Proceedings of the Federated Conference on Computer Science and Information Systems pp. 803–806 DOI: 10.15439/2017F261 ISSN 2300-5963 ACSIS, Vol. 11

Dependable Design for Elderly Health Care

Kasi Periyasamy
University of Wisconsin-La Crosse
La Crosse, WI 54601, U.S.A.
Email: kperiyasamy@uwlax.edu

Vangalur Alagar
Concordia University
Montreal, Quebec, H3G 1M8, Canada
Email: alagar@cs.concordia.ca

KaiYu Wan
Xi'an JiaoTong Liverpool University
Suzhou, China
Email: kaiyu.wan@xjtlu.edu.cn

***Abstract*—Health care systems have started using advanced technologies, such as Sensor Networks and Internet of Things (IoT), to make health care solutions affordable and easier to access. However, elderly patients who are unconvinced about its dependability hesitate to use the immense facilities provided by the advanced technology. A remedy to this problem is to make the health care system dependable and patient-centric so that patients can be convinced to trust the system. Towards achieving this goal, this paper defines a multi-faceted design, explains how the dependability properties can be integrated in it, and briefly illustrate it in a design pattern for sensors that can be used for an elderly home monitoring system.**

I. Introduction

WITHIN the health care sector, elderly health care is regarded as an emerging sector of concern [1], [2]. Although old age that defines "elderly" does not necessarily imply "ill health or disability", the risk associated with both ill health and disability increase as people grow older. A significant conclusion by recent reports is that the proportion of care givers (including income earners) to the elderly with risky profile will be decreasing, while the cost of giving care to the elderly will be increasing. Thus, modern advances in technology should be combined with human wisdom and ethics in order to create "smart systems" that provide *trustworthy* health care for the elderly. In computing literature, *trustworthiness* is defined as the *system property* that denotes the degree of user confidence that the system will behave as expected [3], and *dependability* is defined as "the ability to deliver services that can justifiably be trusted" [3], [4]. A comparison between the two terms presented in [3] has concluded that the two properties are equivalent in their goals and address similar concerns, and suggests that the terms *trustworthiness* and *dependability* can be used interchangeably.

Electronic Patient Records (EPR) and Sensor Networks may be regarded as the two significant moves to use advanced technology in health care. Sensor networked systems, currently developed by several industries and universities [5], [6], have immense potential to provide remote patient monitoring and home care of the elderly whenever and wherever necessary. Because the elderly will become dependent on these technologies, it is necessary to convince them that their expectations are met, in the sense that the services provided to them satisfy the privacy concerns prescribed by them, their personal data is secure and safe, and service providers follow ethical principles. In this paper we explore these issues with particular emphasis in the design of elderly home care.

II. Trustworthiness and Dependability

The most common issues regarding health care needs of elderly are *receiving timely remote care*, *getting daily personal care*, *getting support for loneliness and abuse prevention*, and *acquiring basic health care knowledge*. These requirements must be met without compromising their safety, privacy, and dignity. So health care actors must provide these services in different contexts in a trustworthy manner and respect medical ethics. In addition, every patient should be given a mechanism to state, as part of her EPR, what health information can be shared or disclosed, with whom and when. Using this information, the health care actors should act faithfully in serving the elderly and earn their trust. The system, that consists of health care actors and other technology enabled artifacts should be dependable (trustworthy) in the sense it ensures *safety*, *security*, *survivability*, *privacy*, *availability*, *reliability*, and *accountability* for its clients. Following are some examples of safety policies: (1) Elderly homes should be well-equipped with smart devices; (2) Only certified medical devices that are interoperable should be part of Integrated Clinical Network (ICE); and (3) Care givers should monitor elders in order to protect them from physical and psychological abuses. RFID and Sensor network technology may be used to monitor and prevent unsafe situations in patient care. Security is a system level property that ensures the implementation of appropriate methods to protect confidentiality, authenticity, and integrity of health data of patients, vital research and administrative data of the institution. Survivability refers to the capacity of a heath care system to fulfill its mission, in a timely manner, in the presence of attacks and emergency situations including failures to its infrastructure. Privacy is a user-centric issue. Every human actor in the system has the right to define the information that they (do not) want to share, how they want to share and in what contexts, and how the information may be used and by whom. Availability and reliability are factors arising from system robustness and resilience to external attacks and internal failures. Accountability is the ability of the system to trace the history of every action in the system's life cycle.

