A Generic Architecture for Integrating Health Monitoring and Advanced Care Provisioning

Koen Decroix, Milica Milutinovic, Bart Decker, Vincent Naessens

A generic architecture for integrating health monitoring and advanced care provisioning

Koen Decroix[1], Milica Milutinovic[2], Bart De Decker[2], and Vincent Naessens[1]

[1] Katholieke Hogeschool Sint-Lieven, Department of Industrial Engineering
Gebroeders Desmetstraat 1, 9000 Ghent, Belgium
firstname.lastname@kahosl.be
[2] K.U.Leuven, Department of Computer Science, DistriNet
Celestijnenlaan 200A, 3001 Heverlee, Belgium
firstname.lastname@cs.kuleuven.be

Abstract. This paper presents a novel approach for advanced personalized care and health services. It consists of four tiers and presents a high level of openness, privacy and manageability compared to existing systems. Moreover, the architecture is driven by realistic underlying business opportunities and is validated through the design of multiple scenarios.

1 Introduction

The average age of individuals is increasing significantly. Homes for the elderly are overcrowded and the government has trouble with financing the increasing costs and distributing the work load in those institutions. Moreover, studies show that elderly people are often reluctant to leave their houses. They prefer to stay at home as long as possible. Therefore, many European research initiatives have been bootstrapped in the past decade resulting in systems to monitor and assist the elderly remotely. A first flavor focuses on the development of monitoring technologies. For instance, body area networks consist of a set of wireless nodes that monitor health parameters of elderly. Examples are heartbeat and blood pressure sensors, fall detectors, etc. Also, systems can be installed in the patient's house to control access to his medical cabinet, to encourage him to physical practice, etc. A second flavor focuses on remote health or care services. Many existing architectures consist of three tiers: a set of sensors that generate sensor values, a base station that collects and eventually filters the data, and a care center that takes health related decisions and offers health services based on the received inputs. However, very high trust is required in care centers as they receive and store a lot of sensitive medical information about their users. Hence, care centers are often controlled by the government and lack openness. They typically offer a limited and fixed set of services based on sensor data. For instance, a fall detection camera can trigger an alert in the care center. However, the same camera could also be used for remote care services such as preserving social contacts, remote checks by doctors, etc. Hence, current approaches are

not user centric and the full potential of home monitoring equipment is not exploited. Moreover, they put up a barrier to the entrance of commercial service providers in the eHealth domain.

This paper presents a novel approach for advanced personalized care and health services based on both remote user input and sensor data. The key contribution is that our architecture - which consists of four tiers - presents a high level of openness, privacy and manageability. Moreover, we show that our approach is driven by realistic underlying business opportunities. It allows commercial service providers to penetrate in the eHealth domain.

The rest of this paper is structured as follows. Section 2 points to related work. The general approach is described in section 3. Section 4 focuses on architectural details. Section 5 evaluates the strengths and weaknesses of the current architecture and validates our approach through the development of three scenarios. This paper ends with general conclusions.

2 Related Work

Many research initiatives have been bootstrapped during the last decades in the domain of remote health monitoring. Many research only covers a subproblem and results are typically applied in a three tier architecture which consists of a set of sensors, a base station and a health center. At the sensor side, wireless sensor network protocols are embedded in health sensors. Many practical case studies mainly target to guarantee a minimal level of reliability and performance. For instance, [5] proposes a remote system for health care that consists of heterogeneous wireless sensors. The system applies an optimized IDL to enable communication between low resource platforms. In [9], the authors propose to use a wireless Personal Area Network (PAN) of intelligent sensors as a medical monitoring system architecture. The network is organized hierarchically and individual sensors monitor specific physiological signals (such as EEG, ECG, GSR,etc.). [15] describes a monitoring system for the elderly that provides alarm functionality. It consists of a wrist device detecting user indicated alarms.
Other research focuses on the development of gateways between sensors (or sensor networks) and a service provider. For instance, MobiCare [4] implements a body sensor network manager (BSNM) on a mobile client. Its major task consists of aggregating data from sensors and forwarding them to a health center or another predefined service provider. [12] describes a home server that offers services as OSGi bundles. This approach centralizes data processing and service provisioning in the home server. A similar architecture is applied for patient rehabilitation [8] and emergency situations [16]. Those solutions often lack flexibility and reliability. It is difficult to ensure a service level if the base station crashes or if a service provider is not available. TeleCARE [3] is a more flexible agent-based approach for building virtual communities around elderly people. Agents migrate to the sensors and base station to offer services. The authors claim that security and privacy are important concerns but these are not really tackled in the approach.

