New Framework for Authentication and Authorization for e-Health Service Systems

Song Han, Geoff Skinner, Vidyasagar Potdar, Elizabeth Chang, Chen Wu

School of Information Systems, Curtin University of Technology, GPO Box U1987
Perth WA 6845, Australia.

Abstract-**The development of information technology has eased the medical services and provided the electronic health service in a way that a doctor can keep the records of patients in an information system and be informed of changes of status of patients, and make decisions promptly. However, there are increasing challenges over the privacy of patients due to the exposition of clinic information patients to ubiquitous networks. This paper introduces a framework for authentication and authorization in e-health services. It aims to build the architecture for authentication and authorisation within an e-health service system. The architecture will help to build a secure and privacy-protection e-health service system. The authors hope that understanding the underlying framework will not only inform researchers of a better design for e-health service, but also assist e-health systems developers in the understanding of intricate constructions within authentication and authorisation. Further, our paper highlights the importance of protecting the privacy of medical records of patients in terms of information privacy.**

I. INTRODUCTION

1.1 Background and Related Works

Web services are essential in enabling healthcare administrative members, medical professionals and patients to organise, share and access to the medical services. Due to the development of web technologies, security and privacy issues are rising over traditional medical services (Smith et al., 1999; Agrawal et al., 2004). These requirements can be met by promoting health-care security issues over web services. Web services should be used in such a way that timely and not too cumbersome access to health-care records be provided without compromising patients' privacy.

The purpose of an e-health service system is to take care of the patients. The most important asset of an e-health service system is the patient as well as the intelligence knowledge created by the related GP, specialist, or therapist. In addition to the need to protect the privacy of the patient is the sharing of patient data in order to ensure the availability of accurate and timely information to all authorised communicating partners. Security controls must thus be evaluated in terms of its functional benefits for protecting the privacy of the patient, whilst at the same time providing timely accurate information to service providers and physicians. As a result, governments, administrative bodies and the different players in the health service system are looking for innovative solutions to make health services more efficient and secure.

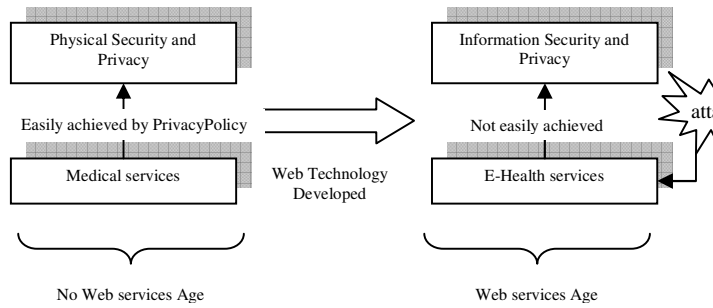


Figure 1. Changes of Security and Privacy for health service

Data privacy is a growing concern among health care sector, which are entrusted with the responsibility of managing patient information. Access control mechanisms are essential in protecting sensitive patient information. These mechanisms should provide for simultaneous access to different patient data, for example, health history, patient-case data, administrative data and the like. In addition, patients require access to various hospital services and features that will enhance their comfort and safety. Access control includes two primary aspects, namely to deny access to health-care data to those users who do not have the right of access and, secondly, they need to guarantee access to all relevant data to those database users who exercise their access privilege properly.

Authorisation is effected according to the access rights specified for each user role. All access-controls may, however, be overridden by specially authorised clinicians using the emergency functions. The principal aim is to develop and implement need-to-know access-controls that would protect patients' medical health data.

In terms of these controls, the user would only be allowed to access information necessary to complete his or her job. A secretary would, therefore, be unable to access a patient's clinical data, whilst a doctor would be. On the other hand, in health-care information systems, it may be necessary to realise two or more databases in one system. For example, if a doctor wanted to hide the real name of a possible disease from a patient in a critical condition until such time as the diagnosis has been confirmed by laboratory tests, the database viewed by the patient should be different from the one used by the doctor. Situations like these need to be controlled,

In an emergency situation, a doctor may need to access information on a patient as soon as possible. This doctor should be first authorised but not authenticated since she/he is an on-duty doctor. Therefore, in order to save time, react efficiently and save life of the underlying patient, it is essential to propose and develop a framework for authorisation and authentication architecture for e-health service system.

