2009 International Conference on Computer Engineering and Applications
IPCSIT vol.2 (2011) © (2011) IACSIT Press, Singapore

Context-Based Access Control to Medical Data in Smart Homes

Mouhcine Guennoun, Jonas Talon, Catherine Weddum and Khalil El-Khatib
University of Ontario Institute of Technology
2000 Simcoe Street North, Oshawa, Ontario, Canada L1H 7K4
{mouhcine.guennoun@uoit.ca, khalil.el-khatib@uoit.ca }

Abstract. Continuous progress in mobile wireless devices and miniaturization in medical devices are bringing pervasive healthcare into reality. With the help of these devices, a large number of people, especially the elderly, can benefit now from high healthcare quality in the comfort of their own homes. Some of the major concerns that still need to be addressed before these devices get a wide acceptance include protecting the security and privacy of medical data collected by these devices. Traditional static access control solutions do not address the complex dynamic security requirements of healthcare applications. This paper presents context-based access control architecture to fulfill the security requirements of protecting medical data in pervasive healthcare. The system continuously collects and analyses medical data, and updates the access control rules to the data based on the dynamically changing medical condition of the user.

Keywords: Access Control, Smart Homes, Health care, Accelerometer.

1. Introduction

Aging population is a global trend [1]: according to a study by Hooyman et. al.[2], the worldwide population aging over 65 is expected to more than double from 357 million in 1990 to 761 million by 2025. By 2050, according to UN estimates, about 20% of people will be aged 60 or over, and the figure could climb as high as 33% in developed countries. Canada exhibits this trend also: according to results published by the Public Health Agency of Canada, seniors will comprise a large share of the Canadian population, growing from 3.5 million people in 1996 to an estimated 6.9 million by 2021.

Smart home technologies can help improve the aging experience by providing an environment which can assist in a medical emergency situation and even help with medication administration. Such technologies provide an excellent infrastructure for healthcare applications, which would allow seniors to get some provisioned healthcare services in the comfort of their homes. Additionally, smart homes have been advocated as one way to reduce the burden on the healthcare sector: using smart homes, early signs of sickness can be easily collected, fused, analyzed used a wide range of medical sensors, hence leading to an early detection and prevention of sickness.

Preliminary research into smart homes have so far focused on the efficiency of the available communication and computation technologies and their cost, with little focus on the security and privacy of the amble data collected in these environment: the granularity and accuracy of the data (especially health data) collected within a smart home present opportunities for severe security and privacy violations, especially when smart homes can continuously monitor, store, data mine, and release data to third parties. Therefore, it is critical that collected data be protected and managed properly to make the users of smart homes feel secure and private while using any smart home healthcare application.

The remainder of this paper is organized as follows. In Section II, we will describe a scenario to show how the proposed architecture can be used. In Section III, we will present a literature review on context-aware systems and available access control models. Our architecture is presented in Section IV, and finally, the conclusion in Section V.

2. A Fallen Elderly Scenario

John, a 75 year-old man has been living alone in his home after his wife passed away and his children moved out of the city. Concerned about the possibility of falling, John's son, Peter, bought him an accelerometer device with heartbeat monitor embedded in it. The device continuously streams its x-y-z coordinates and heartbeat of the person, attached over Bluetooth, to a nearby personal computer.

Upon installing the software for the device, John agreed to an End User License Agreement (EULA) that grants consent for the computer to dial emergency services (911) on his behalf, if his medical condition necessitates that.

It was not long after John started using the device when he suffered a fall, which has a great enough magnitude to be deemed urgent. The computer recognizes this fall using the data from the accelerometer data and by considering the drop in the heart-rates, and calls 911. A paramedic arrives on scene.

Soon a paramedic arrives at John's home, but in order to effectively treat John, he requires access to historical medical data from the database, which includes heart rates and electrocardiograms (ECGs). John has specified in his preferences that a paramedic may only obtain access to the data if they are on duty at the time of emergency; and that he has been in an emergency situation.

The paramedic presents his radio-frequency identification (RFID) card to the RFID card reader connected to the computer where all John's medical data is stored. The system connects to the medical service certificate authority to validate the card and to confirm that the paramedic is on duty. The policy engine evaluates John's policy and his medical condition, and decides to provide the paramedic with access to medical history of John. The paramedic can now use this history to provide better medical service.