In other architectures, many tasks are performed at the care center. For instance, in [10], coordination, data analysis and service provisioning are performed at a central monitoring station. Hence, the user has no substantial control over the services that are deployed and over the information that is released to the care center. Therefore, very high trust is required in those care centers. [14] proposes an architecture for secure central storage of electronic health records (EHRs). The data are pseudonymized. Many research initiatives focus on privacy friendly storage of data. Our architecture does not explicitly focus on EHR storage. It merely focuses on enabling services based on technical means installed in the home environment of elderly people. However, anonymous storage technologies like [6][7] can be foreseen in our platform. Another research flavor that is complementary with our contribution are interoperability initiatives. [11] shows the possibility of interoperability between two standards, namely HL7 and IEEE 1451. HL7 is a messaging standard for exchanging medical information. IEEE 1451 deals with various aspects of sensors, the format of data sheets and how to connect and disconnect the sensors from a system. This work is complementary to our research. These standards can be used to exchange information between entities in our architecture.
Multiple European initiatives also focus on remote eHealth provisioning. epSOS [1] is European project for patient summary and electronic prescription that interconnect national solutions. It develops an eHealth framework and ICT infrastructure that enables secure access to patient's health data. In contrast to this project, our approach is more oriented towards health and care services. MobiHealth [13] develops an architecture for patient monitoring. The framework consists consist of a Body Area Network (BAN) with sensors that collect data from a patient. Data is sent along with video and audio via a cellular network (2.5G and 3G technology) to a healthcare center. This raises major privacy concerns. BraveHealth [2] proposes a patient centric vision to CVD management and treatment, providing people already diagnosed as subjects at risk with a sound solution for continuous and remote monitoring and real time prevention of malignant events.

3 General Approach

Flexibility and reliability are key concerns of our architecture. To increase *flexibility* and *reliability* compared to existing systems, our architecture introduces a dispatch center as an essential component. The dispatch center mediates between the infrastructure installed at the elderly's homes (i.e. a base station and sensors/actuators) and at the service providers, and closes contracts with them. A contract between a patient and a dispatch center defines a set of services that can be consumed by the patient at a (recurrent) fee. Some services are handled by the dispatch center. For instance, the dispatch center detects and handles failures in the user's base station. Other services are forwarded to external service providers. The dispatch center therefore closes contracts with companies. For instance, the former can negotiate and fix contracts with multiple catering

companies. They are responsible for delivering food to elderly people that registered for that service. Similarly, the dispatch center collaborates with hospitals. An emergency call sent out by a base station is forwarded by the dispatch center to a hospital that can handle the call.

Privacy is another major concern in our approach. This is realized by a clear separation of duties. The dispatch center is responsible for discovering and assigning service providers upon a user's request. However, registered users can submit service requests anonymously (if they paid for that particular service). Hence, the dispatch center does not know which user requested a particular service at a given time (and cannot even link multiple anonymous requests of the same individual). The base station only sends minimal information that is required to select an acceptable service provider. For instance, when an elderly person wants to use a catering service, he passes his city (or region) to the dispatch center. Based on that information, the dispatch center can contact a nearby catering provider. Similarly, if the patient wants to be remotely consulted by a specialist, he only needs to submit the type of specialist he wants to the dispatch center. When closing a contract with an individual, the dispatch center defines what personal information is required for selecting an acceptable service provider. Moreover, the patient can optionally release personal preferences. For instance, he may submit a set of unwanted specialists together with a remote consultation request.

