J Med Syst (2012) 36:291–300
DOI 10.1007/s10916-010-9475-2

ORIGINAL PAPER

Emergency Access Authorization for Personally Controlled Online Health Care Data

Tingting Chen · Sheng Zhong

Received: 12 January 2010 / Accepted: 11 March 2010 / Published online: 7 April 2010

Abstract Personally controlled health records (PCHR) systems have emerged to allow patients to control their own medical data. In a PCHR system, all the access privileges to a patient's data are granted by the patient. However, in many emergency cases, it is impossible for the patient to participate in access authorization on site when immediate medical treatment is needed. To solve the emergency access authorization problem in the absence of patients, we consider two cases: a) the requester is already in the PCHR system but has not obtained the access privilege of the patient's health records, and b) the requester does not even have an account in the PCHR system to submit its request. For each of the two cases, we present a method for emergency access authorization, utilizing the weighted voting and source authentication cryptographic techniques. Our methods provide an effective, secure and private solution for emergency access authorization, that makes the existing PCHR system frameworks more practical and thus improves the patients' experiences of health care when using PCHR systems. We have implemented a prototype system as a proof of concept.

Keywords Electronic health record · Personally controlled health records · Access authorization · Emergency

T. Chen · S. Zhong (✉)
Department of Computer Science and Engineering,
State University of New York at Buffalo, Amherst,
NY 14260, USA
e-mail: szhong@cse.buffalo.edu

T. Chen
e-mail: tchen9@cse.buffalo.edu

Introduction

Traditionally, physicians keep the records of patients, such as progress notes, prescription history and test results, on paper. Local paper-based medical records are difficult for the communications between different physicians and healthcare institutions. Electronic health record (EHR) has been brought forth to improve health care quality, efficiency, and patient safety. Under the Health Information Technology for Economic and Clinical Health Act (HITECH; http://waysandmeans.house.gov/media/pdf/111/hitech.pdf), by 2014, hospitals and physicians will need to have adopted electronic health records. American Recovery and Reinvestment Act of 2009 (ARRA) [1] provides substantial financial incentives to encourage helping health care providers adopt and make meaningful use of EHR technology, so that they can give better care and their patients' experience of health care will improve. Architectures for ubiquitous communications of EHR has been studied (e.g., [3, 10, 11]; http://telecom.ntua.gr/~HARP/HARP/HARP.htm), which facilitates the high quality health care with all pertinent clinical data on a patient.

As a special type of EHR, personally controlled health records (PCHRs) [18, 19, 24] enable individual patients to aggregate, securely store and access their own electronic health records from various places. PCHRs are kept by third parties outside the medical care system, for example, in online repositories such as Google Health (https://health.google.com/health/), Microsoft Vault (http://www.healthvault.com), or by large companies willing to keep PCHRs for their employees, such as Dossia (www.dossia.org). Each individual patient can subscribe to the health care records from physicians, clinics, laboratories and pharmacies,

aggregating them into the PCHRs. When a clinic requires the most updated pertinent clinical information of the patient in order to give health care, patients can grant the PCHRs access to the clinic. In general PCHRs motivate patients to cooperate actively in their medical care by taking control their medical information. Moreover, the ubiquitous and shared access to PCHRs improves the efficiency of the medical care system and lowers the cost of communications.

Some system architectures for using PCHRs in the medical care system have been proposed, e.g., a web-based system Indivo (http://indivohealth.org/). Like other PCHR systems, Indivo enables a patient to indicate in the system which other users (such as treatment sites) have particular privileges on specific portions of the records. Normally, if a patient goes to a certain clinic for the first time, after scheduling a treatment appointment, the patient grants this clinic with the access of the related health information in the PCHR system, such as syndrome and allergy history. In this way, the patient can receive good treatment given that clinic has the information needed.

However, in many cases, treatment need is urgent and it is impossible that the patient has the time or ability to get connected to the internet and grant the access to the clinics. For instance, a patient who has passed out is sent to the emergency room where the patient has never been. Unfortunately, since the clinic has not been authorized to any part of the patient's data in the PCHR system, it is extremely difficult to perform high quality treatments. Moreover, it is also almost impossible to obtain the pertinent information from other clinics where the patient has been, under the coverage of the privacy and security regulations of HIPAA [12]. Now consider an even worse case, in which the clinic does not have the account in the PCHR system to log in, and thus it does not have a place to send its request for the patient's medical care data. Creating a new account usually takes a substantial amount of time. It usually has a long and secure procedure to verify the identity and gather all the information to build a database entry for a newly joined clinic. Indeed, making sure the security of the PCHR system is necessary and important. However, it significantly impedes the process of emergency medical treatment, which may cause severe consequence to the patient. Hence we can see that restricting the access control to the individual patient may cause serious problem when the patient's participation is impossible.

In this study we solve the problem of on-demand, especially emergent, access authorization to PCHRs in the absence of the PCHR owner. Our work can be viewed as an important improvement to the existing PCHR systems. In existing PCHR systems, for example PING [21], the authorization module defines the logic for determining whether an access is allowed, based on some pre-defined polices. When an emergent access request occurs which is not allowed by the pre-defined policy, it will be denied by the authorization module. As far as we know, we are the first to consider the emergent access problem in the absence of the PCHR owner, for designing a more practical PCHR system.