III. Extending Role Based Access Controls with Context for Protecting Elderly Home

We conceptualize an elderly health care in three layers. The lowermost layer is the "Elderly Home" (EH), the middle layer is the "Cloud" (CC), and the top layer is for "Health Care

IEEE Catalog Number: CFP1785N-ART ©2017, PTI

Service Provision" (HCSP). In EH layer, patients and their caregivers are coordinated and monitored by "trustworthy" sensory network. The layer CC represents the server where all medical information from EH layer is received, persisted, and made available to HCSP layer. The actors in HCSP layer are Health Care Providers (HP) which includes Physicians (PH), Emergency Care (EC), Pharmacists (PA), Clinical Staff (CL), and a variety of actors with administrative roles. The EH encloses two collections of entities - a collection of elderly patients (EPs) and a collection of care givers (CGs). In our system, a care giver needs to have a unique identification. Each EP also has a unique identity. Both EP and CG have their own profiles. The profile may include personal information as well as system-related information. There is a many-to-many relationship between EP and CG within EH. This means that a care giver in EH may monitor several patients and a patient may be monitored by several care givers. Each EP has a unique *Electronic Patient Record* (EPR). In addition, each EP may be monitored by a set of sensors. Dependability of EH involves protecting its EPR and its associated sensors in EH layer. To achieve this goal, we use "Contextual Role Based Access Control" (CRBAC).

Standard bodies in the US have chosen the Role Based Access Control (RBAC) model [7], [8] to enforce access control policies in traditional health care IT systems. In RBAC, roles of subjects and their access rights are predefined. Exceptions are emergency (unanticipated) situations that threaten patient safety. In such situations, the need arises to override the predefined set of access rights so as to assure patient safety. In [9] a *Break The Glass* (BTG) approach is used to override predefined access controls in emergency situations and argued that it has the *non-repudiation* property. Yet, RBAC is not a "privacy-aware" method. As an example, it is possible for a healthcare actor (playing a role) to comply with access control policies and retrieve personal health information of patients at instances "when they may not be required" for treating the patient and then misuse the information. Recognizing this flaw, *context* that includes "purpose" attribute was introduced [10] into the RBAC model. This extended model is called "Contextual Role Based Access Control" (CRBAC). Informally, a context includes information on "what" (request), "where" (location/spatial), "when" (time, day, and duration), "why" (purpose), and "who" (role). A "contextual constraint" is a conjunction of "constraints" where each constraint is expressed as a $\langle$ key, value $\rangle$ pair. The "key" is one of the five parameters: "what", "who", "when", "where" and "why". The "value" is a boolean expression. As an example, consider a care giver c who works in the same department where a patient with id pid is admitted/registered. Assume that the care giver requests read and write access to a sensor with id sid. Somewhere in the records, it should have been mentioned that this care giver is attending the patient. If the patient is a physician, the care giver must have a minimum service record of 5 years. If the care giver is a nurse, she must be the head nurse of the department. The contextual constraints for this problem can be stated as follows: (1) what: readAccess (pid, sid) $\wedge$ writeAccess (pid, sid); (2) who: $\exists c : CareGiver \bullet$ department(c)=department(pid) $\wedge$ attending(c,pid) $\wedge$ (c.role='physician' $\Rightarrow$ service(c) $\geq$ 5) $\wedge$ (c.role='nurse' $\Rightarrow$ headNurse(c,department(c))='yes'; (3) when: time='alltime'; (4) where: location=room(pid); (5) why: purpose='monitor'.

IV. Secure Elderly Home

The three aspects to be protected in EH are (1) EPRs, (2) Sensor Network, and (3) Care giver actor (CG).