Multiple mechanisms are foreseen to *control access to personal attributes*. First, the user can define personal privacy preferences in his base station. If a dispatch center or service provider requests sensitive information, the user's consent is required (except in case of an emergency). Second, the dispatch center issues a certificate to each service provider he relies on. It contains the set of information that the user's base station may release for that service. For instance, a general practitioner may inspect values generated by body sensors during a remote consultation while a catering provider can only request the user's address. The dispatch center can also intervene in case of *disputes*. For instance, a user can argue that the service provider does not meet a predefined service level. To solve disputes, the dispatch center stores the contracts he has made with users and service providers. Moreover, base stations and service providers can store a secure anonymous backup of evidence at the dispatch center.

It is also clear that this approach presents a higher degree of *openness* than existing three tier solutions. The base station does not need to be updated if new service providers (f.i. catering providers, cardiologists, etc.) are connected to the dispatch center. Similarly, the dispatch center does not need to know if new sensors or actuators are installed in the user's house. Moreover, our approach is holistic in the sense that both occasional health and recurrent care services can be supported. Finally, strong privacy guarantees imply that commercial companies can enter the eHealth domain. The dispatch center is mainly involved in discovery and coordination. Hence, sensitive personal information is hidden from them.

4 Architectural details

This section gives an overview of major actions in the system. It shows that the architecture presents a high degree of flexibility and openness to support new elderly users and service providers. Figure 1 depicts the registration and service consumption actions.

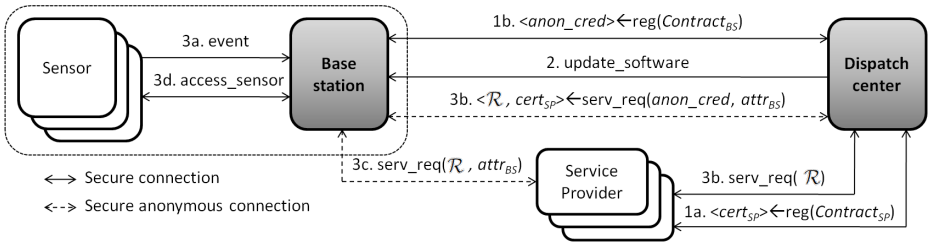

Fig. 1. Registration action and service consumption action

Registration Both elderly people and service providers need to enroll with the dispatch center. The service provider defines the types of services it can offer and defines constraints on the services. Examples are capacity and region constraints. For instance, a catering service can offer up to 500 meals a day within one or more regions. Moreover, it defines the set of attributes that are required from the elderly to fulfill the service request. These refer to personal information that need to be released by the elderly. For instance, catering services need to know the user's address and diet constraints. Similarly, an emergency team needs to know the user's address and a (temporary) code to enter the house. The negotiation results in a contract between the dispatch center and the service provider. At this phase, the service provider receives a certificate that contains – besides service-specific information – a set of personal information the service provider is entitled to request from the user. Different types of contracts are possible. Either the service provider pays a fee to the dispatch center each time a service request is handled, or vice versa. The former implies that the patient pays to the service provider. The latter results in a payment between the user and the dispatch center.

Similarly, users enter a contract with the dispatch center and receive a base station at registration. The contract defines a set of services that can be requested from the dispatch center. Some services are handled by the dispatch center itself. A typical example is failure detection of base stations and support to fix failures within an agreed upon time. The dispatch center acts as mediator for other services. The contract defines (a) the data that must be released to the dispatch center to select an appropriate service provider and (b) the data that must be released to the service provider. During enrollment, the user receives an anonymous credential with capabilities to consume the requested services.

