Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2016, 3(4): 7-11

Research Article ISSN: 2394 - 658X

Securing Pervasive Communications in Healthcare Systems

T Soren Craig, Sudeer Chinta, Mary Eshaghian-Wilner, Nikila Goli, Aman Gupta and Andrew Prajogi

Ming Hsieh Department of Electrical Engineering, Los Angeles, United States of America

---

ABSTRACT

Current healthcare and wellness monitoring devices make medical follow-up convenient. However, the decentralization of data processing and extensive reliance on network connectivity introduces security threats. Current smart health devices often focus their attention more on usability and design rather than solidifying underlying security measures. While web-based security is available, device-level security in smart health devices needs to be explored further. In this paper, we propose an advanced security module that can be used in any generic healthcare and wellness monitoring smart devices. This generic infrastructure can be used as a macro in any available technologies to enhance overall security.

Key words: Healthcare security, encryption, data security, healthcare devices

---

INTRODUCTION

The proliferation of smart health devices makes health monitoring convenient and immediate. Patients collect their physiological data with smart devices, e.g. in the form of wearable computing devices, forming a body area network that collects physiological data autonomously from the wearer. This data can include biomarkers such as glucose levels and blood pressure. This information eventually needs to be augmented with metadata, like its origin and collection time. The monitoring process covers a first data processing step, which is filtering to identify abnormal conditions. In the event of abnormal patterns in health markers, a medical expert is immediately notified. This assists the medical expert as well because more data is available and it is easier to identify abnormal patterns in the data set. This method of data collection is convenient since the monitoring devices are small and noninvasive. Coupled with convenience, however, is the requirement of stringent security measures to protect this highly sensitive data.

Many fitness-oriented smart healthcare devices have flooded the market over the past several years. Fitbit, Garmin, Acer and Withings, among many others, sell devices that measure physiological data such as heart rate, sleeping patterns, and even blood oxygen levels with the goal of encouraging fitness. As the adoption of these smart units ramps up, there are alarming trends regarding the security measures. The initial authentication of the device with the smartphone is the first area of concern. An independent study by the Independent IT-Security Institute has found that during this step some devices like the Fitbit Charge smart device do not have any authentication in place when pairing with the smartphone [13]. This leaves the current health data stored on the device open to a potential hacker. Furthermore, other devices like the Leap Manager by Asus send health information from the smartphone to a central database over an unencrypted http connection instead of the encrypted https protocol. As these devices evolve into more powerful health units with direct control over patient health, like automated insulin injectors for diabetic people, we must ensure that there is a strong security framework protecting the wearer from hackers.

The benefits of a pervasive healthcare system are substantial. Doctors can use more intelligent monitoring to assess the situation of a patient and propose the correct treatment much more rapidly. One approach to continuous and intelligent patient monitoring is represented by pervasive healthcare [1]. They introduce healthcare IT challenges and requirements that are designed for patients and health-care professionals. The issue of collecting and evaluating medical data has been addressed. However, the secure transmission, reception, and retention of the data remain to be fully anatomized. If we are to realize the full benefits of such a system, we need to ensure it has strong security underpinnings.

The security of data from smart health devices is often neglected because of additional cost and hardware considerations. This poses a large threat because sensitive health information is collected based on long-term patterns derived from body-worn sensors. This information covers wide latitude of health markers, from blood sugar levels to sleep patterns and blood pressure. If this data is sent unencrypted over-the-air, malicious attackers can wreak havoc in many ways. First, without device-to-device certification, the process is subject to man-in-the-middle attacks. This attack occurs when a hacker intercepts the communication between two parties that think they are communicating directly. The attacker can receive messages from one person, alter them, and then send new messages to the second party in lieu of the originals. In this context, a man-in-the-middle attack could allow an attacker to replace the health device data sent from the smart device with falsified data. The medical experts that depend on this information would then be prescribing treatments and therapies that are meant for a condition the patient does not have and/or withholding therapies for a condition the patient actually does have. This could pose very serious problems to the patient's health. In addition, the data could lead to discrimination by health insurance providers or move financial markets by providing insight into the health conditions of business executives.