Smith et al. (1999) discussed the trends on security issues with respect to health care information systems. They reviewed the protection of electronic patient records, health care information over the Internet, the application of patient smart cards, the need-to-know access control in protecting sensitive patient information and the database security policies for medical databases. They also reviewed the legal issues related to information technology in the health care sector. In addition, they discussed a number of possible research areas for health care information systems. They pointed out that access control mechanisms that can be effectively control access to patient data in health care systems should be further investigated.

Blobel et al. (2006) focused on the application security challenges and proposed an architectural approach of security. They developed a series of formal models of domains, service delegation, claims control, policies, roles, authorisations, and access control for health information system. Their approach allow for the central management of the users, privileges, rules, policies and separation of security management and secure application functions. It enables scalability of both security services and mechanisms on one hand and applications on the other.

Lopez et al. (2005) stated that most of authentication and authorisation services focus on either authentication or authorisation, and are not complete. It is necessary to extend the scope of security solutions by providing an integrated authentication-and-authorisation service for communicating peers. The disadvantage of their methodology is authentication and authorisation are integrated into one single function process. However, that is not practical for some real-world applications, for example, e-health service system, where authorisation and authentication should be set up in a scenario: there is an e-health service system (EHSS), in which there are a GP, a Specialist, a Dentist, a Therapist, a Chemist, and a Nurse. All these entities are registered users of the EHSS. Then, by the authorisation policy, they will be authorised to enter into the authentication level if they show their passes. Because they have different roles, they will be assigned different Read/Write capabilities once they are authenticated and identified by the authentication mechanism.

Li et al. (2005) studied the problem of patient privacy protection related to medical images. They tried to make an effort towards protecting against unauthorised release of images by an authorised recipient. They proposed a fingerprint model suitable for many-to-many multicast, that is computationally efficient and scalable in user storage and key update communication.

Lopez et al. (2004) surveyed and discussed Microsoft .NET and some related activities (e.g. the Liberty Alliance project), Kerberos-based solutions, digital certificated and public key infrastructures that all can be used to build and operate authentication or authorisation infrastructure. One of their observations is that there is no single best approach for providing an authentication and authorisation infrastructure. Lopez et al. (2004) stated that "… to the observation that e-commerce requires an authentication service only in the foreground, and that an authorization service is very important from a commercial and practical point of view. In this sense, an authentication delivers proof that the identity of an object or subject has indeed the identity it claims to have, while the authorization one means the granting of permission on the basis of authenticated identification. "

The above observation implied that authorization is based on the result of authentication. If the result of authentication is negative/positive, then the result of authorization is negative/positive. In other words, if the authentication for an entity is not successful, then the authorization for the underlying entity will not be granted. However, that principle/observation is not practical to an e-health environment. Why? This is because in e-health environment, each entity (e.g. a GP, a Specialist, …. , a Patient, a Nurse) has a pseudo identification number (e.g. a staff number or a patient number). Whoever holding this kind of number should be authorized to enter into the e-health system. However, that does not mean they can access to every subarea of the underlying e-health system. At this point, role-based authentication will be activated if the underlying entity (e.g. a GP, a Specialist, …. , a Patient, a Nurse) wants to access to some specific subarea (e.g. a subarea where a doctor can provide health service to some patients suffering from insomnia) of the e-health system.

In this article, we will focus on the design of a practical architecture for authentication and authorization within an e-health environment. So far no research focus on authorization and authentication has addressed a practical solution to this issue within an e-health environment.

1.2 Motivation of Proposing a Framework for Authentication and Authorisation for e-Health Services

The aim of our article is to develop a framework for authorization and authentication for identity management within an e-health service system that are critical for the success, security and privacy of the underlying system both from a strategic and information technology perspective.