Service consumption The user's base station keeps track of a set of events that can trigger a service request. Multiple simultaneous requests are handled in priority order. Both (aberrant) sensor data and user input can lead to a service request. For instance, if a heart beat rate threshold value is exceeded an alert is initiated. A user can also input a set of dates at which he wants to receive meals from a catering provider. It is clear that the former request will have a higher priority. The base station first sets up an anonymous connection to the dispatch center. It uses the anonymous credential to prove that it has the right to consume the service and releases the personal information that is required to allow for an acceptable service provider. The dispatch center establishes a secure and mutually authenticated channel with an acceptable service provider and returns the server certificate to the base station. Moreover, it generates a secure random $\mathcal{R}$ that is sent to the service provider and the base station. Next, the base station establishes a mutually authenticated anonymous channel with the service provider. Both entities prove to have knowledge of $\mathcal{R}$. The base station further needs to prove the elderly person's identity and/or release a set of information required to consume the service. Moreover, it can provide access to a set of sensors and/or actuators that are bound to the base station.

Logging and dispute handling Users can log both `history` (such as values generated by sensors) and `evidence` of interactions with service providers at the dispatch center. Central logging increases reliability. Moreover, the storage component allows users to store encrypted data that can be disclosed conditionally by third parties. For instance, values generated by sensors can be consulted by doctors while evidence can be decrypted by juridical instances to solve disputes.

5 Evaluation and validation

The proposed architecture meets the privacy requirements of many users. Service requests initiated by the same user remain anonymous and even unlinkable towards the dispatch center. At communication level, anonymous channels are used. At application level, anonymous credentials are used to access services. Moreover, the user only releases the minimal information necessary to consume the service. This implies that users can even remain anonymous (or pseudonymous) for some services. For instance, an external health center can continuously analyze data generated by sensors. The sensor data can be sent by the base station over an anonymous channel. However, to increase the business potential of our approach, multiple payment schemes must be supported. Either the user can (pre-)pay for a set of services to the dispatch center or pay per service request to the dispatch center or service provider. The strategies can also be combined. For instance, a user can pay a monthly fee to the dispatch center for a service package. Possibly, an additional fee must be paid per emergency request to the dispatch center and to the involved entities (e.g. general practitioner, hospital). Therefore, anonymous payment methods must be supported.

For the validation, three services are prototyped in the first iteration. They They show that a wide variety of services can be supported by the architecture.

The sensor functionality is implemented on SUNSPOT sensors. A Java Virtual Machine runs on the sensors. A middleware layer is implemented to support more advanced communication between the sensors and the base station. The communication middleware consists – amongst others – of a security component to enable secure communication. The Bouncy Castle crypto libraries are instantiated on the SUNSPOT sensors for that purpose. Two sensors are currently configured, namely (1) a fall detection sensor that uses the built-in accelerometer and (2) a sensor that contains buttons to initiate an alert (or emergency) procedure. Moreover, the base station can switch on a video camera and forward video streams to a general practitioner if certain conditions are fulfilled. Finally, the patient can communicate with service providers using a terminal.

Three types of services are currently implemented, namely (1) daily care provisioning services, (2) infrequent health provisioning and (3) statistical analysis. We only give a short of overview of each of these services due to space limitations. Daily care provisioning services are related to tasks for which elderly people need support. Examples are washing, cleaning the house, cooking meals, etc. The patient uses his terminal to specify one-time or recurrent tasks. In that scenario, the dispatch center discovers appropriate service providers based on the user's preferences. The patient only proves that he may request the service while remaining anonymous towards the dispatch center. Moreover, the dispatch center cannot link multiple service requests to the same individual. The second scenario initiates an alert (or emergency procedure) if a fall is detected. The patient can cancel the procedure by pushing the right sensor button. Otherwise, a remote health care provider can switch on the user's camera and take appropriate steps. In the third scenario, researchers can retrieve anonymized data from the base station to enable statistical analysis. The owner of a base station can configure which data he is willing to release. He may get discount vouchers for some services if he enables that service.