Therefore, in this paper, we propose a comprehensive security architecture that addresses the problems in some modern health units. This is accomplished by encrypting all data sent from a body device to a patient's smartphone with a securely exchanged key. The next transmission step is done over the secure https protocol. Overall, this leaves little room for potential hackers to steal sensitive health information.

The rest of the paper is organized as follows. Section two gives an overview of the architecture of the proposed system followed by a description of the security module and its analysis. Implementation details of the system are highlighted in Section three. Next in section four, there is a comparison of the related works. Finally, Section five concludes the paper by highlighting areas of future research and extensions of this project.

PRELIMINARIES

In this section, the terms used to describe the overall architecture are defined and their usages are explained. There are many terms used in this paper that are abbreviated for conciseness. An SBU, or Secure Body Unit, denotes any smart health device that autonomously collects the wearer's health data. An SMU, or Secure Mobile Unit, is a software application on a mobile device, typically a smartphone that generates a readable report out of health data. A PIS, or Patient Interface System, is a convenient online system maintained by healthcare providers that allows easy medical record retrieval by authorized physicians. These components are connected to each other through secure interfaces. Lastly, the AGSK is an automatically generated secure key created by the SMU and later sent securely to the SBU.

This paper establishes a generic infrastructure which targets each data transmission step from smart health device to smart phone, and finally to the physician's online portal. The goal is to lay a secure framework than can be extended to any healthcare infrastructure. In addition, the infrastructure aims to limit the invasiveness of monitoring and sensing. Security can be implemented using many industry-standard encryption protocols like RSA and all processing can be done at the sensor level or device level.

Many health organizations opt to electronically access and analyze a patient's health based on historical patient records. This usually involves data retrieval from a legacy health application and migration of that data into a secure relational database. A typical health data archive includes a front end user interface that allows easy access for viewing historical patient records. This is different from a backup of the historical data, which makes it more difficult to access information on demand [3].

ARCHITECTURE OF HEALTHCARE MONITORING SYSTEM

Here we describe the components of the generic healthcare monitoring system and the security components implemented.

Components of the Pervasive Healthcare Monitoring System

In previous sections, we outlined the intended usage of the generic security system and its security requirements. In this section, we discuss the architecture used to satisfy those requirements. The system must be generic, as users will access it from various platforms. For example, medical experts like physicians, doctors, and nurses can access medical records either through their online interface system or via smartphone.

Fig. 1 shows the key components of the proposed architecture, which are the Secure Body Unit (SBU), the Secure Mobile Unit (SMU), and the Physician Interface System (PIS). The Secure Body Unit (SBU) collects physiological data about the patient and encrypts it with the automatically generated Secure Key (AGSK). A secure connection is established between the SBU and the SMU using the RSA algorithm. This connection could use one of many mediums – Bluetooth, wireless, or even a local connection. The encrypted data is sent through this connection to

the SMU. Even if the information was stolen during this step, it would be unreadable to the hacker due to its encryption. Once stored in the SMU, the data is decrypted. Logic components are then used to analyze and filter the data in order to produce a meaningful report for physician use. The SMU can be downloaded on each individual user's smartphone. We explain the secure generation of the AGSK as well as the installation of the SMU on a smartphone in the security section. Finally, the detailed health report is sent to the PIS via the https protocol. The PIS must know which SMU units are authentic. To achieve this end, a one-time registration must be done with the PIS once the SMU software is installed. Once the report is sent to the online system, the physician can conveniently check the real-time health status of a patient.