3. Context Aware Systems and Access Control Models

3.1. Context Aware Systems

While the demand for in-home healthcare for the aging population is relatively new, research and development for critical enabling technologies have been gaining tremendous momentum in recent years.

The Context-Aware Service Integration System (CASIS) [3] proposed a multi-agent service framework, which uses the OSGi service platform to integrate event-driven services and build a smart home infrastructure containing smart furniture, context-aware services, and healthcare services. The purpose of the framework is to demonstrate how context-aware technologies and mobile web services can help enhance the quality of care for an elder's daily life.

The LiveNet [5] system from MIT presented a mobile platform that can be used to implement proactive health care application. It uses biometric sensors and radio communication to stream bio-signals to remote caregivers, showing how long-term physiology changes can be captured to objectively measure medical treatment and medication efficacy in clinically depressed patients.

The SHARP (System for Human Activity Recognition and Prediction) system at Intel Research and the University of Washington [6] is another work related to context-aware systems. The system objective is to enable a ”widely applicable activity inference” system which attaches several RFID tags to everyday objects throughout the elder's home. An elder wears gloves containing a RFID reader so that information he touches can be gathered. That information can be used to interpret the elder's daily activities.

The Everyday Computing Lab at the Georgia Institute of Technology introduced the digital family portrait (DFP) [7,8] to provide surrogate social support for aging people who are living alone. The aim of the project is to build a living laboratory with multi-discipline sensors to monitor a resident's activities. Digital frames are created using sensor data, which is presented to the elder's family member in a remote house, reflecting a portion of the elder's life. This can provide the distant family members with day-to-day awareness information of their senior relatives.

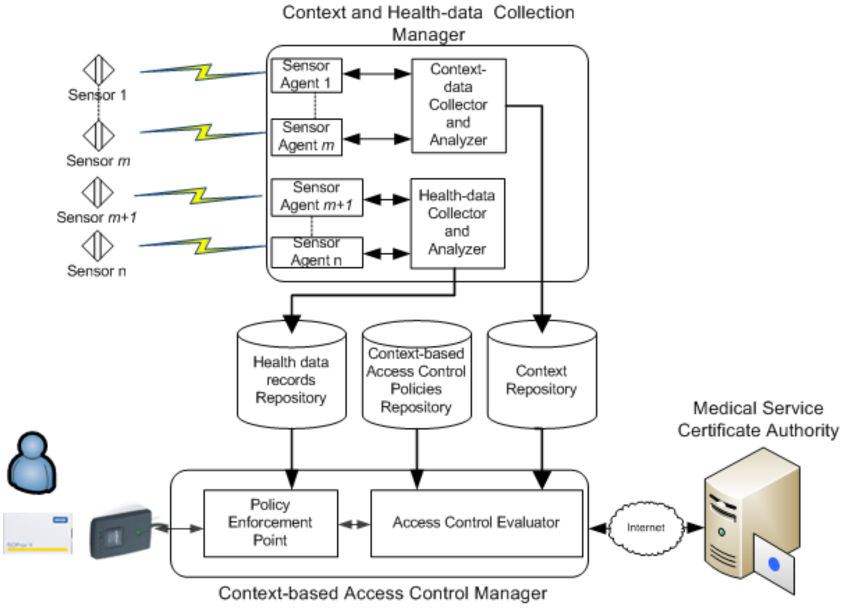
The *House_n* project from MIT [9] shows an example of proactive (or preventive) healthcare system using wearable biometric sensors and cameras to detect symptoms of congestive heart failures (CHF) which occur frequently in people over the age of 65. When symptoms, such as abnormal changes in weight, blood pressure, sleep patterns, etc., are detected, a proactive healthcare system can generate health alerts and recommend remedial changes in lifestyle (e.g., moderate level of exercises) to prevent CHF.

