Privacy-Enhanced Management of Ubiquitous Health Monitoring Data

George Drosatos
Dept. of Electrical and Computer Engineering
Democritus University of Thrace
University Campus, 67100 Xanthi, Greece
gdrosato@ee.duth.gr

Pavlos S. Efraimidis
Dept. of Electrical and Computer Engineering
Democritus University of Thrace
University Campus, 67100 Xanthi, Greece
pefraimi@ee.duth.gr

ABSTRACT

In this paper, we propose a new architecture for managing data in a Ubiquitous Health Monitoring System (UHMS). The purpose of this architecture is to enhance the privacy of patients and furthermore to decongest the Health Monitoring Center (HMC) from the enormous amount of biomedical data generated by the users' wearable sensors. This is achieved by using personal agents that receive and manage the personal medical data of their owners. A component implementing the appropriate level of intelligence can be plugged-in into the personal agent and continuously analyze the raw health data. In case of an aberration detection the component may alert the HMC to initiate a more thorough examination of the possible emergency. Finally, we discuss how the personal agents can support privacy-preserving distributed computations.

Categories and Subject Descriptors

H.4.m [**Information Systems Applications**]: Miscellaneous—*Health data*; K.4.1 [**Computers and Society**]: Public Policy Issues—*Computer-related health issues, Privacy*; J.3 [**Computer Applications**]: Life and Medical Sciences—*Medical information systems*; I.2.11 [**Artificial Intelligence**]: Distributed Artificial Intelligence—*Multi-agent systems*

General Terms

Ubiquitous Health Data Privacy

Keywords

Privacy, Personal Data Management, Ubiquitous Health Data, Personal Agents, Biomedical Data.

1. INTRODUCTION

The necessity to provide health care to special groups of people who have the need of continuous health monitoring is an integral part of today's society. The aging of the populations constitutes a social and economical challenge for the whole world. Related researches which have been carried out both in the United States [9] and the European Union [13], indicate that the number of people over the age of 65 is increasing; a similar increase is estimated that will be observed throughout the developed world. On the other hand, many elderly people suffer from chronic diseases that require health care and frequent visits to hospitals. For people of this category, it is important to continuously monitor the state of their health. Effective monitoring of the health state can improve the quality of the patients' life or even save their life, while simultaneously reducing the cost of health care.

The rapid development of the wearable sensors technology led to the appearance and the implementation of prototype Ubiquitous Health Monitoring Systems (UHMS's) [11, 4, 12]. The objective of a UHMS is to provide continuity of ubiquitous health monitoring, both at home and outside of it. People need to have their health condition under control not only when at home, but wherever they are. One of the main features of a UHMS is to automatically generate alerts to notify the family or the patient's doctor about a possible health emergency so that they should rush to their help to him. Example of the data used for the detection of a possible malfunction, as they are reported in [2], is: heart rate, blood pressure, galvanic skin response, skin temperature, heat flux, subject motion, speed and the covered distance.

Health data are sensitive personal data of patients. Privacy-related legislation like the European Data Protection Directive [6] and the HIPAA (Health Insurance Portability and Accountability Act) [1] explicitly define the rules for protecting the privacy of patients. The so far general architecture of a UHMS requires that all personal medical data (such as those reported above) which are produced by the patients' wearable sensors are collected and stored in a central service, specifically at the Health Monitoring Center (HMC) [11, 4]. The HMC is responsible not only for the collection and storage, but also for the control of these extremely critical personal data. However, this technique runs significant risks as for the security of the actual data as for the privacy of the monitored people, and moreover has an enormous computational and storage cost for the HMC. Our proposed architecture suggests the decentralization of the collection of medical data at the users' side. This is achieved by the use of personal agents that will be continuously online and collect the medical data of their owners. In addition to the data that are obtained by wearable sensors, the agents are de-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

PETRA'11, May 25 - 27, 2011, Crete, Greece.
Copyright © 2011 ACM ISBN 978-1-4503-0772-7/11/05 ... $10.00

sirable to dispose other data such as demographic elements about the patient and further information about his health records, as well.

