J Med Syst (2010) 34:975–983
DOI 10.1007/s10916-009-9313-6

ORIGINAL PAPER

Biometrics for Electronic Health Records

Alejandro Enrique Flores Zuniga · Khin Than Win · Willy Susilo

Received: 10 February 2009 / Accepted: 4 May 2009 / Published online: 2 June 2009

Abstract Securing electronic health records, in scenarios in which the provision of care services is share among multiple actors, could become a complex and costly activity. Correct identification of patients and physician, protection of privacy and confidentiality, assignment of access permissions for healthcare providers and resolutions of conflicts rise as main points of concern in the development of interconnected health information networks. Biometric technologies have been proposed as a possible technological solution for these issues due to its ability to provide a mechanism for unique verification of an individual identity. This paper presents an analysis of the benefit as well as disadvantages offered by biometric technology. A comparison between this technology and more traditional identification methods is used to determine the key benefits and flaws of the use biometric in health information systems. The comparison as been made considering the viability of the technologies for medical environments, global security needs, the contemplation of a share care environment and the costs involved in the implementation and maintenance of such technologies. This paper also discusses alternative uses for biometrics technologies in health care environments. The outcome of this analysis lays in the fact that even when biometric technologies offer several advantages over traditional method of identification, they are still in the early stages of providing a suitable solution for a health care environment.

Keywords Electronic health record system · Biometrics security · Share care paradigm

A. E. Flores Zuniga (✉) · K. T. Win · W. Susilo
Faculty of Informatics, University of Wollongong,
Wollongong, NSW, Australia
e-mail: aefz871@uow.edu.au

Introduction

Biometric recognition refers to the recognition of individuals based on their anatomical, physiological and/or behavioral characteristics [18, 36]. Unlike the usual identification methods centered on what the person has (card, token, key) or what the person knows (password, PIN), biometrics allows the identification of an individual based on who the person is [18, 39]. Biometric recognition is based on pattern-recognition technique that distinguishes a person based on a feature vector which is derived from physiologic or behavioral characteristics such as fingerprint, face, retina, gait, odor, hand geometry, iris, palm print, or voice [18, 36]. Nowadays, biometric is used as a method for identification or confirmation of a person's identity. Identification methods are used to determine a subject identity based on the comparison of a biometric sample obtained from the subject with a set of records stored in a database. Authentication methods are used to confirm the identity claimed by an individual, in this case the comparison is only with the stored biometric feature that corresponds to the claimed identity [39]. Authentication technology based on biometric is used to restrict access to sensitive information, installations and restricted areas [36]. Through its practical application, the use of biometric authentication technologies is relatively minimal in comparison to other technologies used to confirm the identity of individuals such as passwords, PIN or smart cards [39].

In healthcare biometric technology has been gradually introduced as a method to secure and restrict access to medical facilities, protect and manage confidential information, identify patients and reduce fraud in healthcare programs [28]. In this context, biometric technology provides a mechanism for identification or identity verification depending on what organizations need in order to

protect their resources and information. Using biometric to provide security services can be a noteworthy alternative considering the flow of sensitive information present in large software applications and the resources required to manage complex information systems that can be accessed by hundreds or thousands of local as well as remote users.

Even though biometric technologies offer a more compiling and secure method for restricting the access to health facilities and health information than traditional technologies (Table 1), it has not been addressed as a suitable alternative for protecting patient's privacy and confidentiality [38]. Biometric technology offer several security features such as fast and user-friendly authentication and access control as well as the ability of encrypting sensitive information not only for local applications but also in a shared care environment [20, 38]. In this paper the authors explore the uses of biometric technology and its application on security in healthcare. The focus will be placed on secure architecture based on biometric technology for controlling the access and protecting sensitive information contained in electronic health records in a share care environment.

Concern for patient's privacy and confidentiality

Protecting the privacy and confidentiality of electronic health records is a challenge faced by modern health information systems. International regulations such as the imposed by HIPAA (Health Insurance Portability and Accountability Act), the European Data Protection Directive [1, 27] and Australian Privacy Principles Act [17] demand the highest level of security and protection for access, administration and exchange of individuals' sensitive data.

Patients understand the importance of retaining electronic information to support and improve the delivery of health care, even when they recognize the high sensitive nature of the collected data [21]. Moreover, in a shared care paradigm the number of specialist that can have access to EHRs increases and the information can be broken down among different health information systems within the organization or among different healthcare providers. The availability of access for professional and third parties also increases the risk of security breaches [17]. Therefore, the protection of the patient's privacy and the safe disclosure of health information become main concerns during the development of secure health information systems [7, 9, 14].