6 Conclusion

This paper presents an architecture for advanced home care provisioning. Privacy, security and openness were key properties during the design phase. Moreover, the architecture enables commercial entities to enter the eHealth domain. In the first iteration, three services with alternative security and privacy requirements have been developed. Future work will evolve in many directions. First, more advanced scenarios will be designed and included. Second, advanced payment and contracting schemes will be added. A final challenge targets the compatibility with the Belgian eHealth platform. It gives access to medical records (mainly stored by non-commercial health providers). Commercial service providers can benefit of controlled release of such data to increase the quality of service.

Acknowledgement This research is partially funded by the Interuniversity Attraction Poles Programme Belgian State, Belgian Science Policy, and by the IWT-SBO

project (DiCoMas) "Distributed Collaboration using Multi-Agent System Architectures".

References

1. epsos - european patients - smart open services. http://www.epsos.eu/, 2008-2011.
2. Bravehealth. http://www.ctit.utwente.nl/research/projects/international/fp7-ip/bravehealth.doc, 2011.
3. L. M. Camarinha-matos and H. Afsarmanesh. Design of a virtual community infrastructure for elderly care. In *Collaborative Business Ecosystems and Virtual Enterprises*, pages 439–450. Kluwer Academic Publishers, 2002.
4. Rajiv Chakravorty. A programmable service architecture for mobile medical care. In *Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, PERCOMW '06, pages 532–, Washington, DC, USA, 2006. IEEE Computer Society.
5. J.M. Corchado, J. Bajo, D.I. Tapia, and A. Abraham. Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare. *Information Technology in Biomedicine, IEEE Transactions on*, 14(2):234 –240, march 2010.
6. Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Gerardo Pelosi, and Pierangela Samarati. Preserving confidentiality of security policies in data outsourcing. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, WPES '08, pages 75–84, New York, NY, USA, 2008. ACM.
7. Liesje Demuynck and Bart De Decker. Privacy-preserving electronic health records. In *Communications and Multimedia Security*, volume 3677, pages 150–159, 2005.
8. Emil Jovanov, Aleksandar Milenkovic, Chris Otto, and Piet de Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and Rehabilitation*, 2(1):6, 2005.
9. Emil Jovanov, Dejan Raskovic, John Price, John Chapman, Anthony Moore, and Abhishek Krishnamurthy. Patient monitoring using personal area networks of wireless intelligent sensors. *Biomedical Sciences Instrumentation*, 37:2001, 2001.
10. HyungJun Kim, Bart Jarochowski, and DaeHyun Ryu. A proposal for a home-based health monitoring system for the elderly or disabled. 4061:473–479.
11. Wooshik Kim, Suyoung Lim, Jinsoo Ahn, Jiyoung Nah, and Namhyun Kim. Integration of ieee 1451 and hl7 exchanging information for patients sensor data. *Journal of Medical Systems*, 34:1033–1041, 2010. 10.1007/s10916-009-9322-5.
12. I. Korhonen, J. Parkka, and M. Van Gils. Health monitoring in the home of the future. *Engineering in Medicine and Biology Magazine, IEEE*, 22(3):66 – 73, may-june 2003.
13. European MobiHealth Project. http://www.mobihealth.org, 2002-2004.
14. Bernhard Riedl, Veronika Grascher, and Thomas Neubauer. A secure e-health architecture based on the appliance of pseudonymization. *Journal of Software*, 3(2):23–32, 2008.
15. A. Sarela, I. Korhonen, J. Lotjonen, M. Sola, and M. Myllymaki. Ist vivago reg; - an intelligent social and remote wellness monitoring system for the elderly. In *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on*, pages 362 – 365, april 2003.
16. A. Wood, J. Stankovic, G. Virone, L. Selavo, Zhimin He, Qiuhua Cao, Thao Doan, Yafeng Wu, Lei Fang, and R. Stoleru. Context-aware wireless sensor networks for assisted living and residential monitoring. *Network, IEEE*, 22(4):26 –33, july-aug. 2008.