Apart from the management of the personal data, the patient agent's automatically monitors the different changes in medical data with a dedicated health component. As soon as the health component detects aberration in the raw health data, it informs the HMC by giving it access to the user's data so as to decide itself for the danger of the situation. The usage of the agents does not in any case block the remote monitoring of the patient's health by his personal doctor in regular time intervals, but it only ensures the controlled access.

The personal data management approach proposed in this work achieves a number of advantages in comparison with the existing architecture of a UHMS, and simultaneously enhances the privacy of the patients in such a system. More analytically, some of the advantages are:

- The whole history of medical data can be kept in the agent, whereas this might not be possible on the HMC due to practical reasons.
- Decongestion of the HMC from the large amount of data. This keeps the computations requirements for the central servers at a low level.
- Less risk of theft of personal data since they are distributed at the users' side.
- Only controlled access to the health data is provided and every data access is logged by keeping who retrieved which data items and when this happened.
- Usability of these data by third independent services or for performing distributed computations.

The main requirement is that each patient must have a personal agent at his disposal. Its cost will not be high due to small computational requirements for its operation.

The rest of this paper is organized as follows. In Section 2, we describe related work. In Section 3, we introduce the general architecture of our model. In Section 4, we discuss possible privacy preserving distributed computations using the medical data which are available to agents. Conclusions and directions for further research are given in Section 5.

2. RELATED WORK

Personal data of users are commonly stored in central databases at the service provider's side. In this way, the users have essentially no control over the use of their personal data. To address privacy concerns, different kinds of frameworks that are related to personal data have recently been proposed. See for example [10, 5] and the references therein. Moreover, general surveys on privacy enhancing technologies are given for example in [8, 7].

Of particular interest to this work is the Polis platform presented in [5]. Polis is a framework for the management of personal data and its aim is the protection of personal data. The basic principle upon which its operation is based is that each individual has absolute control on his personal data, which remain at the side of their owner and constitute his personal fortune. Each user of Polis is represented as a unique entity which is represented by a Polis agent. The Polis agents constitute the backbone of the Polis architecture; they are used to manage the personal data of an entity and provide controlled access at the entity's data. The service providers request personal data items of users from their personal agents. The agents provide the requested data if there is a corresponding license agreement (policies).

In this work, we actually suggest the use of the Polis agents for the management of the patients' personal data. However, it is essential to add some extra features that are required for their integration into a UHMS, to them.

3. ARCHITECTURE

In this section, we describe the proposed architecture and how it fullfils the goals of protecting the personal data and the privacy of the patient. The emphasis of the description is on the part of personal agents. An overview of the architecture for a UHMS is presented in Figure 1.

The biomedical data that are produced by the patients' wearable sensors are wirelessly collected through a local wireless network in the patient's body into a personal mobile device, such as a smart phone. Afterwards, the measured biomedical data are transmitted via multiple complementary wireless networks (GPRS, 3G, Wi-Fi), through the Internet, towards the patient's personal agent. The personal agents that are used for this task are the Polis agents and have been suitably modified for this purpose. The features which have been added to the Polis agents so as to be used in a UHMS are:

1. Ability to collect dynamic personal data, such as the biomedical data of the patients' wearable sensors.
2. Ability to control the values of the biomedical data for the detection of some indicative cases of emergency.

A snapshot of a patients' personal agent is shown in Figure 3. On the other hand, the patients' personal agents are self-organized into an appropriate virtual network topology that can provide easy organization and identification of the agents. This network topology can be used as a tool to conduct privacy-preserving distributed computations.