We distinguish two cases for emergency access authorization, based on whether the requester can be recognized by the PCHR system. Correspondingly, we propose two emergency access authorization methods, each for one case, respectively leverage the weighted voting [23] and the online source authentication technique [6] in cryptography. They provide an effective, secure and private solution for emergency access authorization to make the existing PCHR system framework more practical and improve the patients' experiences of health care when using PCHRs system. We have implemented our methods in a prototype system.

Background

In the context of EHR system, extensive study has been done on protecting the privacy of patients' data in cross-institutional scenarios, e.g., [4, 9, 13, 16]. The majority of these works are using access-control-based approaches. The Role-Based Access Control (RBAC) was proposed by Sandhu et al. [20]. In RBAC model, instead of specifically assigning the privileges to each user, the users are grouped into roles, and each such group is associated with a number of privileges. The RBAC approach is widely adopted in the health care domain. In the community of medical informatics, the study mostly focused on access role definitions in order to better protect the patients' data. For example, similar to our idea of emergency contact group, in [9], the authors characterized structured roles, offering solutions that allows access only to authorized entities, according to the authorizations supervised by a security committee. Another good example is that, in [16] Motta and Furuie proposed a contextual role-based access control authorization model. They defined a role hierarchy with inheritance of authorizations and modeled the types of data found in an EHR according to clinical content. We note that all of the works above are for EHR systems. None of them aim to solve the emergency access authorization problem, which is unique in the PCHR systems. In our work, we not only design a role model that deals with the emergency requirement,

but also provide a cryptographic-based solution for a tougher situation, i.e., the requester is an outsider.

There are also numerous existing mechanisms for preserving the privacy of database records [2, 5, 7, 8, 14, 15, 22]. These works can be broadly classified into two categories. The first category of works focus on preserving the privacy of individual data records when they are used in mining a large group of data for an aggregate study, e.g., [2, 7, 8, 14]. For example, in [8], Du and Zhan propose a randomized response based privacy preserving ID3 decision tree classification algorithm. The second category of works aim to anonymize the identities when collecting or publishing their data, e.g., [5, 15, 22]. For example, in [5], an anonymity-preserving data collection protocol is proposed, which is secure in the malicious model without relying on zero-knowledge proofs. However, it is difficult to directly adopt these approaches mentioned above in the PCHR system, because the main idea of these works is to hide the identity among many peers in order to protect privacy. Since each patient's data stored in PCHR system is independent from others' and especially the emergency access request is highly individual-oriented, the existing solutions for preserving the privacy of data records can not be used here. In [17], Narayanan and Shmatikov propose an obfuscation algorithm that ensures a new notion of privacy, group privacy. Nevertheless their construction of obfuscated databases are non-interactive, i.e., except those explicitly permitted queries, all other queries become computationally infeasible. Clearly, current PCHR systems are interactive and thus the technique in [17] is not applicable to our problem either.

Challenges

To design the emergent authorization method for personally controlled health care data, we must address some challenges raised by the requirements of the existing PCHR systems and HIPAA regulations, so that our solution can be incorporated and become practical for real cases in health care systems. In particular, we focus on the three most important factors as follows.

- **Security:** In emergency cases, if the entity is not recognized by the existing system (or the PCHR owner), the PCHR system should still be able to give the privilege of temporal access to the entity, if some strict constraints are met to guarantee that the usage of the health care data is necessary and the entity will use it appropriately. Therefore, the system should be able to verify the claimed identity of an entity who has sent the emergency access request, either a person or an organization, in the absence of the PCHR owner. Otherwise, fake requests by fake entities may lead to the unnecessary reveal of patients' health data. Some malicious parties may even personalize others which will cause further serious damage to the PCHR system.
  In addition to the authentication requirement, another security requirement is to protect the data integrity of the emergency access request and response. For example, in some cases, some malicious party may have the ability to capture an emergency access request by a clinic. If it modifies the request information to something different from the original request, then the system may consequentially send invalid response or even worse, lose the access request.
- **Privacy:** The system should preserve the privacy of the patients. In particular, if a clinic inquires about the health care data of a patient, it should be that no one but the patient and the trusted parties can know what kind of health data has been requested.
- **Effectiveness:** Even though the patient cannot participate in the emergency access authorization process, it should be able to review the authorization history afterwards. The system should be effective in that the rate of the unsatisfactory emergency access authorizations should be low to make sure that the emergency access is still under the patients' control.
- **Timely Response:** The authentication and access privilege granting process should be done within a reasonable amount of time, because otherwise the emergent access authentication method will lose its advantage of timely response in providing high quality on-demand treatment.

Methods

To allow the emergency access authentication to the PCHRs without the presence of the patient, we present secure and privacy-preserving emergency access authorization methods. We provide a solution for each of two cases: a) the emergency access requester can be recognized by the PCHR system (i.e., has an account), but has not obtained the privilege to read the patient's health care data; b) the requester is not recognized by the PCHR system. The key idea of both solutions is to distribute the right of granting access, to some trusted parties, such as family and friends, clinics and physicians that the patient is familiar with and thus trust.