Most of the existing research proposals that study authorization and authentication have separated the function of authorization and authentication in terms of access control and identity management, for example, . Microsoft .NET passport (Oppliger, 2003) utilized the authentication approach as the main access control principle; while, the others, e.g. Zhang et al. (2003) studied authorization approach as the main access control principle. In other words, some of the existing works focus on the role-based authentication and authorization [Sandh et al. 1996]; while others focus on attribute-certificate based authentication and authorization, e.g. authentication and authorization infrastructure (AAI) or privilege management infrastructure (PMI) (Farrell et al. 2002; Schlaeger and Pernul, 2005; Lopez et al. 2005; Blobel et al. 2006)

The disadvantage of those studies is that: (1) they did not consider the mutual and sequential impact of authorization and authentication in terms of access control and identity management. (2) They lack of the analysis of the relationship between authorization and authentication from e-health service perspective. Therefore, it is essential to further investigate the relationship between authorization and authentication over access control and identity management, especially from an e-health service system perspective. More importantly, this will be beneficial to the protection of the corresponding patients' information and clinic records within the underlying e-health service system. This is because: (1) we simultaneously utilize the authorization principle and authentication principle within the access control of the underlying e-health service system; (2) we then sequentially cooperate/place the function position of authorization and authentication in a way that the authorization principle acts as the outspace pass as well as innerspace pass to the e-health service system, while the authentication principle acts as the innerspace pass to the underlying e-health service system.

II. Significance of Authentication and Authorisation for e-Health Services

An electronic health service system, is a collection of components working together to implement the e-health services. Because data is processed into practical information by the information system, authentication and authorisation become one of the essential concerns of the e-health service systems. This means that the system should protect data and the information produced from the data from having its confidentiality, integrity and availability violated on any layer.

The proposed architecture for authorisation and authentication for e-Health services system is a practical and new solution for access control within e-health service systems since presently there is no such solution that focuses on the authorisation and authentication simultaneously and sequentially for the access control within e-health service system as one of the applications in real-world scenario.

The architecture will help to build a secure and privacy-protection e-health service system. Physicians participating in a secure e-health service system can benefit from a mix of cooperative resource sharing strategies and cooperative profit sharing strategies.

III. Authorisation and Authentication Architecture for e-Health Services

The proposed authorisation and authentication architecture for e-health services (A3AeHS) system will integrate the role-based method (Hitchens et al. 2000) and the attribute certificate (or privilege) based method (Blobel et al. 2006) into the electronic health service system.

3.1 Authorisation Implication

Authorisation is the policy-driven limitation of access to e-health service systems and the related data.

1. The first step in creating an authorisation policy is to enumerate all of the underlying e-health service system. For example, given an electronic health record of a patient who is registered with the e-health service system, we should enumerate what is history health record (e.g. for reference purpose), what is current general health record (e.g. for physiotherapy purpose), and what is critical health record (e.g. for saving life purpose).
2. The second step in creating an authorisation policy is to determine how sensitive each record is for the underlying e-health service system (especially for patients).
3. The third step in creating an authorisation policy is to determine who should access to each record. For example, a GP can access to all the records of an patient, while a Specialist can only access to a specific record.
4. The fourth step in creating an authorisation policy is to determine the specific authorisation that a role should have for the record. This step is to assign different privileges to different roles in an e-health service system.
5. By the step 3 and 4, we will integrate the role-based and privilege-based policies into the authorisation policy for the underlying e-health service system. Thus, we create the Role-and-privilege-based authorisation policy. That can assign the different levels of privileges by the different roles. This is critical for an e-health service system.

3.2 Authentication Implication

Authentication is the process of verifying the identity of a role in an e-health service system. In our framework, the two-factor authentication mechanism will be integrated into the authorisation and authentication architecture for e-health

service system (A3AeHS). In the two-factor authentication mechanism, each role of the underlying e-health service system is required to use a biometric authentication (Fingerprints, 2005) together with a digital PIN authentication. If and only if the two-factor authentication is successful, the authorisation policy mechanism will be activated and the authorisation right will be granted to the underlying individual.