The concern over patients' privacy and confidentiality also has become a barrier for the adoption of electronic health record systems. Many health professionals and patients fear that electronic health records could be affected by security breaches and that stored data, especially those data collected by web-based EHR systems, could be easily accessible by unauthorized users [2, 32]. Patients expect secured health information systems in which personal data is protected and any disclosed information would be done only for health care purposes [21]. Nevertheless, the disclosure and reuse of data for purposes other than the delivery of health care is also an expanding practice that concerns the interest of patients. The information provided by historical records is a potential source for research and knowledge generation that can be used to improve the delivery of health care [5, 27]. However, the unauthorized release of information could also lead to issues of public concern [16, 29].. Therefore, it is essential for modern

Table 1 Comparative analysis of authentication methods

	Existing models	Biometric technology
User friendly and medical environment	It requires memorization of PIN or passwords. Inappropriate for a high demanding medical environment	Authentication is fastest and easier. Appropriated for most medical environment settings. Some biometric technologies are inappropriate for specific health care settings. Accuracy can be affected by the inability in obtaining a good biometric template, placement of biometric future, temperature, humidity and degradation of the biometric feature. Enrolment can be affected by age, skin color, damage or inexistence of the biometric feature
Global security needs	Inherent security issues related to the use of PIN, passwords or Smartcards such as allow unauthorized share and delegation of access rights. Accidental lost of access credential. Possibility of impersonation It is more likely that users would be able of refuting electronic transactions	Increases security, discourages and detects fraudulent account access, and prevents impersonation. It also reduces the risk of unauthorized access to sensitive information. Biometric futures cannot be shared or delegated. Biometrically transactions are difficult to refute
Share care environment	Current research and implementation are exploring share care environment scenarios	Current research and implementation centered on local networks
Costs	High maintenance costs	Reduces maintenance cost. High level of initial investment

health information systems to consider the right balance between safeguards for protecting the privacy of patient's data and safe access and retrieval of information for primary and secondary uses [34]

Challenges of securing electronic health records

Securing electronic health records could become a complex and costly activity, especially in a scenario where information is potentially maintained by multiple actors. The European Committee for Standardization has released a set of information security standards to provide a framework for secure storage and release of health data [11–13]. The European standards recognize four global security needs that any health information system should accomplish which are availability, confidentiality, integrity and accountability [11].

Availability of the information is a key factor for functional electronic health record systems, user with the rights to access information should be allowed to do so in order to perform their duties. In this case, the principle of need-to-know is the key concept to be applied [7, 19]. Under this premise users should be allowed to access a patient's EHR in order to obtain the relevant information to carry out a task in concordance with the access and security policies of the organization [7, 19]. The principle of need-to-know is driven by the relevance of the information that is acceded. However, relevancy is an ambiguous concept that depends on the context in which the information is generated and the purposes for which the data is released. In any case, the information accessed should be relevant but also sufficient to provide health care services [40]. Consequently, correct authentication of users becomes crucial in order to guarantee that information is accessed, added and modified only by individuals with the privileges to perform such activities [7]. Defining the correct balance between security requirement and availability of information is a critical goal in a complex environment such as health care [6, 9, 10]. Even though, adding excessive security mechanisms could lead a less efficient, more time demanding and less user friendly user authentication methods, which is also a factor needed to be considered.

Confidentiality is an important factor that not only drives the relationship of patient and doctor but also the concerns for protection of patient privacy [2]. The protection of patient privacy is a concept historically embedded in the relation between patient and physician. However, the traditional concept of confidentiality patient–physician becomes less clear in a shared care environment. Nowadays, providing healthcare has turned into a multitask activity in which the intervention of multiple actors is required not only for the treatment of diseases but also in maintaining the confidentiality of increasingly distributed electronic health records [9]. Under these circumstances, managing security services that ensure confidentiality during access to sensitive information become a crucial task for securing EHRs [7].

Security breaches are threats to the integrity of electronic health records and its ability to provide reliable information for accountability purposes. Integrity of the information is not only guaranteed by incorporating additional security mechanisms within the system or for securing a communication channel but also by ensuring that only authorized user can have access, add or alter stored information [9, 10]. In shared care scenarios controlling who is accessing the information turns into complex and time demanding task. Indeed, the solo fact that existing authentication methods, such as PIN or passwords, allows unauthorized delegation of access permissions threaten the integrity and validity of the information [23, 38]. Accountability of information also becomes less accurate when non-authorized users are able to access and manipulate data regardless of the fact that they do not have the privileges to execute such activities. Under this situation, the possibility that a user could refute electronic transaction becomes more likely [38].

The level of investment and cost associated to the use of security mechanisms is also a crucial determinant in any decision regarding the implementation of security technologies [3, 20]. In fact, the level of investment and cost required to implement and maintain security mechanisms becomes a barrier in the adoption of electronic health records systems [2, 20]. Therefore, organizations require to achieve the correct balance between costs and the security solutions selected to board the requirements that surface from the protection of patients' privacy.