In the rest of the paper, we call them the emergency contact group (ECG) for each patient.

When emergency access authorization is needed by a certain medical care center, it sends a request to the PCHR system to access the PCHRs of the particular patient, if the clinic has an account in the PCHR system where the medical care data of the patient stores. In this case, we apply a weighted voting algorithm among the emergency contact group members to decide whether the access request should be granted. If the voting result indicates that all or most of the emergency contact group members are willing to accept the request, then the PCHR system grants the requester temporary access to the patient's data, otherwise it rejects the request. For this part of solution, we choose not to directly grant some clinics with the temporary access right by the patient beforehand in the existing PCHR system. It is mainly due to the reason that the patient does not know when and where the emergency health care treatments will be needed. Hence, if the temporary access right is given in advance, there must be cases that some temporary access is actually never needed in the real world. Then it increases the probability of abusing the temporary access by some medical care providers that the patient is not familiar with. Therefore, we present an emergency access authorization solution in the PCHR system, which is on demand and privacy preserving. Certainly, after the emergency medical treatment, the patient is able to view the temporary access history recorded in the PCHR system. We will describe the weighted voting algorithm used in our method in Section "Weighted voting" and discuss the design details of this on-demand method in Section "Results".

When the clinic does not have an account in the PCHR system where the patient's medical care data stores, it becomes even more challenging to design an authorization method. We apply an advanced cryptographic technique that allows the requester to broadcast its emergency need message using a secure and privacy preserving algorithm. Our method guarantees that only the trusted parties by the requester are able to read the request message and they can verify the identity of the requester. If they are in the emergency contact group of the patient, they will request to be a proxy of the requester in the PCHR system. When there are sufficient number of requests of becoming a proxy for an outside medical provider, the PCHR randomly pick one of them to be the proxy of the requester to read and update the medical care data of the patient. Our method is based on a core component of source authentication algorithm, [6]. Now we first describe this secure and privacy-preserving authentication algorithm Source authentication, and then in Section "Results", we present in detail how this algorithm can be adopted in our method.

Weighted voting

When the emergency access request is sent to the PCHR system by a certain clinic, there will be a weighted voting scheme running among the patient's emergency contact group. A weighted voting scheme is characterized by three components: the voters, the weights and the threshold. The N voters $(P_1, P_2, \cdots, P_N)$ are the emergency contact group members for a particular patient. A voter's weight w represents the importance of the vote by this voter when aggregating the votes. The patient assigns a weight to each emergency contact group member, based on how trustworthy the group member is and how the patient values the vote by this member when making the emergency access authorization decisions. The threshold q is the minimum voting score overall to accept the access request.

Formally, we have

$$t = \sum_{i=1}^{i=N} w_i V_i,$$

where for each voter i, V_i is the vote towards a request and w_i is the weight of voter i. In Section "Results", we will discuss how each vote V_i can be computed in an reliable and efficient way. t is the final voting score for a request. We can see that t is the weighted sum of all the votes from the voters. If the final voting score is above the threshold q, (i.e., $t > q$), the request is accepted and then the requester can have temporary access to the patient's medical care data in the PCHR system. Otherwise, the request will be rejected.

Source authentication

Now we describe a source authentication algorithm [6] applied in our method to deal with the case that the emergency access requester is not in the PCHR system. The source authentication is used when the access requester sends the help messages to its partners, outside the PCHR system. Its partners may have the privilege to the patient's data in the PCHR system and can perform as a proxy for the access requester. Here we define that all the partners and the access requester form a group. A group authentication scheme is used when a partner receives a help message (containing the patient information) from the requester, to make

sure that the message is indeed transmitted from one of his partners and the receiver knows who is the sender. Moreover, only the partners can understand the content of the help message; The help messages are just meaningless data to other receivers who are not in the partner group.

In the following we describe the source authentication technique used in this paper.

- **Initialization** The group uses l primary keys $< s_1, s_2, \cdots, s_l >$. $l = O(w\log(1/q))$, where w and q are security parameters defined in the group. Each key s_i defines a pseudo-random function f_{s_i}. Each partner u in the group holds a subset R_u of the primary keys, such that the probability of each primary key s_i to be included in R_u is $1/(w+1)$. R_u will be used to verify the message when the partner u receives one. Each partner u also has a set of secondary keys $< f_{s_1}(u), f_{s_2}(u), \cdots, f_{s_l}(u) >$. The secondary keys are used when the partner u intends to send a help message to other partners in the group.
- **Message Authentication** When a partner u sends a message M, it computes an authentication using each secondary keys, and attaches all the l authentications to the message M. u sends out the message and authentications sequence, denoted as $M, MAC(f_{s_1}(u), M), \cdots, MAC(f_{s_L}(u), M)$.
  When a partner v receives a message, it computes all the secondary keys of u with primary key that v holds, using the pseudo-random function for each primary key. It then verifies all the MACs which are computed using these keys.

