Personalized and Adaptable mHealth Architecture

Abbas Siddiqui * Oliver Koch* Ahmad Rabie* Uwe Handmann*
* Department of Computer Science
University of Applied Sciences Ruhr West
Bottrop, Germany
Email: abbas.siddiqui, oliver.koch, ahmad.rabie, uwe.handmann@hs-ruhrwest.de

***Abstract*—Health monitoring is a field where one's health condition (i.e., vital signs) is continually measured so that appropriate action(s) can be taken once an irregularity is found. However, a patient vital sings are highly individual based on various factors such as age, gender, weight, environment, daily activities, and medical conditions. Thus, a generalized mHealth solution can not satisfy the needs of all the users. In this paper, a mHealth architecture is presented which can be configured to individual user needs and demands.**

***Keywords*—Flexibility, Architecture, mHealth, Privacy, Security, Context, Biometrics, Mobile WebService**

I. INTRODUCTION

The Technological boom in the industrial countries is the reason behind the thriving economy of those countries. Thus, the people of the industrial countries can grow in a welfare society. Nonetheless, technological advancement is not only found its success in the industries, but also in the field of health, which facilitates the people to live longer than their ancestors.

But, all of the economical flare has its own price to pay, such as the growing market requires overzealous engagement of their workers to push forward the growth which leaves them with less time to socialize and cherish the family life. Consequently, the birthrate in those societies is declining drastically, which brings forth the issues of supporting the currently running system in the coming years, besides, supporting the growing relatively elderly population. Living longer may not be beneficial unless carried out in a good health (i.e., to be able to look after oneself). As many of the industrial societies have free health care system or in other cases an obligatory health insurance system, which insures the well-being of individuals of the society. Unfortunately, the older age poses the higher health risks, and having a large elderly population means higher pressure on the health care system, in addition to, resources exhaustion to support all of those people.

Active aging is about everyday monitoring of one's health, so that prevention can be under taken once a threat to the health is identified. In order to have a comprehensive health monitoring, various bio-sensors are attached to a user's body to record the vital signs. The recorded data can be enriched by tagging the information of the surroundings and the circumstances in which data is recorded. To accumulate the real time values of one's health, the time span for the measurements must be kept short. But if the measurements are captured in short intervals, it can result in a huge amount of data and eventually, over a period of time, it can be turned into complex and massive database.

The individuality is not limited to the sensor data, but also to the user who is using it. Which bring us to the second issue which is related to the customization of the mHealth solution. Vital sings measurement of every use differ significantly depending on the factors such as age, sex, weight, environment and, medical conditions. Our main objective is to use the available resources efficiently in mHealth context and to protect the user privacy.

Problem Statement: The diversity of the mHealth users is the reason that one-for-all approach is unlikely to be applicable for all the scenarios.

The **Goal** is to have an adaptable architecture which be configured to individual's demands and needs.

The following sections describe the challanges, and approach followed by a scenario.

II. mHEALTH CHALLENGES

In order to propose a health solution which meets the users demands, it is necessary to identify the factors which must be taken into consideration during design phase. This section describes the many important challenges related to mobile health domain.

1) Reliability: Health monitoring applications on a user mobile device struggle with reliability which is sub-divided into two aspects

- **Reliability of the Technology:** It is crucial to answer the question that "how much the currently used hardware, bio-sensor and software can be trusted/relied with their desired functions. If the technology doesn't function properly it may generate the faulty or unusable health data.
- **Reliability of Data** The collected health data has no use if it is not associated with it's source (i.e., the user), that's why an issue will arise that: "how to make sure that collected data actually belongs to the user, as it is claimed to be?".

2) Customization & Adaptability: To have a mHealth solution which can address the needs of all users is unlikely to exist. The diversity of the requirements come from different age, sex, health status and social & professional activities. The adaptability of the system will play crucial role in development of a mHealth solution.

978-1-63190-014-3 © 2014 ICST
DOI 10.4108/icst.mobihealth.2014.257483

3) Security and Privacy: The data related to health regarded as one of the most private and sensitive in nature, which is why, it is almost always protected by law of the country. However, it is well known that digital data poses a huge security risk in terms of privacy breach. A data storage which can be accessed globally can be a threat to a user privacy, hence, privacy and trust issues may arise. The protection of health data is a challenge which is yet to be handled properly.