In summary, the key elements for determining what security technology suits better the requirements of a shared care environment are the ability to perform in a user friendly fashion, the consideration of the global security needs (availability, confidentiality, integrity and accountability), the ability to operate locally as well as in shared environments and the efficacy between cost and accomplishment of the security requirements.

A comparative analysis of existing models

Traditional authentication models

Existing authentication and access control technologies require the secure maintenance of PIN, passwords or smartcards in order to provide access to restricted facilities and information. However, the nature of the activities performed by physicians and medical staff requires mobility and multiple accesses to different terminal within the organization or even remotely in the case of web base

health information systems or multi-domain integrated systems [19, 38]. Considering that access to different systems may require multiple authentication methods, it is usual to find that PINs and passwords are maintained stored in the computer terminals used by physicians, stick papers in the office, laboratories, medical consult or at home, or become a simple combination of well known numbers or digits such as phone extension, date of birth or pseudonyms which are easy to remember but also relatively less efficient in avoiding security breaches [19, 38]. The use of smartcards also may present certain disadvantages such as deterioration and accidental lost. Additionally, if physicians forget their PIN/passwords or misplace their smartcards a reinstating process must take place [38]. Considering these facts, it is correct to assume that existing technologies turn out to be unsuitable and less reliable for a medical environment.

In comparison, biometric technology offers a faster, easier and more secure method for authentication as well as for securing sensitive data, which also increase the reliability of the security mechanisms. The fact that biometric features cannot be lost or stolen, and to mimic them is highly unlikely, makes them a more secure method than traditional ones [25, 38]. Biometric technology also facilities the detection of fraudulent account access and discourages the impersonation individuals [25]. Biometric technology also provides a quick authentication method for a physician and nurses by using a simple and transparent method for accessing electronic information through distributed terminals [33].

Delegation of authentication codes is an issue normally associated to the use of traditional authentication model which can lead to medical or legal disputes [14, 23]. Delegation of private authentication codes correspond to the non authorize delegation of personal credentials such as PIN/password or other authentication feature to other physician or nurse to access, modify or include information on behalf of the owner of the private authentication codes [23, 38]. The delegation of access rights grant access to sensitive information to non-authorized user by breaking established policies regarding information privacy and confidentiality [23, 38]. This also could have legal repercussions when restricted information is leaked to third parties without the proper authorization or when the addition of erroneous information compromises the safety of patients [2, 17, 34]. On the contrary, biometric features cannot be shared, delegated, stolen or copied, making delegation of access rights highly improbable. The unlikely possibility of impersonation or delegation of access rights dramatically reduces any attempt to refute an electronic transaction [25, 38].

The use of biometric technology also has demonstrated to be efficient in reducing the costs of systems maintenance [3]. In fact, the administration of security systems based traditional access control technology can have a significant impact on the organization's budgets. The Gartner group estimated that password maintenance alone costs US$150–US$200 per user per year [20]. The password maintenance cost can be reduced significantly by using biometrics authentication technology, especially cost related to the reposition of defective, lost or stolen cards, and the reissuing of forgotten access credentials such as PIN and passwords [20]. On the other hand, the high level of initial investment required in the implementation of biometric is a downsized in the implementation of this technology [33]. For example, the cost of fingerprint scanners varies between US$200 and US$1,500 per identification node. Integration and maintenance of biometric technology could also become an important component of the budget of a health care organization. A balance between cost and efficiency of the selected biometric technology should consider facility of integration to existing application, durability of the scanner devices and minimal maintenance requirements [30].

Biometric technology

As it was discussed before, approaches based on biometric technology have demonstrated to be reliable user authentication mechanisms by restricting the delegation of access rights as well discouraging fraudulent access or impersonation of users [38]. Moreover, implementation of biometric authentication technology also facilitates the remote access to electronic health records by using a biometric feature as a method of authentication. This has demonstrated to be beneficial in the management of treatment for aged patient in remote areas, as well as allowing patients to update their online personal health records [28]. It also has been used to reduce fraud in health insurance, protect facilities, reduce costs of maintenance, promote and protect patient privacy, help in the management of confidential data and identify patients [28]. However, there are technical and usability issues to be considered when selecting and using biometric technology such as accuracy of the biometric lecture, technological obsolescence of the scanners, existence of the biometric feature, enrollability and suitability for the medical environment.

The accuracy of the biometric technology depends on the ability of the system in obtaining a good initial image of the biometric feature as well as the ability of matching individual with their original templates. The false acceptance rate (FAR) and false rejection rate (FRR) can be affected by factors such as incorrect placement of the biometric feature, dirt, humidity and changes in the biometric feature [19, 30]. Degradation of the biometric feature also affects the accuracy of the matching system [31] and rises the necessity of maintenance and re-enrollment of existing users. Enrollability of user is also the other issue that can affect the accuracy of the matching

system. For example, optical fingerprint scanners fail to read significant portion of the population such as older people with dry skin and children [31]. It is also the possibility of damage or inexistence of the biometric feature generated by injuries or mutilation [19].