The health component of the personal agent checks automatically the incoming vital signs with the purpose to address for further thorough check in HMC if there are indications of an emergency. If necessary, the HMC can be consulted by the personal doctor of the patient. The personal doctors are shown as “Doctors” in Figure 1. Depending on the situation, the HMC can coordinate the immediate medical service at the closest or most appropriate local medical facility using the best available transportation service (e.g.: ambulance). Finally, an additional responsibility of the HMC is to inform the family of the patient about his condition so that they could rush to provide their help to the patient.

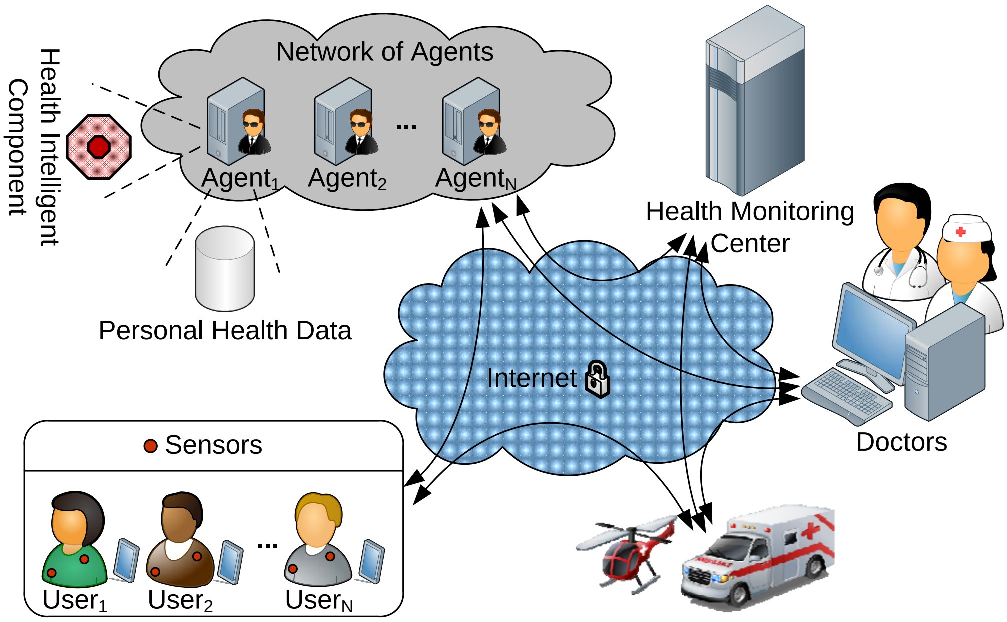


Figure 1: The proposed architecture for a UHMS.

4. DISCUSSION

The idea of a decentralized architecture for storage and control of the patients' medical data into their personal agents, as it has already been mentioned provides the advantage of enhanced control on the user's personal data. This grants to the patient the right to control the disclosure of his health data and mitigates its feeling of being under permanent surveillance. In addition to enhancing privacy, the decongestion of HMC from the huge amount of data that would be accepted if the patients sent their data directly to it, is achieved. Even in the case that the data would be collected at the HMC, these would be much less in volume than those that would actually be produced by the sensors, thus the analysis would not be as effective as the one that would be made by the agents themselves by having the complete data. With the proposed health data management approach of this work, the HMC has now to handle only those cases which may be at a certain risk. In case that the patient's agent is out of operation, the patient's data which are collected by his smart phone could be transmitted for storage and control directly to the HMC until the failure is restored. This will ensure fault-tolerance against possible agent failurer.