Results

In this section, we present our emergency access authorization method in details which utilizes the weighted voting and source authentication techniques. In Section "Emergency contact group and requester's partners group", we describe the emergency contact group and requester's partners group, and their relationship as well. In Section "Emergency access authorization for insiders" and Section "Emergency access authorization for outsiders" we respectively present our emergency access authorization method for two cases, i.e., the requester has an account in the PCHR system and otherwise. We implement a prototype of our proposed emergency authorization methods, using Microsoft Visual Studio 2005.

Emergency contact group and requester's partners group

An important component in our method is introducing an Emergency Contact Group (ECG) for each patient, storing in the PCHR system. The initialization of an emergency contact group include the following steps.

- **Picking ECG members** Patients choose their trusted actors in the PCHR system as the ECG members. The members can be individuals like the family and friends of the patients. The patients can also pick the organizational actors in the PCHR system (e.g., doctors, clinics, physicians) who have the access authorization to the patient's health records. The patients define different levels of power for ECG members by their weights as described below.
- **Assigning weights to each ECG member.** Some ECG members may be more familiar to the patient and thus more trustworthy, so we introduce ECG member's weight and rank to represent how the patient values the ECG members differently. After choosing ECG members, the patient decides the rank of each member, in the order of their trustworthiness. By default, the system assigns a weight $\frac{N-r_i+1}{N}$ to each member i, where N is number of ECG members and r_i is rank of i. The patient can also assign a weight w_i for each ECG member i. Each weight is limited in the range $(0, 1]$, i.e., $0 < w_i \leq 1$. If patients assign weights by themselves, the member ranks are no longer used. A ECG member with a higher weight will play a more important role in the access decision making when the patient is absent.
- **Assigning vote threshold.** The vote threshold indicates overall to what extent the patient trusts the decision by the emergency contact group. The system has a default threshold value as $\frac{1}{2}N$. Patient can also assign thresholds by themselves. In this case, the system default threshold is no longer used.

Requester's partners group can be formed outside the PCHR system. For example, if two medical care center have cooperation, or they are simply within the same association, they can form a partners group.

Figure 1 illustrate the relationship between patient's ECG members and the requester's partners. As we can see, the requester may be a partner with some of the ECG members of the patient. Although the requester does not have access privilege to the patient's health record in PCHR system, it can get help from those who are at the same time the ECG members of the

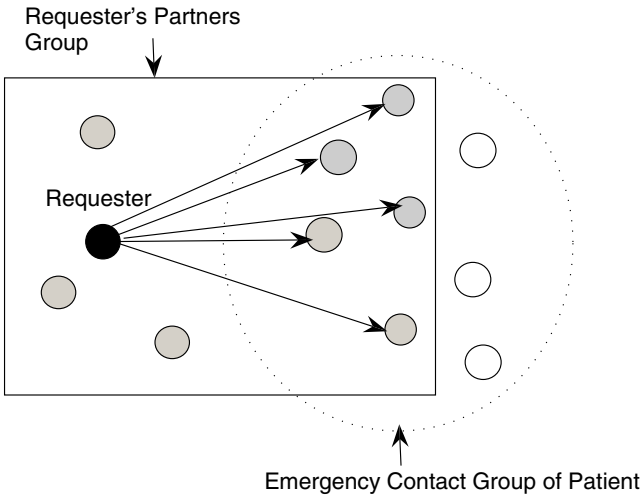

Fig. 1 Illustration of the relationship among the Patient, Emergency Contact Group (ECG) and the requester's partners group

patient and partners with the requester, based on the trust between the patient and the ECG group members.

Figure 2 shows the screenshot of the page where the patient adds a new emergency contact group member and inputs the member information in our emergency authorization prototype.

Emergency access authorization for insiders

Figure 3 summarizes the work flow of emergency access authorization for the PCHR system insiders. Within the PCHR system, requester first sends its request to the authorization module, asking for emergency access authorization for patient *A*. Then the authorization module looks up the emergency contact group members of patient A. It sends the patient and requester's information to the weighted voting scheme, which will perform a weighted voting scheme, as described in Section "Weighted voting", to sends back the voting result to the authorization module. If the final voting score *t* is above the threshold set by the patient beforehand, then the authorization module grants the requester with the temporary access privilege. After that, the PCHR system makes a record of this emergency access authorization.

How the ECG group members vote We now explain in the weighted voting scheme how the ECG members compute their votes in an reliable and efficient way. A valid vote is limited to a real number between 0 to 1. The voting can be done manually by the ECG members in the PCHR system. However, it may actually take a lot of time to wait for a ECG member's response.