4) Resources Limitations: The scarcity of resources (e.g., bandwidth, processing, memory, and energy) is one of the main issues in mHealth context, which must be tackled before the technology can be used pragmatically in every day scenario. A simple bio-sensor like temperature provides the values such as body-temperature, unit and, time-stamp. If a single data entry needs 24 bytes (assuming java double for each value), thus, for an entire day it will generate $\sim$2 megabytes (24bytes * 86400sec) of data. The amount of data will be even more for the sensors like motion, which generates ten different values (x;y;z: current position, $\theta 1$;$\theta 2$;$\theta 3$: rotation, $\triangle 1$;$\triangle 2$;$\triangle 3$: change in position plus a time stamp). The advancement in the wearable sensors fitted into fabric will increase flexibility, mobility, and consequently generated amount of data. The equation 1 can be used to calculate the amount of data in bytes generated by all the attached sensors in a day.

$$AmountofData(bytes)perday = \sum_{i=0}^{i=n} Z_i * f_i \qquad (1)$$

Where Z = Size of single entry (bytes) and f = Number of measurements per day (seconds)

The hand-held devices pose limited resources which enforces the special design requirements for a proposed mHealth solution.

5) Usability: The diversity of mHealth application users makes it harder to create an easy-to-use graphical interface. The *physical constraints* of devices such as Small Screen [1], display resolution[2], and limited resources (e.g., processor, memory, energy) can significantly effect usability of the application. The usability of the application has also to do with *user* of the application and his/her activities. A user with limited mobility will have different usability issues than an athlete with higher mobility. Usability also depends on the *environmental circumstances*, an application is used in dark has different challenges than one is used in bright light.

6) Efficient Data Handling: As described in section II-4 that, the accumulated sensors and contextual data over a large period of time can be in a vast amount. However, the issue is not limited to the storage capacity and limited bandwidth but, also in case of analyzing the data. The health staff will not be interested in every vital sign and activity of a patient but rather scenario oriented health data. In other words, the storage and retrieval of the health data based on the scenario requirements is a challenge which must not be neglected.

III. Approach

The proposed architecture only deals with data handling and system configuration. The Human-Machine-Interface is a crucial part but, it is not part of the architecture. The figure 1 shows the entire view of the architecture, the individual components are described in the following sub-sections.

A. Identification: Finger Printing

Biometric identification/verification serves both the goals of authenticating the reliability of collected data on the side of the patient and sustaining privacy and specificity issues of the patient on the side of health institute (hospital). On the side of patient, we employed the very well known biometric treat of face in addition to the traits of finger vein and palm vein. The reason for this is that these features don't demand any direct contact to the used sensor, which serve the goal of having a touch-less assisting system. All used traits are integrated in a single multi-modal biometric system by using a decision-level-fusion method [3], [4].
Considering the recently used health monitoring systems (smart mobile devices), which are equipped with diverse biometric sensors, such as camera for the capturing of face images or fingerprint sensor to acquire fingerprint data, the system proposed in [3] can be modified in two different ways. The first is to edit the biometric PC-Software in such a way, that it will be able to perform all steps of biometric identification locally. The second is just to acquire the biometric data through the sensors of the smart device and forward them to the central biometric server. The server will then process these data, extract some biometric features, get the ID of the person and send it back to the smart device. On the side of health institute camera and fingerprint sensor could be amounted to the central PC directly, which contains the central database of all patients of the institute and has the ability of identifying the responsible person using the same biometric system as on the side of patient. The privacy of the patient is still constantly sustained, as the access to private data of the patient depends on the identified personality of team member.

B. Data Storage

In the proposed approach, the data is stored based on the customized configured *rules* depending on the user needs and health demands. A rule is a tuple of conditions and actions - R(C,A) (Where C is set of conditions and A is set of Actions). A condition or set of conditions must be fulfilled before an action can be executed. A condition must itself relate to actions which are taken place once the condition is satisfied as listed below.

- if diastolic $\geq$ 80 OR diastolic $\leq$ 90 (pre-hypertension for diastolic)

An action is an independent entity, it is nothing but a software module or a service which is executed on demand such as data aggregation, automatic call to emergency, and display warnings.

Rules are created with an expiry date, so that, unnecessary processing can be avoided. We propose to describe the rules in XML because of its flexible and extensible nature. A rule, in case of hypertensive blood pressure - an automatic emergency call will be placed, is described in listing 1.

Listing 1. Rule for Hypertensive Crisis
```
<Rule sensor = "BP" id = "a234">
    <Condition  Name = "Emergency" Type =
        "ANY"
    Action = "CallEmergency">
```

```
    <Condition  param = ”systolic”
        operator = ”>”
      value = ”180”/>
    <Condition  param = ”diastolic”
        operator = ”>” value = ”110”/>
    </Condition>
    <Action Name = ”CallEmergency” Method
        = ”AutoRecordedCall”>
</Rule>
```

C. Data Transmission

In the proposed approach, the data is protected by the encryption mechanism during the transmission. The strength (Key in bits: 32,64,128,etc) and the type (e.g., blowfish, AES) of an encryption can be configured. However, the both communicating parties must use same technique which must be agreed before the communication takes place.