Protecting EPRs: The EPR of a patient is either created by the patient or by care givers in charge of the patient. The EPR includes the health status, personal information, a list of friends and family members authorized to share patient information, and names of medical staff and care givers attending the patient. If EPR is prepared by care givers, then it is legally certified that persons who prepared the EPR will use it ethically for patient care. The EPR of a patient can be encrypted and saved in a mobile device associated with the patient, and care givers of the patient are given access to this device. It is uploaded to CC, from where physicians and other health care providers may access it, and may add details on the services provided to the patient. Here we briefly discuss the safety, security, and privacy issues of the EPR stored at patient's computing platform.

Every patient has a unique mobile unit. The pair (PID, MID) constitutes the key for encryption in EPR, where PID refers to the patient identity and MID refers to the mobile unit identity. This key is also used for authenticating others to access EPR. The authentication rules are set by the patient, in consultation with the care giver, so that any desired part of EPR information may be disclosed in a privacy-preserving manner when CRBAC is used to enforce access to the information. The mobile unit used by the patient uses RAS to encrypt EPR information while transmitting to CC. It may use its own internal (hard-wired) method for encrypting EPR and store it locally. As a consequence, neither the patient nor any of her authorized users need to worry about data integrity. All users, except the patient, will have "read only" access to disclosed information. Only the patient or her authorized agent has the right to add, delete or modify the information in the EPR. It is expected that the agent (relative or care giver) will be bound by ethical principles while following the instructions of the patient. To safeguard against threats, the profile of the agent may be collected in each context of agent's access to the mobile unit of the patient, and the history of access may be audited periodically. Emergency situations for each patient may be enumerated. For each emergency context an appropriate access rule should be provided. For this discussion, an emergency situation is one in which the authenticated person has the right to access the EPR but may not have the right to perform a task related to the patient's care (e.g., an operation on the patient). The following steps are followed in emergency situations: When an authorized person signs in, the system at first *denies* access because the current context is an “emergency” context (not anticipated earlier). It checks the “history of access” of the person to verify whether or not any violation of ethics was recorded; if the answer is “yes”, the system sends a “SOS” message to the supervisory control through the Cloud and “freezes”. If the answer is “No”, and the user agrees to “non-repudiation” (recording her access and reporting to supervisory system), she is given access right to perform the requested task. In the “Yes” case, the system remains “frozen” until either a response is received from the supervisory system or receives biometric data of the current user; in the former case, the system follows the supervisory protocol; in the latter case, the system uses the biometric data for non-repudiation procedure.

Protecting Sensor Network: A variety of sensor types are used in an EH. Broadly classified, these are (1) bodyware sensors, and (2) external sensors. Each EP has a unique ID, a data collection inspector (DCP) and has one or more sensory devices. The design details of DCP and sensor, described below, contribute towards dependable EH design.

Sensor: In [11] we have introduced “Health Care Design Pattern” paradigm, and illustrated the design of *Sensor Design Pattern* (SDP). SDP has been designed using three well-known software design patterns - Abstract Factory pattern, Observer pattern and Strategy pattern. It contains a sensor hardware that actually gathers the data, a RF chip to transmit the data out of the sensor, and a micro controller that coordinates the activities of the sensor hardware and the RF chip. In addition, the micro controller also enables a user to store, retrieve and modify authentication data to protect data access from the sensor. Using appropriate protocols such IEEE standard 802.15.2.6 - Level 3 which requires both authentication and encryption, data access from a SDP can be tightened. Though any amount of details can be stored and processed in the micro controller, it is preferable to store only minimal necessary information and to keep processing within the micro controller to the minimum in order to save battery life of the sensor and to protect the sensor from adversaries [12]. Typically, for a sensor used in an elderly home, the following information is sufficient: patient ID, sensor ID, authentication data to access the sensor (includes the authorized entities such as devices, software entities and humans, who can access the data from the sensor), and a log of transactions where each log includes the date and time of access as well as the ID of the entity which accessed the data from the sensor. While authentication data provides security to the sensor, the list of authorized entities enables the sensor to protect the privacy of data collected by the sensor. The authentication details within the micro controller can be described in the form of contextual descriptions in which case the SDP will act as an independent entity by itself. Instead, we suggest that the authentication details should be kept to the minimum in the micro controller (to prolong the life of the hardware in SDP) and more contextual details should be loaded in DCP (discussed next). System-related information such as encryption keys and code implementing secure communication protocol between the sensor and authorized entities will also be stored in the micro controller.