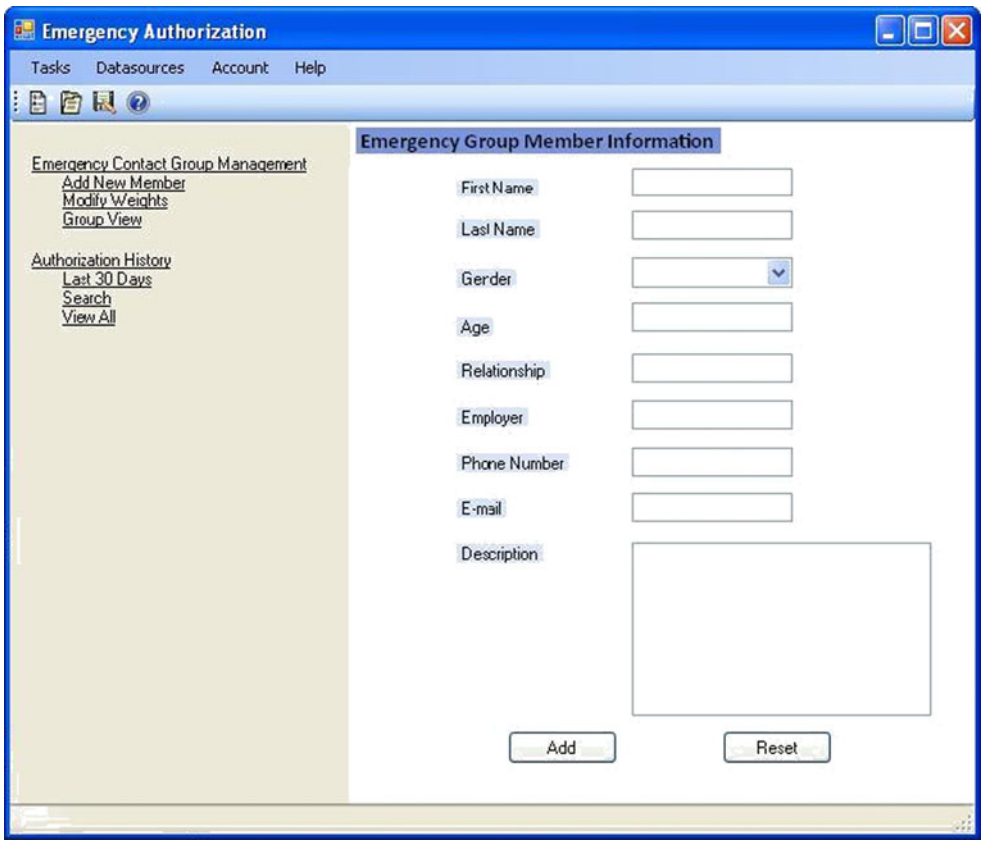

Fig. 2 Screenshot of Emergency Authorization Prototype. Patients' view. The page where the patient adds a new emergency contact group member and inputs the member information

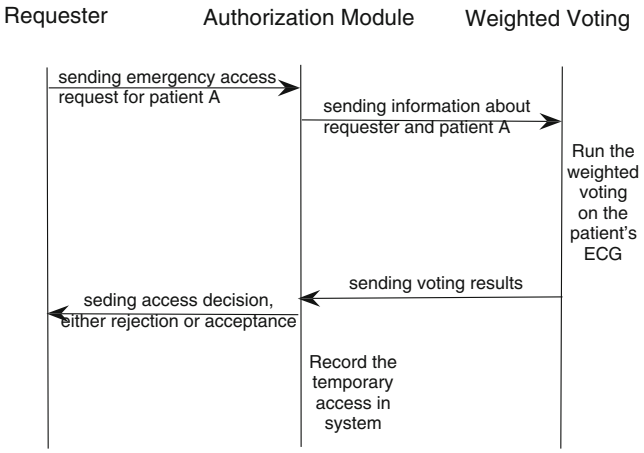

Fig. 3 Work flow of emergency access authorization for the PCHR system insiders

A simpler but more efficient back-up method is that in the PCHR system, it stores the information about the connections between the requester and the ECG members (e.g., both parties are in a partners group), and the vote can be automatically computed based on this information. In our design, every emergency access request has a valid period. When the request expires, if the manual-voting response has not been received from a certain ECG member, its vote is set to 1 by the system if the requester and the ECG member are in the same professional association or partner group. Otherwise, its vote will automatically be 0. Moreover, if the automatically set vote is used for a ECG member, its weight will be reduced to half of its original value when counting towards the final voting results. If the ECG members do not know requester, they are suggested to behave conservatively by not reacting. Each voting record of the ECG members is stored in the PCHR system, so that patients can check how their emergency contact groups voted in granting the access on behalf of them. Patients can always change or remove ECG members, if they find that some ECG members maliciously voted for false emergency requests such as those from a data mining group.

The patients can view the voting history of every ECG member,

Figure 4 is a screenshot of our emergency authorization prototype, showing the page where patient manages the emergency contact group members by assigning trust-weights and rank to each member.