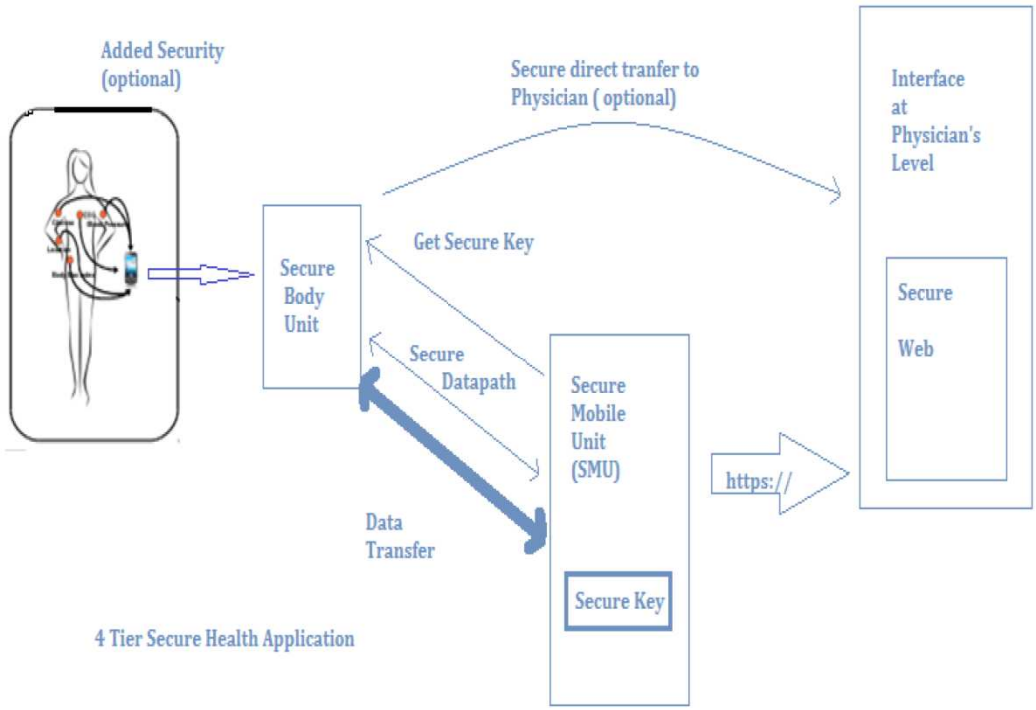

Fig. 1 Components of the Secure Health Application

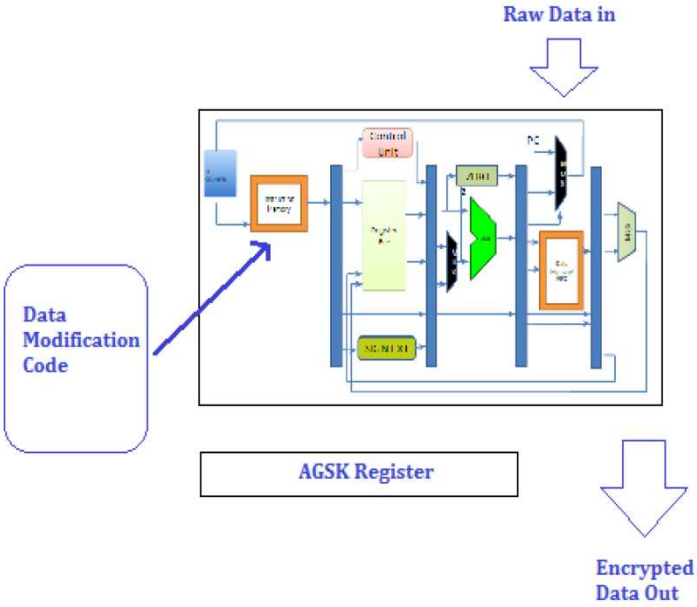

Fig. 2 Block Diagram of SBU

Implementation of Security in the Architecture

There were several guiding principles that led to this secure architecture: we prefer simple and reliable security protocol over more complex or error prone ones and attempt to secure every interface to minimize the surface area that can be attacked. By implementing security at a modular level, we can ensure greater security of the overall architecture.

The SBU has a built-in processor and the data type of the pipeline is a convertible FIFO. The raw data that coming into the device memory is stored in the FIFO. The AGSK received from the SBU is stored in a temporary register. Once the FIFO is full or raw data input has stopped, the processor begins encrypting the data in the FIFO with the AGSK. Any industry standard processor can be used for this purpose. The key is to develop an application-oriented processor that uses minimal area and has a reduced instruction set. The reduced instruction reduces the necessary hardware components, which allows for the entire device to be as small and minimally invasive as possible.

System Operation and Security Implementation

The authentication of the phone is done with an encrypted key certificate within the smart phone. Then, users can be provided with a QR code, containing the keys for the certificate store and for encryption on the phone. This allows for secure installation of the application on a smartphone or any handheld device. The SMU is unique to each and every device it is installed on. Once securely installed, as explained previously, the SMU generates a unique key, AGSK. The AGSK is then sent to the SBU once the secure channel between the SMU and SBU has been achieved. The generation of AGSK on SMU is random and requires unique key generation anytime a connection has been established between SBU and SMU.