3.2. Access Control Models

Access control is defined as: “a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy”[10]. A number of access control models have been identified in the literature: mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC) [11]. In the MAC model, security levels (e.g., public, restricted, etc.) are associated to resources, and access levels are associated to users. A user’s access to a resource is allowed only if the user’s access level matches the resource’s security level. The DAC *model* defines users’ privileges over resources based on ownership relations. The owner of a resource decides who has access to the resource and what operations are allowed on it. An alternative approach to MAC and DAC is the RBAC model which provides more flexibility for specifying and managing users’ privileges. Each user, known as subject, is assigned one or several roles. Based on an assigned role, a subject can access a resource in conformance with the privileges granted to the corresponding role. A subject with a system management role defines the roles and the privileges associated to them. Variations to RBAC include Temporal-RBAC (TRBAC) [12] which uses time to support periodic role enabling and disabling and temporal dependencies among permissions, extended TRBAC [13] which includes the location and system status constraints, and the Generalized Role Based access Control (GRBAC) [14] which supports context in the authorization phase. GRBAC is similar to RBAC, but it additionally allows for incorporating the notion of object roles and environment roles with the traditional notion of subject roles.

4. Context-based Healthcare Framework

In this section we will present the software architecture of our context-*based* healthcare framework. We will also give a detailed description of every component of the architecture.



Context and Health-data Collection Manager
Sensor 1
Sensor *m*
Sensor *m+1*
Sensor n
Sensor Agent 1
Sensor Agent *m*
Sensor Agent *m+1*
Sensor Agent n
Context-data Collector and Analyzer
Health-data Collector and Analyzer
Health data records Repository
Context-based Access Control Policies Repository
Context Repository
Medical Service Certificate Authority
Policy Enforcement Point
Access Control Evaluator
Internet
Context-based Access Control Manager

Fig. 1: System Architecture

Context and Health-data Collection Manager: The Context and Health-data Collection Manager uses variant sensors to collect the context and health information from the occupants of a smart home. It is made of one Context-data Collector and Analyzer, one Health-data Collector and Analyzer, and one Sensor Agent for each data or health sensor.

Sensor Agent: The Sensor Agent (SA) is sensor-specific software (driver) that communicates with the controlled sensor to gather medical or context data and transforms it into a format that is understood by either the context data collector and analyzer or the medical data collector and analyzer. The sensor agent can also communicate sensor-dependant instructions to each sensor, such as changing the frequency or granularity of data collection.

Context-data Collector and Analyzer: The Context-data Collector and Analyzer (CCA) manages the collection and filtering of context data provided by the context sensor agents, performs analysis on the data, and stores the data into the database.

The Health-data Collector and Analyzer: The Health-data Collector and Analyzer (HCA) manages the collection and filtering of health information provided by the health sensor agents, performs analysis on the data, and stores the data into the database. Based on the collected data, the HCA might also trigger events such as dialling 911, or raising some warnings to get the attention of the data owner or the medical service provider to some concerns with the medical data.

The Context-based Access Control Manager: The Context-based Access Control Manager (CASM) acts as a Policy Decision Point (PDP) and a Policy Enforcement Point (PEP) for the system. It receives requests from the applications to access the health data, authenticates the identity of the data requestor, uses the data in the context database, and evaluates the access control policies stored in the policy repository to decide whether to grant or deny requests. The decision is passed to a Policy Enforcement Point (PEP) for enforcement.

Access Control Evaluator: The Access Control Evaluator (ACE) is the policy decision point in the system. When an application makes a request to the system to access the data in the database, the ACE contacts the certificate authority of the medical service provider to evaluate the identity of the requestor, and uses the context information to retrieve the policies in the database that apply to the current context. The decision to grant/deny access to the data is passed to the policy enforcement point for implementation.

Policy Enforcement Point: The Policy Enforcement Point (PEP) is the logical entity that accepts the request from an application that tries to access health data in the system, and passes the request to the ACE. When the ACE makes a decision, it passes this decision to the PEP to enforce it.

The Database System: The system requires the usage of three databases: a Health-data Repository, a Context-data Repository, and an Context-based Access Policy Repository.

Health-data Repository: The Health-data Repository (HR) stores the health data generated by the health data collector and analyzer. This data consists of the medical history of the person to which the medical sensors are attached. Such data might include electrocardiogram data, heart beat information, and blood pressure, to list a few.