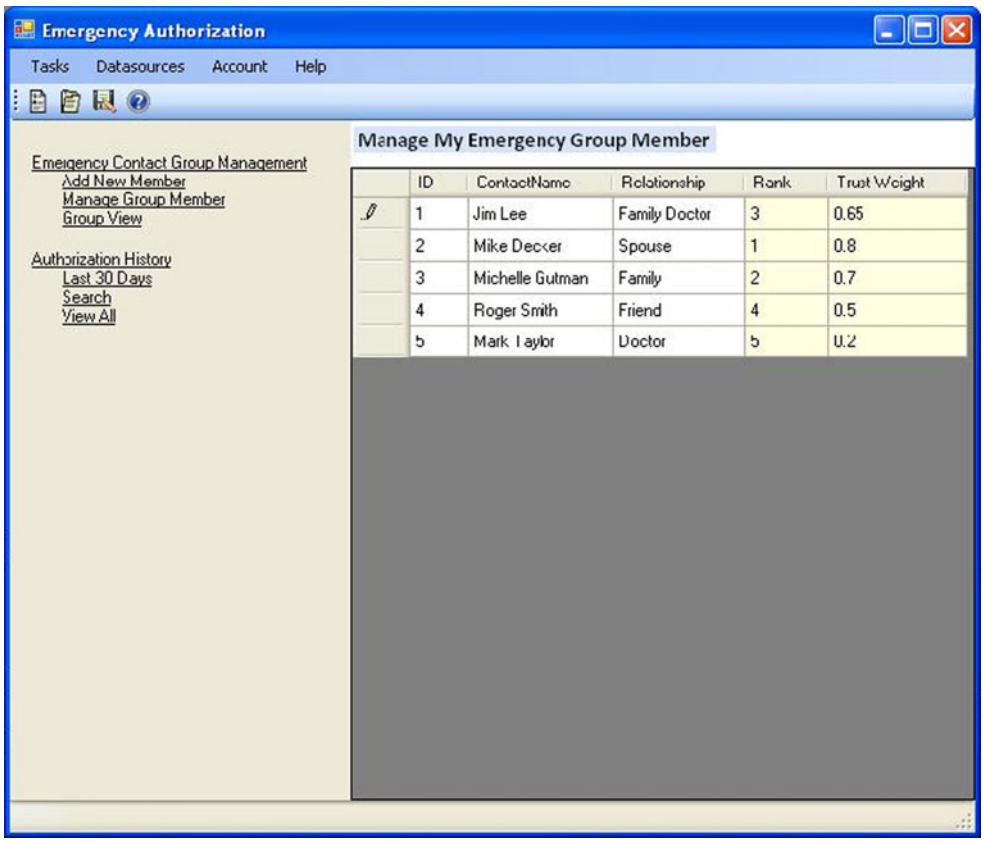

Fig. 4 Screenshot of Emergency Authorization Prototype. Patients' view. The page where patient manages the emergency contact group members by assigning trust-weights and rank to each member

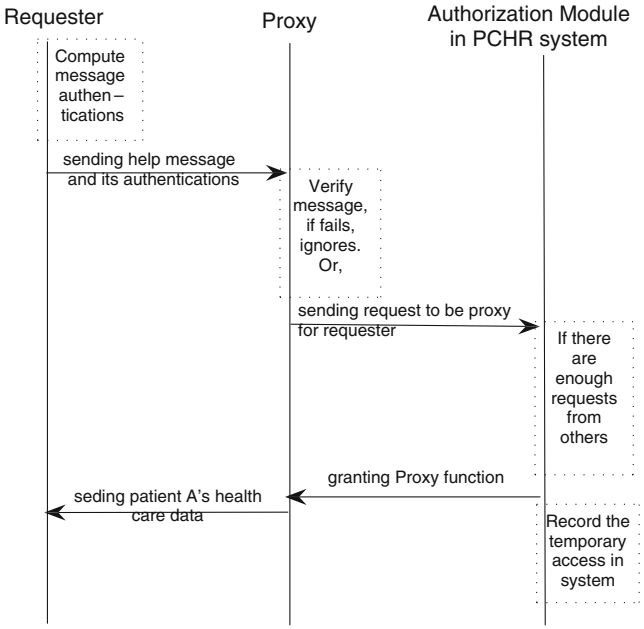

Fig. 5 Work flow of emergency access authorization for the PCHR system outsiders

Emergency access authorization for outsiders

The work flow of emergency access authorization for the PCHR system outsiders is illustrated in Fig. 5. First, using source authentication method discussed in Section "Source authentication", the requester broadcasts its help message, which contains the identity of the patient and the health record it requests, together with the authentication codes of the message to all his partner group members. When receiving the message, its partner verifies that the message is indeed sent by the requester. After looking at the content of the message, if the partner is one of ECG members of the patient, it sends a request to the PCHR system asking to be a proxy for the requester in getting access to the patient's health records. When the PCHR system receives enough such proxy requests from the ECG members of a particular patient, the system randomly picks one of them as the proxy for the requester, and authorizes such proxy function for a limited period of time. In this way, the proxy can first access the patient's health records which are requested by the requester and then transmit the data to the requester in a safe way, such as using asymmetric crypto-system.

