Medical and Health Sciences Research Journal
ISSN: 2997-6693|
Volume 13 Issue 2, April-June, 2025
Journal Homepage: https://ethanpublication.com/articles/index.php/E7
Official Journal of Ethan Publication

INTEGRATING CONTEXT AWARENESS FOR SMARTER PERSONAL HEALTH RECORDS

Ramesh Kumar Varma and Neha Priya Reddy
Department of Information Technology,Saint Martin's Engineering College ,Hyderabad, INDIA
DOI: https://doi.org/10.5281/zenodo.17192346

Abstract
On one side of India, we have multi-specialty hospitals which satisfy the healthcare needs of people with specialized and speedy treatments. On the other side, a large part of the population in India resides in rural areas where basic medical facility is sometimes unavailable. People in the rural areas do not get proper treatment due to the non-availability of required number of registered medical practitioners. This paper presents the architecture of Context Aware Health Monitoring System developed for connecting Primary Healthcare Centres in the rural areas with the sophisticated hospitals in the urban areas of India through mobile communication and IT infrastructure. The system aims to provide affordable, efficient and sustainable healthcare service by leveraging mobile communication and information technology. The system monitors and delivers patient's physiological readings to the hospitals and provides an alert mechanism triggered by the patient's vital signs which is linked to a medical practitioner's mobile device.

Keywords: Telemedicines, Secure key, sensors, Mobile application.

I. INTRODUCTION

In the existing scenario, the information relating to patient are stored and accessed through online which is very complex task because there is a chance of losing the data. So, in the proposed system, to safeguard the information there is solution to the existing system is that maintaining the records and information in digital devices by developing an application in Mobile devices. Through mobile phone accessing, the life of every individual becomes simple and easy because the patient's detail can be stored and easily accessible on hand. The doctor can render services more efficiently through mobile phones. The interaction between the patient and the doctor can be done anytime of the day. The patient can come into contact with the doctor at anytime from anywhere. There will be easy access of information at anytime from anywhere. In emergency situations, the information and patient's details which are recorded in the mobile phones is very helpful for a person for giving first-aid to injured patient till he/she taken to hospital. Through this process, one can save the life of a patient. There are various benefits for the patient as well as for doctor by developing the PHRs application in mobile devices.

Therefore, mobile phones are helpful in emergency circumstances where there is no chance of utilizing

Medical and Health Sciences Research Journal
ISSN: 2997-6693|
Volume 13 Issue 2, April-June, 2025
Journal Homepage: https://ethanpublication.com/articles/index.php/E7
Official Journal of Ethan Publication

Computer systems. The quality of health can be improved by this process. Through mobile PHR, one's life can be saved at the time of accidents. There is less scope of misusing the information because the records are saved individually in PHRs. The information is easily accessible to everyone in any urgency conditions through mobile health records.

HEALTH MONITORING SYSTEM

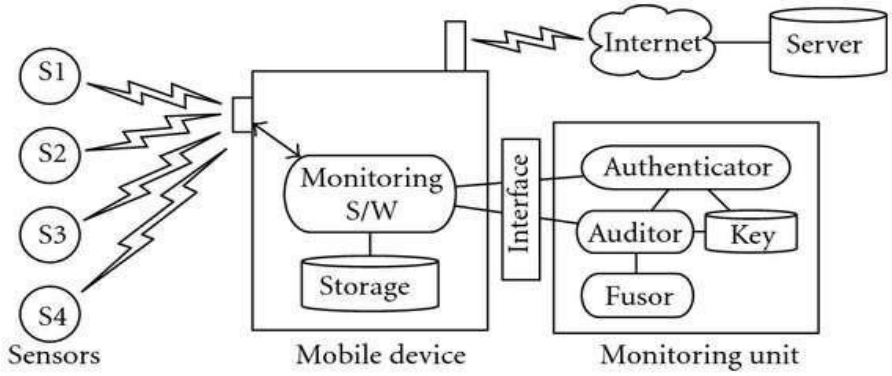

Figure 1: Health monitoring architecture.

II. IMPLEMENTATION

[John et al, 2008]Software development life cycle assist the software engineer in building a well-defined and reliable software product by forcing them to follow systematic and cost efficient process. Implementation is crucial phase of software development life cycle. This is the third phase of developing process, where program coding is developed by the software engineers. In implementation phase hardware and software testing is carried out. This phase is executed after complication of system design.

Implementation phase primarily focuses on site collection, deployment preparation and training the end users so that they can handle system applications efficiently. This phase involves final testing of entire system to ensure that it is working according to the client specifications and management of preliminary functions of the system. Implementation phase mainly concerns about the security of the system.