The different activities hold in a health environment demands an easy to use and friendly technology for secure access to electronic health records [19]. Even though, biometric technology offers several advantages in comparison to traditional authentication methods, it also has usability setbacks. Users require placing their biometric feature in a specific position, heat, cold and perspiration can affect the accuracy of the lecture and the technology is not suitable for certain cases. For example, fingerprint technology can be easily implemented for accessing electronic health records in several health care settings, however the fact that many health care staff would be usually wearing hygienic gloves becomes a usability problem [19]. Iris recognition is more accurate technology and also provides a solution to several usability issues, however, the high cost, reticence of users and the fact that this technology has not been tested for large implementation makes it less suitable for several health care settings [33].

Additionally, biometric implementations assume that electronic health records are applications based on private, and most of the time, local networks that do not need external communication [38]. This assumption is not entirely accurate for a shared care paradigm [7–9]. Nowadays, it is common to observe that patient's medical information is shared among different health providers or used not only for primary purposes but also for secondary reasons such as research, education, treatment, elaboration of public health policies, etc. [34]. However, sharing sensitive information brings the concern that the overall security will be as strong as the weakest system within the network. Therefore, to become a valid alternative, biometric technology requires considering multi-domain scenarios, where information is transferred among different domains within the organization or among health care providers.

In general, biometric technology does offer several advantages over traditional method especially in matters related to security and authentication. However, several issues rise from the usability perspective that could affect the accuracy of the technology and that needs to be considered to reduce the rates for false acceptance and false rejection.

Uses of biometric in healthcare

Authentication and access control

Technology based on biometric provides a better and more secure method to identification and access control than traditional technologies. Biometrics features are almost impossible to reproduce and user can be easily identified based on their physical or behavioral characteristics [18]. As we discussed before, biometric technology presents several advantages in comparison to traditional methods such as providing a friendly and easy to use access control method, the restrictions in the delegation of access rights, increase of security and discourage of fraudulent access to restricted information. Additionally, international regulations and legislations that promote protection of patient confidentiality have pushed forward the concern regarding unauthorized access and release of information [1, 17, 27]. In this scenario, biometric technology provides a reliable solution for ensuring that only authorized personnel have access to patient's information. Biometric technology also could be used to protect patient's privacy in share care scenarios by making information network systems more secure [3, 28].

Biometric technology dramatically reduces the chances of unauthorized delegation of access right as well as facilitates the maintenance of appropriate access privileges, positioning this technology as a suitable solution for guaranteeing security and accessibility to electronic health records [20, 38]. As biometric technology uses unique physical features of a person, the level of security is increased by preventing the fraudulent access to restrict information. Moreover, biometric allows the elimination of end-user generation of passwords as primary source of information for system security, which has become a main security issue for current information systems [20, 38].

In general, using biometric technology as an authentication and access control method enhances the protection of patient privacy by adding an accurate authentication technology, eliminates cost associated to password maintenance, reduces unauthorized access to sensitive information by restricting delegation of access right and impersonation of individuals, reduce fraud associated to insurance claims and become a long term solution for access system management [20].

Biometric encryption of medical data

Biometric encryption is a technological solution that increases security over the encrypted data. In this case, the sensitive information is encrypted base on a biometric feature making the information available only to the person that possesses the biometric characteristic. Since biometric encryption can be considered a more effective approach for protecting and restricting access to sensitive information, a step forward would be to use of this technology to protect medical data. For instance, biometric can be used to generate a secure crypto key to encrypt sensitive information or use a biometric profile as an attribute for accessing encrypted information in schemes such as fuzzy Identity-based Encryption [24].

The use of biometric encryption provides a secure mechanism for protecting medical information such as electronic health records and offers an effective method to grant access to physicians and medical staff. However, using biometric to encrypt medical data also poses the challenge of maintain the correct level of accessibility to medical records. The main difficulty of using biometrics for encryption of electronic health records is that the principle of need-to-know becomes less clear and difficult to manage. Availability of the information, which is a key factor for functional electronic health records, could become compromised with the use of biometric encryption [7, 19]. In this case, the principle of need-to-know is applied [7, 9], however using biometric encryption increases the difficulty of accessing the secured data, especially in cases in which the information is used for secondary purposes. Additionally, producing the same feature vector for a single feature characteristic in different exposures to a biometrical sensor is limitation of biometric technology. Therefore, direct encryption of medical data by using a biometric feature is rather difficult [18, 24]. An approach generally used to overcome this issue is to hide the crypto key within the biometric profile. A biometric matching system is used to verify the identity of the user and release the encrypted information by matching scores over the biometric profile [24]. The crypto key contained within the biometric profile can be stored in a secure database where it can be accessed in order to encrypt or decrypt the information by either patient or authorized staff.