Context data Repository: All the context information is stored in the Context-data Repository by the context data collector and analyzer. This data will help the ACE to make its decision based on the current state of the system.

Context-based Access Policy Repository: The Context-based Access Policy Repository database stores the context policies which are used in combination with the context data record to grant/deny access to the user's health data.

Service Provider Certificate Authority: The Service Provider Certificate Authority is responsible to issuing certificates such as from an RFID card to the paramedic. It is also responsible for confirming that the paramedic is on duty when he/she is trying to access the medical data of the user.

5. Conclusion & Future Works

The design of context-aware access control framework to medical data is a very particularly challenging problem and requires re-thinking of traditional subject-based access control solutions, e.g., access control lists and capability systems. In this paper, we have presented a detailed framework to provide access to the medical data of a user based on the identity of the data requestor, and the context of the data owner. We have already implemented the framework and we are currently collecting some experimental data which will be published later.

For future work, we will be working on elaborating our scenario. The scenario on which our current system is designed is fairly simple. It would be beneficial to add more multifaceted scenarios including a wider range of monitoring devices, a greater variety of medical ailments, and additional interested medical practitioners including specialists, nurses, etc. Our architecture is designed to be flexible to such variables, but can benefit from the test cases that result from the additional scenarios.

In addition, the entire purpose of this context-based access control system is to prevent unauthorized parties from viewing the personal medical information of the patient. While we have assumed that the data will be stored in a secure manner and all transactions will also be secure, our architecture would benefit greatly by including mechanisms for encryption and decryption as well as a digital-signature system to guarantee non-repudiation of transactions.

6. References

[1] E. Dishman "Inventing wellness systems for aging in place," IEEE Computer, 37(5), May 2004.

[2] N.R. Hooyman and H.A. Kiyak, "Social Gerontology, A Multidisciplinary Perspective," 6th ed., Allyn and Bacon, 2002.

[3] W.R. Jih, Y.J. Hsu, T.C. Lee and L.L. Chen , "A Multi-agent Context-aware Service Platform in a Smart Space," Journal of Computers 18(1), 45 — 60.

[4] M.E. Pollack, "Intelligent technology for an aging population: The use of AI to assist elders with cognitive impairment" AI Magazine 26(2) (2005) 9 – 24

[5] MIT Media Lab, "MIThril, the next generation research platform for context aware wearable computing," http://www.media.mit.edu/wearables/mithril/ (2003)

[6] Intel Research Seattle, "SHARP: A system for human activity recognition and prediction," (http://seattleweb.intel-research.net/projects/activity/)

[7] E.D. Mynatt, J. Rowan, S. Craighill, and A. Jacobs, "Digital family portraits: supporting peace of mind for extended family members," In Proceedings of the SIGCHI conference on Human factors in computing systems (CHI 2001) (2001) 333–340

[8] J. Rowan and E.D. Mynatt, "Digital family portrait field trial: Support for aging in place," In Proceedings of the SIGCHI conference on Human factors in computing systems (CHI 2005), New York, NY, USA, ACM Press (2005) 521–530

[9] Department of Architecture research group at the Massachusetts Institute of Technology, "House n: MIT home of the future," http://architecture.mit.edu/house n/ (2005)

[10] R. Shirely, "Internet Security Glossary," Available at http://rfc.dotsrc.org/rfc/rfc2828.html

[11] M. Ventuneac, T. Coffey, I. Salomie, "A policy-based security framework for Web-enabled applications", In Proceedings of the 1st international symposium on Information and communication technologies, pp. 487-492 Dublin, Ireland, 2003

[12] E. Bertino, P. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model", ACM Transactions on Information and System Security, vol. 4, no. 3, August, 2001, pp. 191-233.

[13] M. J. Covington, W. Long and S. Srinivasan, "Secure Context-Aware Applications Using Environment Roles," Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, May 2001, Chantilly, Virginia, USA.

[14] M. J. Moyer, M. Ahamad, "Generalized role-based access control," in: ICDCS '01: Proceedings of the The 21st International Conference on Distributed Computing Systems, IEEE Computer Society, Washington, DC, USA, 2001, p. 391.