Biosensor-Transceiver Pair: Wide range of biosensors can be found in the market. Examples are sensors for heart rate, temperature, falling, bending, etc . Each sensor needs to be paired and packaged with a miniature low-power transceiver. As a matter of practicality, it would be much easier to use if the sensortransceiver pair is packaged as a patch.

Gateway: The gateway, would be responsible for data collection, processing and overall BAN network management. Having enough memory and processing power (a mid-size microprocessor) is inevitable. The gateway also includes two types of wireless communication: (i) a receiver to get data from biosensors and (ii) a wireless Ethernet adapter to communicate with the standard wireless router/switch.

Monitoring Server: Monitoring server runs powerful back-end software to collect, analyze profile and make decisions. It is well understood that bio metrics of each individual are very much unique. Thus, for effective

Medical and Health Sciences Research Journal
ISSN: 2997-6693|
Volume 13 Issue 2, April-June, 2025
Journal Homepage: https://ethanpublication.com/articles/index.php/E7
Official Journal of Ethan Publication

processing a personalized profile should be "learned" automatically by the server. This is a crucial step to minimize (and even achieves zero-level of) false positive (i.e. raising alarm for non-critical situations) and false negative (i.e. missing a critical, perhaps life-threatening situation). To do so, a combination of innovative learning and reasoning algorithms are required to interpret data properly during monitoring.

These are two types of the threats: mis-use of Patient identities, unauthenrized access and modification of PHI in the health monitoring system in figure 2. We consider three types of adversary: the Patient himself or herself, insiders (authorized EHR users, staff of the EHR organization, or staff of other mHealth support systems), and outsiders (third parties who act without authorization).

Identity threat: There are three concerns here. First, the Patient may lose (or share) their identity credentials, enabling others to have access to their PHI in the EHR (or in their MN). Second, insiders may use Patient identities for medical fraud, for example, by submitting fraudulent insurance claims [16];the result can be financially or even medically damaging to the Patient. Furthermore, in the growing problem of medical identity theft, outsiders (or insiders) may use a Patient's identity to obtain medical services [17], potentially with financial or medical damage to the Patient. Finally, in some settings (such as research) Patient identities are removed from the PHI, and the risk is that an outsider may combine the de-identified data with data from another source to re-identify the Patients, that is, to re-link Patient identity to their PHI [18].

Access threats*:* we explore threats related to unauthorized access to PHI, whether in the MN or the EHR. The first threat comes from the Patient himself or herself, because (under the definition of health information privacy) the Patient has a right to control the collection, use, and disclosure of PHI; if the Patient fails to express their consent consistent with their actual preference, for whatever reason, they may allow broader-than-intended collection, access or disclosure; Insiders may "peek" at Patient data, out of curiosity, or with the intent to harm the Patient (e.g., an employer who snoops on employer-provided EHR and fires workers with expensive conditions) [19], [20]. Outsiders may break into Patient records, which may lead to embarrassment (e.g., exposing a Patient's psychiatric data to his divorced spouse) [21]; Several of these threats involve the modification of health records. In a EHR, Patients (or insiders [19]) may mistakenly modify their data if the access-control policies are too permissive, or if the mechanisms too easily allow mistakes. Insiders may modify PHI intentionally, to obtain reimbursement via insurance fraud [22]. Outsiders may also modify a Patient's PHI, for fraud or malice.

III. QUALITY CONTROL FRAMEWORK

In this section, we design a quality-control framework based on the risk analysis in the previous section. The framework is a set of processes that ensure, verify, and evaluate the data quality.

To design a quality-control framework, we first analyzed the health-monitoring system as a sequence of processes, assigned related factors to each process, and then identified possible methods for the quality control of individual factors. Figure 1 illustrates our analysis. Medical sensing begins with sensing the physiology of the patient (*sense* process). Each sensor generates sensor data at a certain rate and transmits

Medical and Health Sciences Research Journal
ISSN: 2997-6693|
Volume 13 Issue 2, April-June, 2025
Journal Homepage: https://ethanpublication.com/articles/index.php/E7
Official Journal of Ethan Publication

them to the device through a wireless connection (*transfer* process). The monitoring device collects data from sensors, processes them as needed (*collect* process), and then forwards them to the provider (*transfer* process). Upon receiving the data from the device, the provider's server evaluates the validity of the data (*verify* process) and then presents the data to the provider. When it presents the data, the server also presents the level of the data quality to the provider (*assess* process). Figure 1lists the factors that are related to each process. For each factor, the possible methods for quality control are shown. In the following, we discuss our analysis in more detail.