3.3 Architecture of Authorisation and Authentication within e-Health Service System

The architecture for authorisation and authentication within e-health service system should address the topology of authorisation and authentication and the grading of authorisation and authentication.

The topology of authorisation and authentication can classify the architecture of authorisation and authentication within e-health service system in a security overview.

The following figure shows the topology of the authentication and authorisation for e-health service system.

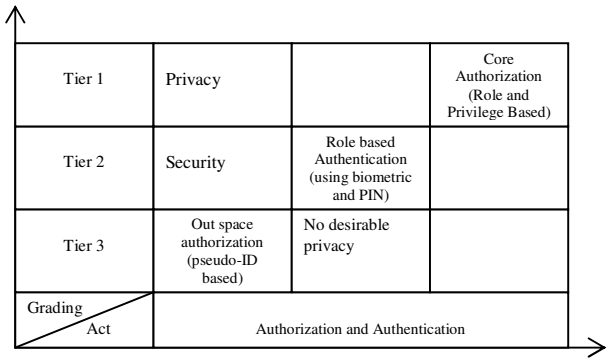
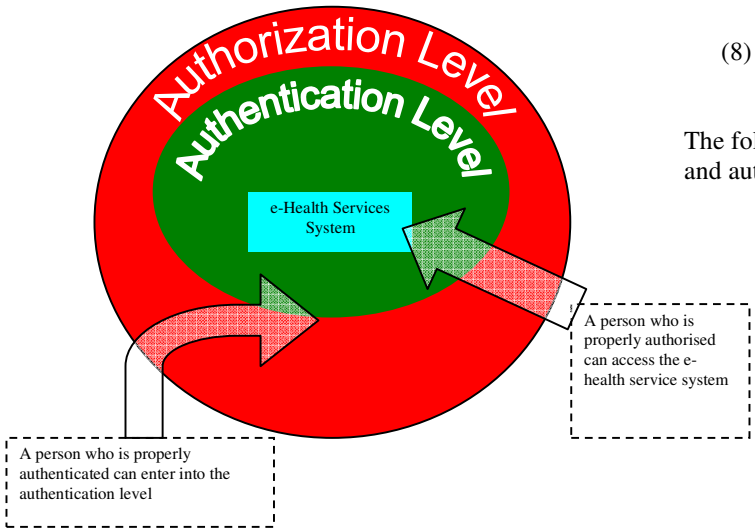


Fig 3. Grading of Authorisation and Authentication for e-health service system



The proposed grading of authorisation and authentication is displayed in the following figure Fig 3.

The grading of authorisation and authentication can rank the level of authorisation and authentication within an e-health service system. This will clarify that the different fundamental function of authorisation and authentication on the security and privacy for e-health service systems.

3.4 Authorisation and Authentication Procedure within e-Health Service System

Consider there are Dentist, GP, Specialist, Nurse, Chemist and a number of patients, who will first register with an e-health service system. Suppose the GP wants to access an electronic health record within the e-health service system.

(1) The users first register at the administrator with the e-health service system will send an access request by the access request agent.
(2) If needing service from the system, the user, for example, one GP, generates an access request.
(3) The access request agent then sends the access request token to the administrative agent.
(4) The administrative agent then refers to the authorisation policy of the system and then sends the preliminary authorisation reference for the GP.
(5) The GP will be authenticated based on the biometric information and the digital PIN. If the authentication is successful, the GP will be granted a formal authorisation reference.
(6) By the formal authorisation reference, the GP will be verified whether he has the privilege of reading/writing into the e-health service system.
(7) By the role-and-privilege based authorisation policy, if the GP's status satisfies the requirements of the policy, the identity of the GP will be send to will be sent to Authentication agent.
(8) If the identity of the GP is correctly identified, he will granted to access to the targeted patient electronic health record.

The following figure displays the procedures for authorization and authentication within the e-health service system.