Following this concept, biometric technology could be used not only as an approach for verify the identity of an individual or for providing access authorization to stored data but also as a method to encrypt sensitive information maintained in the database or to encrypt data during the exchange of messages. Encryption based on the biometric schemes can be used to increase security during the release of information, for instance, by encrypting the data before the exchange of medical information or by encrypting personal health records and then releasing the information only to who have the biometric feature that identifies the intended receptor of the data. Fuzzy Identity-Based Encryption can be used to encrypt and then decrypt sensitive medical data on these cases. The Fuzzy Identity-Based Encryption (IBE) scheme is based on the Identity-Based Encryption first proposed in [37]. The IBE scheme allows a sender to encrypt a message by using an identity without accessing a public key certificate [35, 37]. In this case, the identity is viewed as a string of characters (e.g. user's name, a email address, or telephone number) which serve as a user's public key [26]. In this scheme neither the user's public key authentication nor the recipient been online at the time of creation are necessary in order to create an encrypted message [26, 35].

The Fuzzy Identity-Based Encryption scheme is an application of Identity-based Encryption (IBE) which enables the encryption of a message by using fuzzy inputs, such as biometric inputs as identities. In the Fuzzy IBE scheme, the identity corresponds to a set of descriptive attributes that will be used to encrypt and decrypt the message [35]. Fuzzy IBE scheme describes an error tolerance which allows the use of biometric as an identity attribute (i.e., the fuzziness of the scheme, which refers to the tolerance that the scheme can provide). In this case, a secret key, SK, is use to decrypt a ciphertext encrypted with an identity attribute, Id, if and only if the identity attributes are "close" to each other as measured by the "set overlap" distance metric [35]. In other words, the noise of a sampled biometric identity is considered within the scheme, and the error-tolerance will allow the decryption of a message if the discrepancy measured by the distance between the identity attributes is within the tolerated boundaries. To decrypt the message, a private key is required. The scheme requires of a trusted authority, known as the Private Key Generator (PKG), with the task of generating the private key (SK). The PKG will provide such a private key only after the user has been successfully identified [4]. The generated key can then be used to decrypt the ciphertext originally receive from the sender (see Fig. 1). In the following, d denotes the "tolerance" provided by the scheme, which refers to the maximum difference between the biometrics provided during the key extraction with the PKG and the biometrics presented during the decryption process.

Fuzzy Identity-based Scheme can be "turned" into a fuzzy authentication scheme. In this case, the owner of the biometric can "authenticate" some information and this information will be verifiable using the biometric owned by the "signer". The technique to convert from a fuzzy identity-based scheme to a fuzzy authentication scheme is straightforward, as mentioned in [35].

Data encryption during the exchange of medical information

An important functionality provided by EHR systems is the feasibility of remote access to relevant health information at any time and location. However, functional and reliable interconnected EHRs require a special consideration over the protection of patient's privacy and confidentiality when information is remotely accessed for primary and secondary purposes [2, 17]. In a shared care environment, medical records are expected to be maintained by different health care units that are involved in the care process. Actually, in modern healthcare environment different care services are offered by different health care units within the organization or in a healthcare network that involves multiple actors, and therefore, medical information is generated and

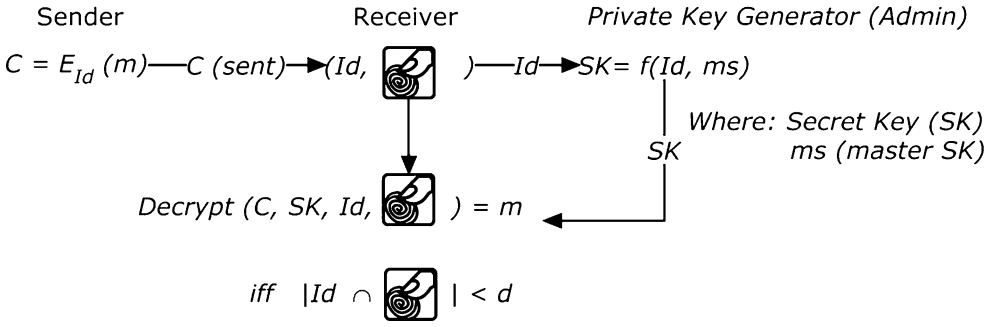

Fig. 1 Fuzzy Identity-Based Encryption

stored by several organizations [22]. For that reason, the implementation of a share care paradigm not only requires the support of standardized Information systems architectures but also considering secure mechanisms for protection of patient's sensitive information specially when information is expected to be shared among different healthcare provides [9, 10].