It is noteworthy that storing health data at the patients' side does not exclude the possibility to access the data from a central database as long as the database is entitled to do so. As shown in [5], the personal agents of Polis can be interconnected with mainstream database servers to provide transparent access to the personal data fields (Figure 2). The basic idea is that personal data fields in the central database do not contain the actual data; instead, a ticket represented by an appropriate data object is used to retrieve the data value on the fly. This approach was tested with an Oracle database server.

```
SQL> Select IDPatient ,TimeStamp ,BodyTemperature ,
     HeartPulses From CurrentBiomedicalData
     Where IDPatient = 142127;
```

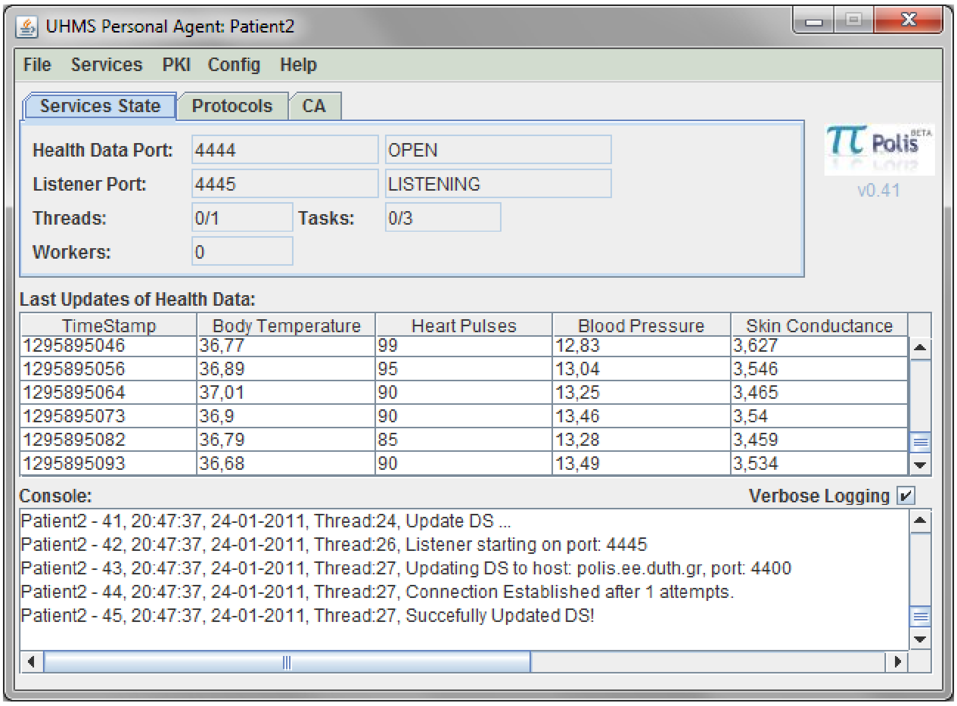
IDPatient	TimeStamp	BodyTemperature	HeartPulses
142127	1295895093	36.68	90

Figure 2: SQL access to remote health data.

From the moment that the patient's data are located in an agent the ability to utilize these data for the common wealth is given. The Nearest Doctor Problem (NDP) [3] is mentioned as a typical example. The NDP is a privacy-preserving protocol, which uses a network of the doctors' agents aiming to find the nearest doctor at an emergency, by using dynamic data such as their location. In our case, the data of the patients could be used for a similar privacy-preserving distributed computation. Such an example is the monitoring progress/spread of a pandemic in a region. Data such as the location and the body temperature of the patients would be required for this example. Furthermore, another example would be a medical statistical research on the biomedical data of the wearable sensors as well as on the medical records of patients. We are currently working on privacy-preserving distributed statistics within large communities of personal agents.

5. CONCLUSION

The tendency of the society towards increasing numbers of elderly people and generally people who need continuous health monitoring makes imperative the need of Ubiquitous Health Monitoring Systems. At the same time the concerns of the public about privacy are also rising. For this reason we proposed an architecture for privacy-enhanced UHMS that allows the patients to have enhanced control over their personal data, so as not to have the feeling of being continuously under surveillance. The enhanced control on their



Health Data Port: 4444 OPEN

Listener Port: 4445 LISTENING

Threads: 0/1 Tasks: 0/3

Workers: 0

Last Updates of Health Data:

TimeStamp	Body Temperature	Heart Pulses	Blood Pressure	Skin Conductance
1295895046	36,77	99	12,83	3,627
1295895056	36,89	95	13,04	3,546
1295895064	37,01	90	13,25	3,465
1295895073	36,9	90	13,46	3,54
1295895082	36,79	85	13,28	3,459
1295895093	36,68	90	13,49	3,534

Console: Verbose Logging ☑

```
Patient2 - 41, 20:47:37, 24-01-2011, Thread:24, Update DS ...
Patient2 - 42, 20:47:37, 24-01-2011, Thread:26, Listener starting on port: 4445
Patient2 - 43, 20:47:37, 24-01-2011, Thread:27, Updating DS to host: polis.ee.duth.gr, port: 4400
Patient2 - 44, 20:47:37, 24-01-2011, Thread:27, Connection Established after 1 attempts.
Patient2 - 45, 20:47:37, 24-01-2011, Thread:27, Succefully Updated DS!
```

Figure 3: A snapshot of UHMS personal agent.

personal data was achieved by using personal agents for the management of the patients' personal data. The existence of the agents opens the way for the creation of new services for the public well-being, which use and simultaneously ensure the patients' personal data.

6. REFERENCES

[1] 104th U.S. Congress. Health insurance portability and accountability act. In *Public Law 104-191*. Aug. 21, 1996.

[2] F. Camous, D. McCann, and M. Roantree. Capturing personal health data from wearable sensors. In *Proceedings of the 2008 International Symposium on Applications and the Internet*, pages 153–156, Washington, DC, USA, 2008. IEEE Computer Society.

[3] G. Drosatos and P. S. Efraimidis. A privacy-preserving protocol for finding the nearest doctor in an emergency. In *Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments*, PETRA '10, pages 18:1–18:8, New York, NY, USA, 2010. ACM.

[4] A. Durresi, A. Merkoci, M. Durresi, and L. Barolli. Integrated biomedical system for ubiquitous health monitoring. In *Proceedings of the 1st international conference on Network-based information systems*, NBiS'07, pages 397–405, Berlin, Heidelberg, 2007. Springer-Verlag.

[5] P. S. Efraimidis, G. Drosatos, F. Nalbadis, and A. Tasidou. Towards privacy in personal data management. *Journal on Information Management & Computer Security*, 17(4):311–329, 2009.

[6] European Parliament. Directive 95/46/EC. *Official Journal L 281*, pages 0031–0050, 24 October 1995.

[7] I. Goldberg. Privacy-enancing technologies for the internet iii: Ten years later. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, editors, *Chapter 1 of Digital Privacy: Theory, Technologies, and Practices*. December 2007.

[8] J. Hong. *An Architecture for Privacy-Sensitive Ubiquitous Computing*. PhD thesis, University of California at Berkeley, Computer Science Division, Berkeley, 2005.

[9] G. Huang. Monitoring mom: As population matures, so do assisted-living technologies. In *Technical Review 20*, July 2003.

[10] G. Lioudakis, E. Koutsoloukas, N. Dellas, N. Tselikas, S. Kapellaki, G. Prezerakos, D. Kaklamani, and I. Venieris. A middleware architecture for privacy protection. *Comput. Networks*, 51(16):4679–4696, 2007.

[11] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov. System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring. *Journal of Mobile Multimedia*, 1:307–326, January 2006.

[12] A. Yamazaki, A. Koyama, J. Arai, and L. Barolli. Design and implementation of a ubiquitous health monitoring system. *Int. J. Web Grid Serv.*, 5:339–355, December 2009.

[13] A. Zaidi. Features and challenges of population ageing: The european perspective. In *This Policy Brief is derived from the presentation made at the Social and Economic Council of Spain (CONSEJO ECONOMICOY SOCIAL, CES, Madrid), as their keynote speaker in the conference "Ageing of Population"*. European Centre for Social Welfare Policy and Research, 2008.