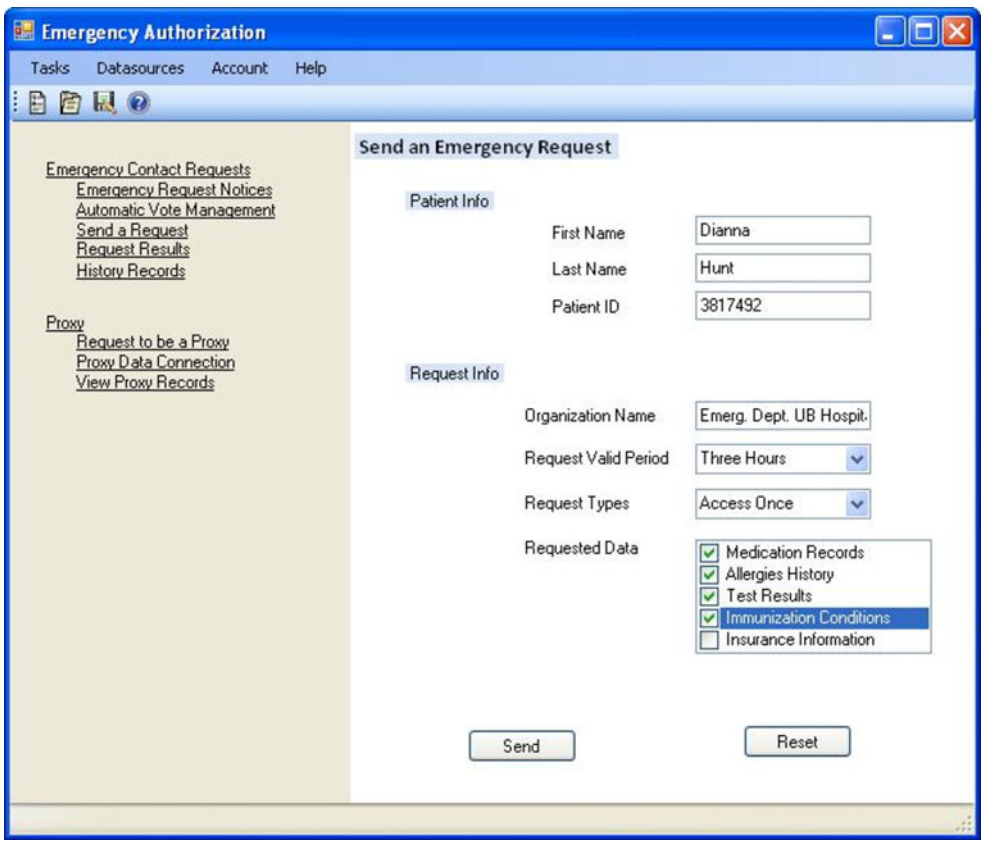

Fig. 6 Screenshot of Emergency Authorization Prototype. Requester's view. The page where the requester sends an emergency request

Figure 6 shows the screenshot of the page where the requester sends an emergency request in our emergency authorization prototype.

Security analysis

Emergency Access Authorization for Insiders: Our weighted voting scheme is mainly based on the following formula:

$$t = \sum_{i=1}^{i=N} w_i V_i. \quad (1)$$

In Eq. 1, each w_i and N are decided by the patient, so their values are always truthful. Since our solution is designed within the PCHR system, the information V_i is authenticated by the PCHR system. Here we assume that each emergency contact group member does not collude with the requester and thus their votes V_i are also truthful. Hence the voting result t is truthful.

It is very difficult to completely prevent the tacit collusion between the requester and the ECG members. It usually needs a cryptographic setup and protocols to guarantee the security under collusion attacks. We leave it for future work. As for our current solution, there are usually multiple ECG members for each patient. Unless the requester have colluded with the majority of ECG members, the final voting decisions will not be affected by the collusion.

Emergency Access Authorization for Outsiders: In our solution of emergency access authorization for outsiders, we utilized a cryptographic technology of source authentication [6] to make sure that the help message from a requester to its partners cannot be falsified. Even there is a coalition of bad members in the group, as long as the coalition is smaller than a certain parameter value, the authenticity of help message can still be maintained. Please see [6] for detailed security analysis of this source authentication method based on shared keys. The main idea is that the sender holds a set of l keys and attaches l message authentication codes (MAC) to each packet, (each MAC is computed with a different key). Each group member holds a subset of the l keys and verifies the MAC according to the keys it holds. Appropriate choice of subsets can ensure that with high probability no coalition smaller than w group members (where w is a parameter) can know all the keys held by a good member. In this way, the authenticity of the help message is achieved.

Discussion

Security and privacy issues have become the major concerns of applying personally controlled online health care data in the existing medical systems. When designing our emergency access authorization methods for such systems, we have carefully considered these issues and hence our methods can achieve the following desirable properties.

- The emergency access authorization process is confidential. No one else other than parties trusted by the patient will know who sent an emergency access authorization request for the patient.
- The authorization communication is secure. We leverage the advanced cryptographic techniques to guarantee that no one can send a fake authorization request using a fake entity, and furthermore, the request content cannot be maliciously modified by others.
- The emergency access authorization process is effective. In our method, the emergency access authorization is done with the help of the parties who are trustworthy to the patient and the patient can review the emergency request and authorization history. Therefore, we provide effective emergency access authorization methods to the PCHR information, and meanwhile, the authorization is still under the control of the patient.