D. Data Retrieval

The data is retrieved by health professionals to assess the health conditions of the patients. The retrieved data can be in chunks and it is hard to analyze huge amount of data. Hence, in the proposed architecture, we use data filtering based on individual patient health condition and profile of health professional, or in other words context-oriented[5] data retrieval. The context filtering is combined with the bio-metric identification so that once a health professional enter his credentials via facial or finger printing based on his specialty, experience, and role the list of the patients will be shown. Now when a patient is selected, based on his health context, staff identity, and configured privileges the filtered data will be displayed. By using this method of filtering, the privacy of a patient can be protected besides, the valuable time of professional staff as they do not need to browse through all the data to come to intended data. The table I shows the context which are considered during the filtering process.

Health Professional	specialization, work experience, role,etc
Patient Health	diagnosis, age, gender, history, current health status, etc
Process	current activity (surgery, monitoring), precautions, etc
Environment	location (home, field), time, available technology, etc

TABLE I. CONTEXT INFORMATION

IV. SCENARIO

A surgical ward is quite crucial in terms of revenue of a Hospital besides, having a long waiting list of patients for an elective surgery. Triage department is responsible for managing the urgency of the surgeries based on the patients health status. A violation of pre-operative directives or sudden change in the health condition could be a cause for rescheduling the surgery and consequently waste of resources and planned staff if a proxy surgery can not be carried out. E-Health comes in handy to resolve the issue to some extent by monitoring the patients health prior to operation so that a rescheduling of planned surgery and scheduling of other elective surgery can be managed as early as possible.

A 61 years old patient is scheduled for an elective abdominal surgery in two weeks. The patient have history of hypertension condition. The surgery can not be taken place if the condition reoccurs as arterial hypertension poses a risk of cardiovascular complications after anesthesia, besides risks of organ damage and post operation bleeding. Thus, the doctor defines some pre-operation directives and which vital signs to be monitored during these two weeks. Then a trained staff ask permission of the patient to enter the defined rules and actions.

Sensor: Blood Pressure (Frequency: 30 minutes)

- Rule 1:
  if (systolic $\geq$ 121) OR (diastolic $\geq$ 81) (Pre-Hypertensive State)
  Action: No Aggregation of Data
- Rule 2:
  if systolic $\geq$ 180 OR diastolic $\geq$ 110 for time$\geq$ 10(Hypertensive Crisis, time in minutes)
  Action: Then Automated notification to Hospital Service

As the doctor is more interested in an abnormality (hyper/hypo-tension) in the blood pressure so that an appropriate action can be taken once the condition occurs. If the hypertension condition occurs and persists then the surgery must be rescheduled and the current symptoms must be cured first. The condition should at least remain for 10 minutes persistent before the authorities are notified so that accidental hype can be avoided. Once the rules are configured into the device, the staff asks for the permission to retrieve the data from the patient device as demanded so that the institute is aware of patient's health. The privilege is configured for the limited time-span and for the specific data (e.g., blood pressure, temperature) and furthermore, it is dependent on the specific identity (i.e., a general finger print from the hospital) to protect the user privacy and to provide the security to the data. The incoming request for the data retrieval must accompany the identification of the requester in order to dispatch the data from the patient's device.

After 2 weeks of monitoring, the patient health remained stable which gave the doctor confidence to carry on with the planned surgery. After the successful surgery, the doctor wants to be sure about post-operation state of health and let new rules and privileges to be configured. The previously configured rules and privileges are already expired but not removed from the system. Rise in the body temperature is an indication of an infection. Thus, the new rules are configured to monitor the body temperature so that appropriate measures can be taken before an infection spread in the body.

Sensor: Pulse (Frequency: 1 second)

- Rule 1:
  if temperature $\leq$ 37 (temperature is measured in degrees Celsius)
  Action: Data Aggregation
- Rule 2:
  if temperature $\geq$ 37 for time$\geq$ 120 (temperature is measured in degrees Celsius, and time in minutes)
  Action: Then Automated notification to Hospital Service

The rule 1 say, if the temperature is normal then data will be aggregated to reduce the amount of data. The rule