Secure disclosure and exchange of electronic health records over insecure channels, such as Internet, requires the implementation of comprehensive security technologies that allow the exchange of data, but at the same time guarantees protection of patient's privacy [9, 15, 29]. Biometric technology provides both a method for authentication of users and encryption of data. In a share care scenario user can remotely access and retrieve information by using their biometric profiles. During the exchange of the information, the extracted data can be encrypted by using a public key identifier and then decrypted with the biometric profile of the user. In this way, the only one that can retrieve the information would be the owner of the biometric profile.

Remote access for patients

A specific application of biometric technology is identification of patient for remote access to personal medical information. In this case, patients can have access to their personal information by using a biometric feature such as fingerprint. In this scenario, a biometric scanner will be able to capture an image of the biometric feature and send it to a centralized system for verification purposes. The image is matched with the stored biometric profile of the patient. When the identity of the patient is verified the system sends back the information originally requested by the patient.

Authentication technology other than biometric does not guarantee that the person who is remotely accessing personal records is who claims to be. In previous sections, we discussed several security issues regarding the use of personal key (passwords and PIN) normally generated by the end-user [20, 38]. Although, patients, who are accessing medical records, are not allowed to modify medical information, the unauthorized access to the remote repository could have personal, legal or social repercussions. Biometric technology helps preventing unauthorized access to remote repositories by avoiding impersonation of individuals [25, 38]. Also, as it was discussed in Section "Data encryption during the exchange of medical information", biometric technology could be used to encrypt the medical data. In this scenario patient would be able to access personal data remotely, the system would be able to encrypt the information using the biometric profile of the patient and then transmit the encrypted data to the patient's computer.

Experiences using this model have been implemented in United Kingdom and South Africa. In United Kingdom a web based application with fingerprint technology has been developed to allow the remote identification and access to aged patients' electronic health records. Patient in this program are able to access their medical records, prescription and medical procedures as well as indications made by physicians. A similar system has been implemented and used in South Africa to facilitate the patient identification and provides access to historical electronic health records.

Verifying patient identity

Biometric identification and verification of patient's identity had been used mainly to prevent fraud in insurance claims and for healthcare programs. Several experiences have reported successful results in countries such as USA, Australia, United Kingdom and South Africa. Identification of both healthcare provider and patients has been the primary purpose of the use of such technologies. For example, in Texas (USA) a biometrics-smartcard program has been implemented for recipient authentication at the attention point to reduce fraud associated to the provision of healthcare services, in Australia a retina verification system has been employed to support the treatment of patients addicted to heroin [28].

Fingerprint biometrics also can be used for purposes of patient registration and identification. Under a biometric identification system, a non-registered patient entering healthcare service may place a biometric feature (iris, fingerprint, etc.) on a biometric scanner to generate a

biometric profile. The biometric profile is then used for identity verification purposes during patient's further visits. The technology could also restrict the access to electronic health records unless the identity of the patient has been verified. A system with these characteristics has been implemented and used at Lourdes Hospital in Kentucky, USA.

Biometric profiles also have been used to identify patients in emergence situations. When biometric profiles are linked to the electronic health records the information can be accessed even when no information or identification of the patient can be provided. For example, if unconscious patients are derived to a health service they could be identified based on their biometric profiles and then linked to their personal records. The data would be released providing to the medical staff with the information required to offer an efficient medical care service. Furthermore, the released information may prove to be beneficial for other purposes such as contact the family of the patient. The Ballard Hospital, Washington, has used this method to identify unconscious assault victims that are received in the emergency services. Also, after the devastating effects of the hurricane Katrina, emergency services used biometrics profiles to identify unconscious patients and victims [28].

The attention at the point of care also may be benefited using biometric identification methods. The remote access to electronics health records by PDA, smart phones or laptop computers also is possible by using biometric for security purposes. A biometrical sensor, which is used to capture a biometrical sample of the patient, can be added to a portable devise. The image captured by the sensor is sent to a centralized system that matches the image with the stored biometric profile. When the identity is verified the patient information is released and sent to the portable device. The portable device displays the information that is used to provide a better health service. This technology has been used in USA to provide better medical care to patients and victims during emergency situations such as car accidents, fire incidents, and natural disasters.

Conclusions

We presented a comparative analysis based on a literature review of secure technologies used to protect health information. The motivation of this analysis was to explore the suitability of biometric technology to protect the privacy and confidentiality of electronic health records in a shared care environment. Our findings propose that biometric technology offer several security advantages over traditional methods. Such advantages are reliability of user authentication mechanisms, restriction in delegation of access rights as well as discouraging fraudulent access or impersonation of users. In addition, biometric authentication technology also facilitates the remote access to electronic health records for both patients and physicians, reduces maintenance cost and provides a secure method for encryption of personal data. We also described and discussed several uses for biometric technology in the health care sector. The focus was placed in biometric authentication, biometric encryption of electronic health records and identification of patients and how biometric technology can be used to improve security and provide better healthcare services.

