science. Berlin - Heidelberg: Springer, 2006, vol. 4061, pp. 744–751.

[12] A. Marco, R. Casas, J. L. Falco, H. Gracia, J. I. Artigas, and A. Roy, "Location-based services for elderly and disabled people," *Comput. Commun.*, vol. 31, no. 6, pp. 1055–1066, 2008.

[13] M. N. K. Boulos, A. Rocha, A. Martins, M. E. Vicente, A. Bolz, R. Feld, I. Tchoudovski, M. Braecklein, J. Nelson, G. . Laighin, C. Sdogati, F. Cesaroni, M. Antomarini, A. Jobes, and M. Kinirons, "CAALYX: A new generation of location-based services in healthcare," *International J. Health Geographics*, vol. 6, no. 9, pp. 1–6, Mar. 2007.
[14] Medical-Intelligence. Urgentys. http://www.medicalintelligence.ca/en/products/hardwares/urgentys/tech.html.
[15] Vodafone (Spain). Simap. http://www.simapglobal.com/.
[16] People-Track-USA. GPS Monitoring Services for Alzheimer Patients and children with Autism. http://www.peopletrackusa.com/GPSTrackingofAlzheimerPatientsandAutismWanderers.html.
[17] P. Ray, N. Parameswaran, V. Chan, and W. Yu, "Awareness modelling in collaborative mobile e-health," *J. Telemedicine Telecare*, vol. 14, no. 7, pp. 381–385, 2008.
[18] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Comput. Commun.*, vol. 31, no. 6, pp. 1181–1191, 2008.
[19] A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté, and V. Daza, "A distributed architecture for scalable private RFID tag identification," *Comput. Netw.*, vol. 51, no. 9, pp. 2268–2279, 2007.
[20] R. Trujillo-Rasua and A. Solanas, "Efficient probabilistic communication protocol for the private identification of RFID tags by means of collaborative readers," *Comput. Netw.*, vol. 55, no. 15, pp. 3211–3223, 2011.
[21] R. Trujillo-Rasua, A. Solanas, P. A. Pérez-Martínez, and J. Domingo-Ferrer, "Predictive protocol for the scalable identification of RFID tags through collaborative readers," *Comput. Industry*, vol. 63, no. 6, pp. 557–573, 2012.

Agusti Solanas (Tarragona, Catalonia, Spain, 1980) is a researcher at the CRISES Research Group and the UNESCO Chair in Data Privacy in the Department of Computer Science and Mathematics at the Rovira i Virgili University (URV) of Tarragona, Catalonia, Spain. He received his B.Sc. and M.Sc. degrees in Computer Engineering from URV in 2002 and 2004, respectively,the latter with honours (Outstanding Graduation Award). He received a Diploma of Advanced Studies (Master) in Telematics Engineering from the Technical University of Catalonia (UPC) in 2006. He received a Ph.D. in Telematics Engineering from the Technical University of Catalonia in 2007 with honours (A cum laude). His fields of activity are privacy, security, clustering, neural networks and evolutionary computation. He has participated in several European-, Spanish- and Catalan-funded research projects. He has authored over 70 publications and he has delivered several invited talks. He has served as Chair, programme committee member and reviewer in several conferences and journals. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM).

Antoni Martínez-Ballesté received the M.Sc. in Computer Science and Engineering from Universitat Rovira i Virgili, (Catalonia, Spain, 2001), and Ph.D. degree in Telematics from Universitat Politcnica de Catalunya, (Catalonia, Spain, 2004). He is a tenured assistant professor at the Universitat Rovira i Virgili. His research interests are security and privacy in ICT and specially the privacy of their users. Since 2001, he is with CRISES research group where he has taken part in several research projects. Moreover, he is serving as vice-dean for Computer Science and Engineering and collaborates with the Universitat Oberta de Catalunya.

Pablo A. Pérez-Martínez (Lleida, Spain, 1985) is a Predoctoral Grant-holder at CRISES Research Group and at the UNESCO Chair in Data Privacy in the Department of Computer Science and Mathematics at Universitat Rovira i Virgili (URV) of Tarragona, Catalonia, Spain. He obtained his B.Sc. degree in Computer Science from the University of Lleida, and his M.Sc. in Computer Science and Security from Universitat Rovira i Virgili, currently Ph. D. student in CRISES Research Group, Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili. His main fields of interest are privacy and security in location-based services.

Albert Fernández de la Peña , born in Tarragona in 1990, obtained his bachelor's degree in Telecommunications from the Rovira i Virgili University in Tarragona (Catalonia, Spain). He is currently a master degree student at the Technical University of Denmark in Lyngby, Denmark.

Javier Ramos , born in Tarragona in 1989 holds a M.Sc. in Computer Security. His research interests are security and privacy. He is a member of the CRISES Research Group and the UNESCO Chair in Data Privacy in the Department of Computer Science and Mathematics at the Rovira i Virgili University (URV) in Tarragona (Catalonia, Spain).