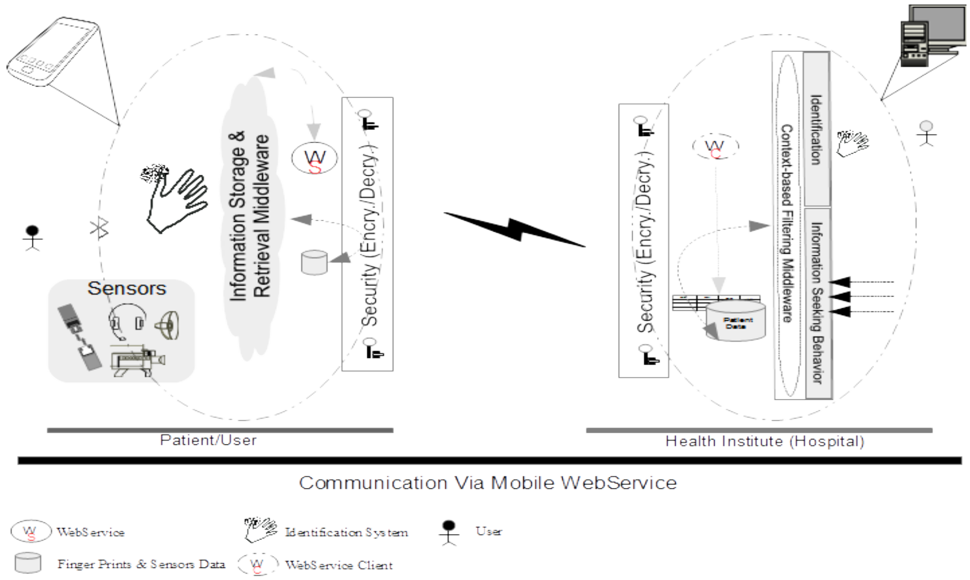

Fig. 1. architecture

2 defines that if the body temperature rise above norm and remain high for the two hours then authorities must be notified. The pulse rate is monitored every second. Furthermore, the doctor must also define filtering criteria so that once he enters his credentials via his finger prints, the only desired data from the patients are shown to him.

Personalization of the patient and the health institute staff member could be achieved by employing sufficient biometric traits. It provides person-specific healthy support for the patient, including listing all person-specific medication, taking time of them and alerts the patient in the case of taking medicament either later or earlier as normal taking time. On the side of health institute biometric-based personalization serves for setting access privileges of staff members, which enables a permanent controlling of her vital values without the privacy issues of her being threaten.

V. mHealth Challenges and Proposed Architecture

As shown in Table II, the biometric identification methodology helps to protect the user privacy in addition to keeping the personalized configuration reloaded once a user identified. Identification also fosters the reliability of the data by forcing to have a biometric log-in before system can be used.

Configurable rules make the proposed-architecture context and user oriented, eventually being nearer to individual needs. The storing only the required data helps in efficient use of resources. The use of context and case based filtering helps the medical staff to come to a faster analyzing of targeted data rather than retrieving the irrelevant chunk of data. Which consequently saves precious resources and time of medical professionals.

VI. Conclusion

A brief detail of the proposed architecture is presented here which can adapt to user, health condition, health staff needs and demands. It also provides the way to protect user privacy and to secure the sensitive data. However, the described approach doesn't take into consideration the usability of the system and interdependence among the vital signs. Such as how to be certain if a increased pulse is because of arrhythmia or excessive activity, however, in most of cases it can be avoided by including the time span for the continual abnormal vital signs. There are aspects like interdependence, usability and performance which are on our list for the future tasks.

Method	Privacy	Security	Reliability	Custom	Efficiency	EDA	Usability
Id	X	X	X	X			
Rules				X	X	X	
Enc		X					
Filtering				X	X	X	

TABLE II. Issues covered in the Proposed Approach

- **- EDA:** Efficient Data Handling **- Id:** Identification
- **- Enc:** Encryption **- Custom:** Customization

References

[1] L. Kim and M.J. Albers Web design issues when searching for information in a small screen display, Proceedings of the 19th Annual International Conference on Computer Documentation, Sante Fe, New Mexico, USA, 2001.

[2] M. Jones and G. Marsden and N. Mohd-Nais and K. Boone and G. Buchanan Improving Web Interaction on small displays, Proceedings of the Eight International Conference on World Wide Web, Toronto, Canada, 1999.

[3] A. Rabie, U. Handmann Nfc-based person-specific medical assistant for elderly and disabled people, in, Proceedings of the International Conference on Next Generation Computing and Communication Technologies ICNGCCT, Dubai, UAE, 2014.

[4] A. Rabie, U. Handmann NFC-Based person-specific Assisting System in Home Environment, Proceedings of 11th World Congress on Intelligent Control and Automation WCICA, Shenyang, China, 2014.

[5] O. Koch, E. Rotaru Using Context to Improve Information Supply in the Medication Sector, Proceedings of Workshop BIS 2010, 2010.