In addition, we discussed several technical and usability issues regarding the use of biometric technologies in health care environments. Accuracy is a keystone of biometric technology. However, it can be affected by the inability in obtaining a good initial biometric template as well as incorrect placement of biometric future in the scanner, temperature, humidity and degradation of the biometric feature. Moreover, the ability of enrolled user can be affected by age, skin color, damage or inexistence of the biometric feature. In addition, biometric technology could not be suitable for certain health settings. For example, fingerprint technology for laboratories and hygienic areas where user would be required to wear hygienic gloves.

In conclusion, biometric authentication technology offers several security advantages over traditional methods and also can be used for different purposes. However, several technical and usability issues have to be considered to select a suitable solution for a health care environment. Future work in this area is to explore and provide solutions to reduce the impact of the technical and usability issues associated to the use of biometric technology in healthcare environments.

Acknowledgements The authors acknowledge the Government of Chile and University of Talca (Chile) for the support of this research.

References

1. Agrawala, R., and Johnson, C., Securing electronic health records without impeding the flow of information. *Int. J. Med. Inform.* 76:471–479, 2007. doi:10.1016/j.ijmedinf.2006.09.015.
2. Anderson, J. G., Social, ethical and legal barriers to E-health. *Int. J. Med. Inform.* 76:480–483, 2007. doi:10.1016/j.ijmedinf.2006.09.016.
3. Atkins, W., A bill of health for biometrics. *Biometric Technol. Today.* 8 (9)8–11, 2000. doi:10.1016/S0969-4765(00)09010-X.
4. Au, M., Huang, Q., Liu, J., Susilo, W., Wong, D., and Yang, G., Traceable and retrievable identity-based encryption. Applied Cryptography and Network Security, 2008, pp. 94–110.