Data Collection Inspector: The Data Collection Inspector (DCP) acts as a front end that manages data collection from various sensors associated with the patient and also enables data manipulation stored in SDPs. Generally, a mobile device such as a smart phone or a laptop acts as DCP. It includes the profile of the patient, the set of all sensors associated with the patient, the list of other authorized entities who will use these sensors, and a contextual description for data access from each sensor. The DCP is responsible to gather data from each SDP and provide authenticated access to it to the entities in EH layer and through CC to entities in other layers. It has built-in mechanisms for data authentication, data integrity, and data privacy. Another important functionality is that it periodically transfers log transactions from each SDP to both local and CC units. Requests for data access from the sensors associated with an EP should be made through the DCP of the corresponding EP. Each request must specify the sensor ID from which data is requested and parameters required for constructing the contextual description. After validating the request based on the context, the DCP executes a command to gather the data or provides a summary of already gathered data from the particular sensor. The DCP acts as the console for EP so that the patient may change privacy and security parameters at any time. Since most patients are not computer savvy, it is important to design the DCP user interface that is easy to use and easy to operate. Thus, the DCP user interface will provide simple dialogs for the five parameters by which the patient can recognize the meaning of each parameter and provide the required information for each parameter. A patient who is unable to use the DCP interface can be substituted by one of those authorized by her in her EPR. This is achieved in our design through role delegation.

Care Giver Authentication: An entity with *Care Giver* (CG) can monitor a patient’s status through the sensors associated with the patient, only after an authentication of her credentials. Each entity in CG role must have been registered in the patient’s DCP. Every care giver attending a patient must be a member of the list of care givers included by the patient in her EPR, which being part of the DCP is controlled by the patient. Each care giver is given an Access Control Point (ACP) through which the care giver communicates with the corresponding DCP of the patient. Like DCP, each ACP also has a unique ID. When a care giver wants to access a patient’s status, the care giver makes a request (including purpose/why) through her corresponding ACP. This request will be checked against the access control list of the corresponding DCP. If matches, the request will be converted internally into a contextual description and the corresponding DCP will execute the request. Like the DCP for a patient, the ACP thus acts as the front end for a care giver. It is generally installed on a mobile device or a laptop. Therefore, a care giver has complete control over his/her ACP and can set up an initial profile. This profile can include the set of patients to monitor and hence the corresponding DCPs to access.

V. Conclusion

Elderly health care is a critical sub-sector of health care infrastructure. From the review of many existing health care systems and mobile apps that support them [13], [14], [15], [16] we are convinced that they are focused on providing information to and aiding medical staff, but not in improving quality of care. More importantly, these systems do not guarantee the trustworthiness perspectives. From a user-centric view of system usability, these systems are not fully embraced by elderly patients either because their interfaces are complex to learn or because the patients do not have sufficient knowledge and technical skills to use them. The root of this problem can be traced to the early stages of designing these systems, wherein patient-centric modeling decisions have not been made. In our short exposition in this paper, we have explained how quality of care can be improved by instituting a dependable elderly home infrastructure and integrate it with CC for remote health care service provision. A summary of results are as follows:

Safety: In an elderly home environment, there are two groups of people - patients and care givers. A patient's safety is ensured by using only certified medical devices which are operated by only authorized people. While selection and certification of medical devices is beyond the scope of this paper, the DCP of the patient protects her from unauthorized people accessing the sensors. Further, the sensor logs are stored inside and possibly in the DCP as well. This, to some extent, can be used to trace attacks by adversaries. Since care givers monitor the patients remotely using their ACPs, it is guaranteed that they are free from contamination and infections.

Security: The use of contextual information in authenticating sensor data access is the biggest advantage of our approach. Every access to the sensor is protected by the patient's DCP. The "who" parameter of the contextual description ensures that only registered people can access the data, and the "when" parameter ensures that these people are allowed to access the data at the time specified in the contextual description. Thus, the role-based access model along with the contextual description ensures high security.