The simple procedure is as follows. Raw data comes into the SBU as input and is stored in a convertible FIFO. A secure connection is established between the SBU and the SMU. The connection is secure because it is created using RSA Protocol. The SMU sends the AGSK key through the secure network connection to the SBU. The SBU encrypts the data in the convertible FIFO using the AGSK key using the AES algorithm. Now the encrypted data in the FIFO of the SBU is sent to the SMU through the secure network. The SMU gets all the data and stores it in an array. Using the local AGSK key (which was previously sent to the SBU) the data is decrypted. The SMU generates a local report from the data received, after filtering out irrelevant readings. The SMU now sends this report to the PIS using a secure https connection. Then, the medical expert can access and analyze it.

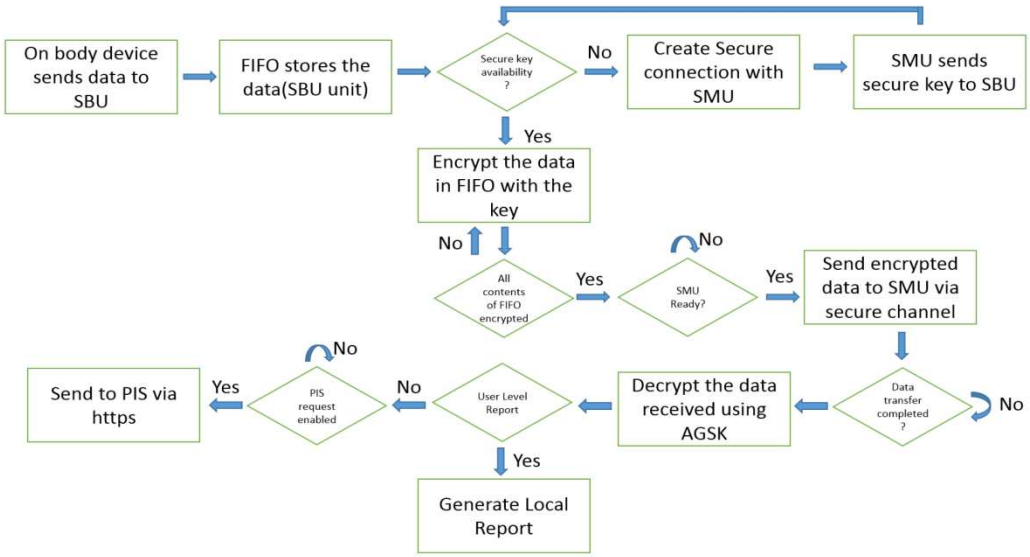

Fig. 3 Flowchart for secure data transfer

RELATED WORK

"An Agent Based Pervasive Healthcare System: A First Scalability Study" discusses the implementation of a Pervasive Healthcare System intended to support pregnant women affected by Gestational Diabetes Mellitus [14]. The architecture is composed of a mobile interface connecting to a distributed multi-agent system which in turn is connected to a patient management system. Very similar to the PIS discussed in this paper, their patient management system stored the data produced during the monitoring phase and allowed for convenient and rapid access by doctors. However, this paper doesn't emphasize the security considerations during the data collection. Though some security safeguards are employed by these applications to comply with existing medical data security and privacy regulations, they are not adequate in today's context.

"Enforcing Security in Pervasive Healthcare Monitoring Gestational Diabetes Mellitus" addresses the problem of securing the communication between the patients and the doctors [15]. The result is a fully implemented telemedicine system for GDM that mitigates the risks associated with the most common malicious attacks directed to a distributed system. The proposed model, however, is not generic. A more generally applicable model is necessary to accommodate the plethora of different devices that are going to comprise the pervasive healthcare model.

CONCLUSION

In this paper we presented a generic and secure infrastructure for a variety of healthcare or wellness applications. The infrastructure covers many loose ends on security and strengthens the data transfer from body-worn devices to hand-held mobile devices. The interconnections are made secure using industry standard security protocols, leaving minimal open ends for attacks. As described in Figure 1, one extension to this infrastructure could be a direct, encrypted data transfer from body-worn devices to the physician interface. This can be achieved if the body-worn device has an optimized processor to generate the detailed health report out of raw, physiological data.