5. Bakker, A., Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. *Int. J. Med. Inform.* 73:267–270, 2004. doi:10.1016/j.ijmedinf.2003.11.008.
6. Blobel, B., Application of the component paradigm for analysis and design of advanced health system architectures. *Int. J. Med. Inform.* 60 (3)281–301, 2000. doi:10.1016/S1386-5056(00)00104-0.
7. Blobel, B., Authorisation and access control for electronic health record systems. *Int. J. Med. Inform.* 73 (3)251–257, 2004. doi:10.1016/j.ijmedinf.2003.11.018.
8. Blobel, B., Comparing approaches for advanced e-health security infrastructures. *Int. J. Med. Inform.* 76 (5–6)442–448, 2007. doi:10.1016/j.ijmedinf.2006.09.012.
9. Blobel, B., Nordberg, R., Davis, J. M., and Pharow, P., Modelling privilege management and access control. *Int. J. Med. Inform.* 75 (8)597–623, 2006. doi:10.1016/j.ijmedinf.2005.08.010.
10. Blobel, B., and Roger-France, F., A systematic approach for analysis and design of secure health information systems. *Int. J. Med. Inform.* 62 (1)51–78, 2001. doi:10.1016/S1386-5056(01)00147-2.
11. CEN-ENV. Health informatics—Security for healthcare communication—Part 1: Concepts and terminology. Published Standard CEN ENV 13608-1:2000: European Committee for Standardization; 2000.
12. CEN-ENV. Health informatics—Security for healthcare communication—Part 2: Secure data objects. Published Standard CEN ENV 13608-2:2000: European Committee for Standardization; 2000.
13. CEN-ENV. Health informatics—Security for healthcare communication—Part 3: Secure data channels. Published Standard CEN ENV 13608-3:2000: European Committee for Standardization; 2000.
14. Chen, Y.-C., Chen, L.-K., Tsai, M.-D., Chiu, H.-C., Chiu, J.-S., and Chong, C.-F., Fingerprint verification on medical image reporting system. *Comput. Methods Programs Biomed.* 89 (3)282–288, 2008. doi:10.1016/j.cmpb.2007.11.007.
15. Choe, J., and Yoo, S. K., Web-based secure access from multiple patient repositories. *Int. J. Med. Inform.* 77 (4)242–248, 2008. doi:10.1016/j.ijmedinf.2007.06.001.
16. Choi, Y. B., Capitan, K. E., Krause, J. S., and Streeper, M. M., Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *J. Med. Syst.* 30 (1)57–64, 2006. doi:10.1007/s10916-006-7405-0.
17. Conrick, M., and Newell, C., Issues of ethics and law. In: Conrick, M. (Ed.), *Health informatics: transforming healthcare with technology*Thomson Social Science Press, Melbourne, 2006.
18. Delac, K., and Grgic, M., A survey of biometric recognition methods. 46th International SymPoSium Electronic in Marine. ELMAR 2004, Zadar, 2004.
19. Garson, K., and Adams, C., Security and privacy system architecture for an e-hospital environment. Proceedings of the 7th Symposium on Identity and Trust on the Internet. ACM, Gaithersburg, Maryland, 2008.
20. Gates, M. A., Biometrics—passing on using passwords. *Radiol. Today.* 8 (17)28–31, 2007.
21. Grain, H., Consumer issues in Informatics. In: Conrick, M. (Ed.), *Health informatics: transforming healthcare with technology*-Thomson Social Science Press, Melbourne, 2006.
22. Gritzalis, D., and Lambrinoudakis, C., A security architecture for interconnecting health information systems. *Int. J. Med. Inform.* 73 (3)305–309, 2004. doi:10.1016/j.ijmedinf.2003.12.011.
23. Heckle, R. R., and Lutters, W. G., Privacy implications for single sign-on authentication in a hospital environment. Proceedings of the 3rd Symposium on Usable Privacy and Security. ACM, Pittsburgh, Pennsylvania, 2007.
24. Hoque, S., Fairhurst, M. C., Deravi, F., and Howells, W. G. J., On the feasibility of generating biometric encryption keys. *IEEE Electron. Lett.* 41 (6)309–311, 2005. doi:10.1049/el:20057524.
25. IBG, Biometric Basics: What are the Benefits of Biometric Technology? In International Biometric Group Reports and Research International Biometric Group <http://www.biometricgroup.com/reports/public/reports_and_research.html>. Accessed, 2008
26. Liu, S.-L., Guo, B.-A., and Zhang, Q.-A., An identity-based encryption scheme with compact ciphertexts. *J. Shanghai Jiaotong Univ. Sci.* 14 (1)86–89, 2009. doi:10.1007/s12204-009-0086-3.
27. Lusignan, S. D., Chan, T., Theadom, A., and Dhoul, N., The roles of policy and professionalism in the protection of processed clinical data: a literature review. *Int. J. Med. Inform.* 76:261–268, 2007. doi:10.1016/j.ijmedinf.2005.11.003.
28. Marohn, D., Biometrics in healthcare. *Biometric Technol. Today.* 14 (9)9–11, 2006. doi:10.1016/S0969-4765(06)70592-6.
29. Ohno-Machadoa, L., Silveira, P. S. P., and Vinterbo, S., Protecting patient privacy by quantifiable control of disclosures in disseminated databases. *Int. J. Med. Inform.* 73 (7–8)599–606, 2004. doi:10.1016/j.ijmedinf.2004.05.002.
30. Pierce, F. S., Biometric identification. *Health Manag. Technol.* 24 (5)38, 2003.
31. Pons, A. P., and Polak, P., Understanding user perspectives on biometric technology. *Commun. ACM.* 51 (9)115–118, 2008. doi:10.1145/1378727.1389971.
32. Rash, M. C., Privacy concerns hinder electronic medical records. The Business Journal of the Greater Triad Area 2005 April 4.
33. Reynolds, P., The keys to identity: as healthcare organizations strive for greater security, some are using a very personal approach in the form of biometrics.(Security/Authentication) (Cover Story). *Health Manag. Technol.* 25(12):12(14), 2004.
34. Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., and Detmer, D. E., Toward a national framework for the secondary use of health data: an American medical informatics association white paper. *J. Am. Med. Inform. Assoc.* 14 (1)1–9, 2007. doi:10.1197/jamia.M2273.
35. Sahai, A., and Waters, B., Fuzzy identity-based encryption. Advances in Cryptolog EUROCRYPT 2005, 2005, pp. 457–473.
36. Schneier, B., Security engineering: a guide to building dependable distributed systems. Wiley, New York, 2001.
37. Shamir, A., Identity-based cryptosystems and signature schemes. Advances in Cryptology, 1985, pp. 47–53.
38. Shin, Y. N., Lee, Y. J., Shin, W., and Choi, J., 110 P.s.-. and 10.1109/WAINA.2008.289 D.O.I. Designing Fingerprint-Recognition-Based Access Control for Electronic Medical Records Systems. INAW 2008—2nd International Conference on Advanced Information Networking and Applications—Workshops, Okinawa, Japan, 2008.
39. Stamp, M., Information security: principles and practice. Wiley, Hoboken, 2006.
40. van der Linden, H., Kalra, D., Hasman, A., and Talmon, J., Inter-organizational future proof EHR systems: a review of the security and privacy related issues. *Int. J. Med. Inform.* 78 (3)141–160, 2009. doi:10.1016/j.ijmedinf.2008.06.013.