Privacy: All sensors are protected by the DCP of the patient. The patient (or the representative of the patient who is legally authorized) has ultimate authority of issuing access rights to the care givers and others. In addition, the patient also has the ability to change the settings on access rights at any time by changing the corresponding contextual description. Therefore, we claim that our model ensures privacy of patient information.

Availability: The system is considered to be "unavailable" when any sensor data is not accessible by a role who is authorized to access. We claim that the sensors and the DCP can be configured to log sensor data gathering as well as to log transactions at appropriate time intervals. These can be transferred to the cloud via EH and can be automatically monitored to be continuous. If there is a break or gap in the log, the system must generate an alarm and then the corresponding role can interfere the sensor network to find out the cause. Thus, our design is capable of ensuring "availability".

Accountability: This property is important to identify the cause and the role when something goes wrong. As stated earlier, the log transactions will help trace the identity of the role who accessed and the duration of the access, from which it should be possible to determine who is accountable and for what. As we stated earlier, ethical behavior of all roles including patients are covered by this property.

References

[1] World Health Organization, "Definition of an older or elderly person," http://www.who.int/healthinfo/survey/ageingdefnolder/en/, 2015, [Online; accessed 29/01/2015].

[2] "mhealth: New horizons for health through mobile technologies," http://www.who.int/goe/publications/goe_mhealth_web.pdf, June 2011, [Online; accessed 29/01/2015].

[3] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11–33, January-March 2004, doi: 10.1109/TDSC.2004.2.

[4] D. Jackson, "A direct path to dependable software," *Communications of the ACM*, vol. 52, no. 4, pp. 78–88, April 2009, doi: 10.1145/1498765.1498787.

[5] Intel, "Integrated medical hospital," http://www.intel.com/business/bss/industry/healthcare/index.htm, Tech. Rep., [Online; accessed 29/06/2014].

[6] J. Chapman, "Sensor systems research," http://www.gla.ac.uk/media/media_227573_en.pdf, Tech. Rep., 2011, [Online; accessed 27/04/2017].

[7] D. Ferraiolo and R. Kuhn, "Role based access control," in *Proceedings of the National Computer Security Conference*. NIST, 1992, [Online at http://carc.nist.gov/rbac/ferraiolo-kuhn-92.pdf].

[8] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. Youman, "Role based access control models," *IEEE Computer*, vol. 29, no. 2, 1996, doi: 10.1109/2.485845.

[9] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, and E. Oliveira-Palhares, "How to break access control in a controlled manner," in *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems (CBMS'06)*. IEEE, 2006, pp. 847–854, doi: 10.1109/CBMS.2006.95.

[10] V. Alagar and K. Wan, "Context based enforcement of authorization for privacy and security in identity management," in *Proceedings of the First IFIP WG 11.6 Working Conference on Policies & Research in Identity Management (IDMAN 2007), IFIP Publications (2008)*, 2008, pp. 25–38.

[11] K. Periyasamy, K. Wan, and V. Alagar, "Healthcare design patterns - an internet of things approach," in *Proceedings of the 32nd International Conference on Computers and Their Applications (CATA 2017)*, March 20-22 2017, pp. 293–299.

[12] D. Halperin, T. Kohno, T. Heydt-Benjamin, K. Fu, and W. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, January/March 2008, doi: 10.1109/MPRV.2008.16.

[13] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," in *International workshop on wearable and implantable body sensor networks (BSN'04)*, vol. 5, Imperial College, London, 2004.

[14] J. W. Ng, B. P. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, and G.-Z. Yang, "Ubiquitous monitoring environment for wearable and implantable sensors (ubimon)," Imperial College, London, Tech. Rep., 2004.

[15] "Care coordination and communication software for senior care — caremerge," http://www.caremerge.com/, CareMerge, [Online; accessed 29/01/2015].

[16] J. Ma, C. LeRouge, J. Flaherty, and G. DeLeo, "Use smart phones to promote diabetes self management:robust elderly in urban and rural china," http://www.cadaproject.com/, 2010, [Online; accessed 06/05/2016].