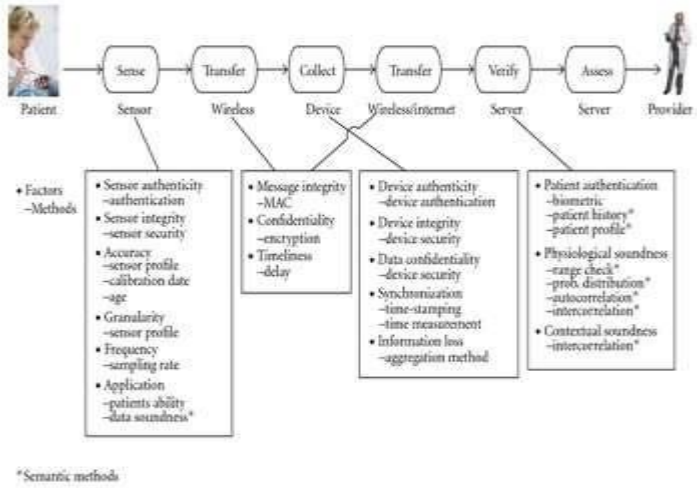

Figure 2: Quality control of remote health monitoring.

(i)Accuracy

The accuracy of a sensor depends on its design and manufacturer (i.e., sensor profile), the time since the latest calibration, and the age of the sensor. The data quality depends on the accuracy expressed by the expected error bound.

(ii)Granularity

The quality of sensor data also depends on the level of detail that a sensor can provide.

(iii)Application

The data quality also depends on correct application of the sensor to the body; if the sensor is not correctly applied to the body, it generates incorrect sensor data. If the patient is responsible for the application, the quality of sensor application depends on the patient's ability and diligence. The patient's ability depends on the education, age, and prior experience. When a sensor is incorrectly applied, the data is likely to deviate from the range of values that are considered *reasonable* as a physiological value. We call this reasonableness of the medical data *soundness*. The soundness of data includes physiological soundness and contextual soundness; we explain these in more detail below where we explain the verification process.

(iv)Synchronization

It is often medically necessary to collect multiple sensor readings of different modalities, and a health professional can derive a medical condition from their combination. For the combination to be useful, the sensor readings should be temporally synchronized. If sensors cannot time-stamp each data, the device should do so, but it should also make sure that the sensor data is sampled at that moment (i.e., not replayed by an adversary). The data quality depends on the granularity of the synchronization.

(v)Information Loss by Aggregation

Communication is costly. To save the amount of information to be sent, the device can aggregate sensor readings before sending (e.g., reporting the average per minute). However, every aggregation loses some information in data, and the quality of data depends on the amount of information lost by the aggregation.

IV. Conclusion

This project has been carried out successfully on the mobile application pertaining to personal health records. As per the time schedule, development research methodology is managed accurately in the project. For conducting this research, RAD model is used for completing the project successfully. Throughout the project without any variations the literature review has guided the research. The main aim of the research is to develop application pertaining to personal health records with ease of accessibility in mobiles. The RAD model is utilized to accomplish the research within the stipulated time in this project. In this project, various problems are identified through system analysis, identifying the feasible solutions for existing systems through system design, to detect the errors, system testing is used and implementation of software to the end users is described. Various types of testing are also explained in order to overcome the issues while implementing wide variety of tools. Finally, collected information is effectively analyzed in order to illustrate the basic conclusions that help the developer in implementing suitable software application in mobiles.

REFERENCES

Rash, M.C. Privacy concerns hinder electronic medical records. The Business Journal of the Greater Triad Area (Apr. 4, 2005).

Lin X, Lu R, Shen X, Nemoto Y, Kato N.SAGE: a strong privacy preserving scheme against global eavesdropping for ehealth systems. IEEE Journal of Selected Areas of Communications.

Ou, C.-M. and Ou, C. R., "A High-Level 3G Wireless PKI Solution for Secure Healthcare Communications", EuroPKI 2006, Lecture Notes in Computer Science 4043, Springer-Verlag, 2006, pp. 254-256.

[4]. Yuhai Zhang, Yongyong Xu, Lei Shang, etc.An investigation into health informatics and related standards in China. International Journal of Medical Informatics [J]. 2007(76), 614–620.

Medical and Health Sciences Research Journal
ISSN: 2997-6693|
Volume 13 Issue 2, April-June, 2025
Journal Homepage: https://ethanpublication.com/articles/index.php/E7
Official Journal of Ethan Publication