Conclusion

PCHR systems have emerged to allow patients to control their own medical data. The data access privilege is given by the patient. However, in many emergency circumstances, medical treatments are immediately required when the patient may have lost the ability to give the access privilege to the clinics or the corresponding medical treatment providers. We consider two cases to solve the emergency access authorization problem in the absence of patients, i.e., a) the access requester is inside the PCHR system but does not have the access privilege of the patient's health records, and b) the requester does not even have an account in the PCHR system to submit its request.

To address the emergency access authorization problem for the two cases, we have respectively utilized advanced weighted voting and source authentication techniques, to guarantee that our emergency access authorization method is secure and effective. We have implemented our methods in a prototype system.

References

1. The American Recovery and Reinvestment Act of 2009 (ARRA), P.L. 111C5, 6. 123 Stat 115, 17 February 2009.
2. Agrawal, D., and Srikant, R., Privacy-preserving data mining. In: *Proc. ACM SIGMOD*. pp. 439–450, 2000.
3. Grimson, W., Jung, B., van Mulligen, E. M., van Ginneken, A. M., Pardon, S., and Sottile, P. A., Extensions to the HISA standard—The SynEx computing environment. *Methods Inf. Med.* 41:401–10, 2002.
4. Blobel, B., Authorization and access control for electronic health record systems. *Int. J. Med. Inform.* 73(3):251–257, 2004.
5. Brickell, J., and Shmatikov, V., Efficient anonymity-preserving data collection. In: *Proc. of ACM KDD*, 2006.
6. Canetti, R., Garay, J., Itkis, G., Micciancio, D., Naor, M., and Pinkas, B., Multicast security: A taxonomy and some efficient constructions. In: *Proceedings of IEEE INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. Vol. 2, pp. 708–716, 1999.
7. Chen, K., and Liu, L., Privacy preserving data classification with rotation perturbation. In: *Proceeding of ICDM'05*. pp. 589–592. Washington: IEEE Computer Society, 2005.
8. Du, W., and Zhan, Z., Using randomized response techniques for privacy preserving data mining. In: *Proceeding of SIGKDD'03*. pp. 505–510, 2003.
9. France, R., Security of health care records in Belgium application in a university hospital. *Int. J. Med. Inform.* 73(3):235–8, 2004.
10. Grimson, W., Berry, D., Grimson, J., Stephens, G., Felton, E., Given, P., and O'Moore, R., Federated healthcare record server—The synapses paradigm. *Int. J. Med. Inform.* 52:3–27, 1998.
11. Grimson, J., Grimson, W., Berry, D., Stephens, G., Felton, E., Kalra, D., Toussaint, P., and Weier, O. W., A CORBA-based integration of distributed electronic healthcare records using the synapses approach. *IEEE Trans. Inf. Technol. Biomed.* 2:124–138, 1998.
12. HIPPA, National Standards to Protect the Privacy of Personal Health Information, [Online]. Available at: http://www.hhs.gov/ocr/hipaa/finalreg.html, 2006.
13. Haaka, Mvd, Wolffa, A. C., Brandnera R, Dringsb P, Wannenmacherc M, and Wetter T., Data security and protection in cross-institutional electronic patient records. *Int. J. Med. Inform.* 70(2–3):117–130, 2003.
14. Lindell, Y., and Pinkas, B., Privacy preserving data mining. *J. Cryptol.* 15(3):177–206, 2002.
15. LeFevre, K., Dewitt, D. J., and Ramakrishnan, R., Incognito: Efficient full-domain k-anonymity. In: *Proceedings of the 2005 ACM SIGMOD*, 12–16 June 2005.
16. Motta, G., and Furuie S., A contextual role-based access control authorization model for electronic patient record. *IEEE Trans. Inf. Technol. Biomed.* 7(3):202–7, 2003.
17. Narayanan, A., and Shmatikov, V., Obfuscated databases and group privacy. In: *Proc. of ACM CCS*, 2005.
18. The Personal Health Working Group, *The personal health working group final report*. Washington, DC: Connecting for Health: A Public–Private Collaborative, 2003.
19. Committee on Data Standards for Patient Safety, Board on Health Care Services, *Key capabilities of an electronic health record system*. Washington, DC: Institute of Medicine of the National Academies, 2003.
20. Sandhu, R. S., Coyne, E. J., and Youman, C. E., Role-based access control models. *IEEE Comput.* 29(2):38–47, 1996.
21. Simons, W. W., Mandl, K. D., and Kohane, I. S., The PING personally controlled electronic medical record system: Technical architecture. *J. Am. Med. Inform. Assoc.* 12(1):47–54, 2005.
22. Teng, Z., and Du, W., Comparisons of K-anonymization and randomization schemes under linking attacks. In: *Proceedings of the 2006 ICDM*. pp. 1091–1096, 2006.
23. Tannenbaum, T., *Excursions in modern mathematics*, 6th Ed. Upper Saddle River: Prentice Hall, 48C83, 2006.
24. Thompson, T. G., and Brailer, D. J., The decade of health information technology: Delivering consumer-centric and information-rich health care. Available at: http://www.hsrnet.net/nhii/materials/strategic_framework.pdf, Accessed 24 August 2004.