REFERENCES

[1] U Varshney, *Pervasive Healthcare Computing: EMR/EHR, Wireless and Health Monitoring*, Springer Publishing Company, Incorporated, **2009**.
[2] G Ghinea, S Asgari, A Moradi, T Serif, A Jini-based Approach for Electronic Prescriptions, *IEEE Transactions on Information Technology in Biomedicine*, **2006**, 10 (4), 794-802.
[3] A Maji, A Mukhoty, A Majumdar, J Mukhopdhyay, S Sural, S Paul and B Majumdar, Security Analysis and Implementation of Web-based Telemedicine Services with a Four-tier Architecture, *Pervasive Computing Technologies for Healthcare.* Tampere Finland, **2008**.
[4] S Bromuri, M Schumacher, K Stathis and J Ruiz, Monitoring Gestational Diabetes Mellitus with Cognitive Agents and Agent Environments. *Conference on Web Intelligence and Intelligent Agent Technology*, Lyon, France, **2011**.
[5] P de Toledo, S Jimenez, F del Pozo, J Roca, A Alonso and C Hernandez, Telemedicine Experience for Chronic Care in COPD, *IEEE Transactions on Information Technology*, **2006,** 10 (3), 567-573.
[6] M Beauscart-Zéphir, S Pelayo, P Degoulet and J Meaux, A Usability Study of CPOE's Medication Administration Functions: Impact on Physician-nurse Cooperation, *Study in Health Technology and Informatics*, **2004,** 107 (2), 1018-1022.
[7] S Murthy and BS Manoj, Ad Hoc Wireless Networks Architectures and Protocols. Englewood Cliffs, NJ: Prentice Hall, **2004.**
[8] E Lemaire, D Deforge, S Marshall and D Curran, A Secure Web-based Approach for Accessing Transitional Health Information for People with Traumatic Brain Injury, *Computer Methods and Programs in Biomedicine*, **2006,** 81(3), 213–219**.**
[9] J Zhang, J Sun, Y Yang, X Chen, L Meng and P Lian, Web-based Electronic Patient Records for Collaborative Medical Applications, *Computerized Medical Imaging and Graphics*, **2005,** 29(2), 115–124**.**
[10] N. Maglaveras, L Chouverda, VG Koutkias, G Gogou, I Lekka, D Goulis, A Avramidis, C Karvounis, G Louridas and EA Balas, The Citizen Health System (CHS): A Modular Medical Contact Center Providing Quality Telemedicine Services, *IEEE Transactions on Information Technology in Biomedicine*, **2005,** 9(3), 353–362.
[11] M Wang, C Lau, F Matsen and Y Kim, Personal Health Information Management System and its Application in Referral Management, *IEEE Transactions on Information Technology in Biomedicine*, **2004**, 8(3), 287–297.
[12] Y Xiang, Q Gu and Z Li. A Distributed Framework of Web-based Telemedicine System. *Proceedings of the 16th IEEE Symposium of Computer Based Medical Systems*, **2003,** 108–113.
[13] E Clausing, M Schiefer, U Losche and M Morgenster, Security Evaluation of Nine Fitness Tracker, *The Independent IT-Security Institute*, Web. https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf, **2015.**
[14] J Krampf, S Bromuri, M Schumacher and J Ruiz, An Agent Based Pervasive Healthcare System: A First Scalability Study, *Electronic Healthcare*, Heidelberg, **2011**.
[15] S Bromuri, J Krampf, R Schumann and M Schumacher, Enforcing Security in Pervasive Healthcare Monitoring Gestational Diabetes Mellitus. *The Fourth International Conference on eHealth, Telemedicine, and Social Medicine*, Valencia, Spain, **2012**.
[16] T Soren Craig, Mary Mehrnoosh Eshaghian-Wilner, Nikila Goli, Aman Gupta and Chinta Sudeer Kumar Reddy, Security in Pervasive Healthcare Systems, Accepted for publication in *8th World Medical Nanotechnology Congress and Expo*, Dallas, USA, June 8-9, **2016**.