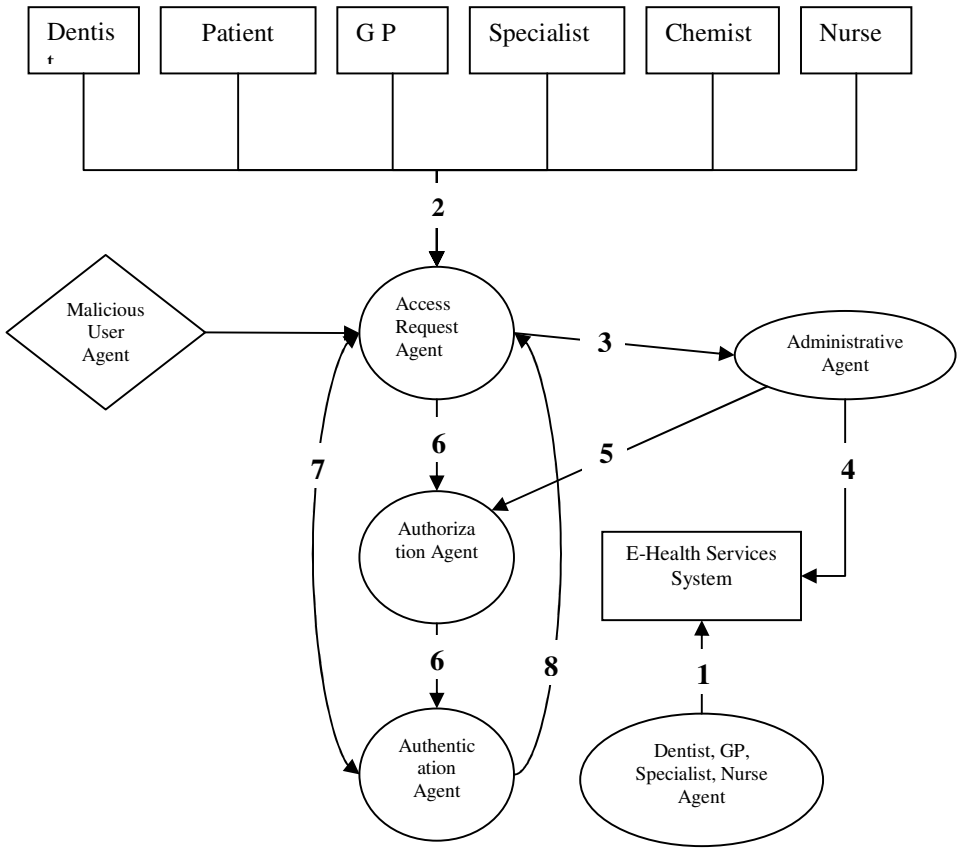


Fig 4. Procedures for authentication and authorization

IV. DISCUSSIONS

This architecture can better guarantee the confidentiality of the underlying e-health service system. This is because the proposed architecture utilised both authorisation and authentication that initial the access control over the underlying e-health service system.

This architecture can maximize the possibility of fitting the real-world applications. Specially, this is suitable to the e-health service system, where the authorisation should be first initialled, and the two-factor authentication, and then followed by the role-and-privilege based authorisation. This will help different roles with access to different levels of the underlying e-health service system.

This architecture can better preserve the privacy of the underlying patients' information and clinical records within the e-health service system, as well as protect the intelligence copyright of the underlying GP, specialist, dentist or therapist who has contributed to the treatment of the corresponding patients. This is because the integrated authorisation mechanism is a role-and-privilege based authentication.

V. CONCLUSIONS

This paper presented a framework for authentication and authorisation for e-health services system. The framework provides the architecture for authentication and authorisation. The proposed architecture integrated the role-based access

control and the privilege-based access control into the authorisation and authentication services. This will better suit to the e-health service system in terms of identity management. The authors hope that the proposed framework would help the developing and administration of e-health service systems in a secure, efficient and flexible way. In the next step of this research, we will design and implement the authorisation policy and the role-and-privilege based authentication for e-health service systems.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers.

REFERENCES

[1] Agrawal R, Kini A, LeFevre K, Wang A, Xu Y and Zhou D (2004) Managing Healthcare Data Hippocratically. Proc. of ACM SIGMOD Intl. Conf. on Management of Data, 2004.

[2] Blobel B (2006) Advanced and secure architectural HER approaches. International Journal of Medical Informatics, 75: 185-190.

[3] Blobel B, Nerdberg R, Davis JM, Pharow P (2006) Modelling privilege management and access control. International Journal of Medical Informatics, 75: 597-623.

[4] Chiu YH, Chen LS, Chan CC, Liou DM, Wu SC, Kuo HS, Chang HJ, Chen HH (2006) Health information system for community-based multiple screening in Keelung Taiwan. International Journal of Medical Informatics, 75: 369-383.

[5] Clarke, R. (1999), Introduction to dataveillance and information privacy, and definitions and terms. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

[6] Farrell S, Housley R (2002) An Internet attribute certificate profile for authorisation. Request for comments 3281. IETF PKIX Working Group.

[7] Gobuty DE (2004) Defending medical information systems against malicious software. International Congress Series, 1268: 96-107.

[8] Goldberg, I. (2002), Privacy-enhancing technologies for the Internet, II: Five years later. PET2002, San Francisco, CA, USA 14 - 15 April 2002.

[9] Han Z, Liu CP (2000), Fingerprint classification based on statistical features and singular point information. Advances in Biometric Person Authenticaiton, International Workshop on Biometric Recognition Systems, Beijing, October 22-23, 2005, 119-126.

[10] Hes, R. and Borking, J. (2000), Privacy-enhancing technologies: The path to anonymity. Registratiekamer, The Hague, August 2000.

[11] Hitchens M, Varadharajan V (2000), Design and specification of role based access control policies. IEE Proceedings in Software, 47(4):117-129.

[12] Knaup P, Garde S, Merzweiler A, Graf N, Schilling F, Weber R, Haux R (2006) Towards shared patient records: an architecture for using routine data for nationwide research. International Journal of Medical Informatics, 75: 191-200.

[13] Lopez J, Oppliger R, Pernul G (2004) Authentication and authorisation infrastructure (AAIs): a comparative survey. Computers and Security, 23: 578-590.

[14] Li M, Poovendran R, Narayanan S (2005) Protecting patient privacy against unauthorised release of medical images in a group communication environment. Computerized Medical Imaging and Graphics, 29: 367-383.

[15] Lopez J, Montenegro JA, Vivas JL, Okamoto E, Dawson E (2005) Specification and design of advanced authentication and authorisation services. Computer Standards and Interfaces, 27: 467-478.

[16] Misic J, Misic VB (2006) Implementation of security policy for clinical inforamtion systems over wireless sensor networks. Ad Hoc Networks.

[17] Quantin C., Allaert F., Dusserre L (2000) Anonymous statistical methods versus cryptographical methods in epidemiology. International Journal of Medical Informatics, 60: 177-183.

[18] Ravera L, Colombo I, Tedeschi M, Ravera A (2004) Security and privacy at the private multispecialty hospital Istituto Clinico Humanitas: strategy and reality. International Journal of Medical Informatics, 73: 321-324.

[19] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (1996) Role-based access control models. IEEE computer, 29(2): 38-47.

[20] Schlaeger C, Pernul G (2005) Authentication and authorisation infrastructures in b2c e-commerce. EC-WEB 2005, Lecture Notes in Computer Science, 3590: 306-315.

[21] Smith E., Eloff JHP (1999) Security in health-care information systems-current trends. International Journal of Medical Informatics, 54: 39-54.

[22] Oppliger R (2003) Microsoft .NET Passport: a security analysis. in health-care information systems-current trends. IEEE computer, 36(7): 29-35.

[23] Zhang K, Kindberg T (2003) An authorisation infrastructure for nomadic computing. Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT).