An Access Control Framework for Protecting Mobile Health Records: The Case Study of Developing Countries

R.Ssembatya

Department of Computer Science, University of Cape Town, South Africa
e-mail: richard.ssembatya@uct.ac.za

Abstract

Mobile health records are a good way of providing users with on-demand access to health care data. Standard approaches of securing health records include role-based access control (RBAC) because this is a flexible approach to assign permissions to a wide variety of users. However, traditional RBAC models are not designed to enforce fine-grained access control. For instance, in mobile health record systems, it is difficult to configure a policy that permits a patient to selectively share his/her personal records with healthcare workers. Therefore, defining policies that express application-level security requirements with respect to mobile records is challenging. In this paper, we present an RBAC inspired framework that provides fine-grained encryption for mobile health records where patient records have different access control policies. Our proposed framework ensures that the data can be made available securely offline. This approach can leverage systems where information needs to be shared securely under constraints of energy and/or Internet coverage.

Keywords

Role Based Access Control, Attribute-Based Encryption, Mobile Health Records

1. Introduction

Electronic health records (EHRs) are basically medical records in electronic format (Markle Foundation, 2004; department of health and human services, 2006). EHRs can exist on a variety of computing devices and can be accessed online via Internet technologies. The popularity of the Internet as a vehicle for communication has resulted in an increased drive to cut the costs of healthcare services by encouraging the use of EHRs. The new healthcare scenario has led to the provision of web services that support the distribution of healthcare information. The process by which healthcare information is shared can be depicted as shown in figure 1 below. The hospital server runs an access control program that verifies that the parties (health workers, insurance companies and other healthcare organization) accessing patient's records have appropriate permissions. When a user makes a request to access the records, access control authorities verify the request and determine the access rights. A user with appropriate permission(s) will be able to access the records.

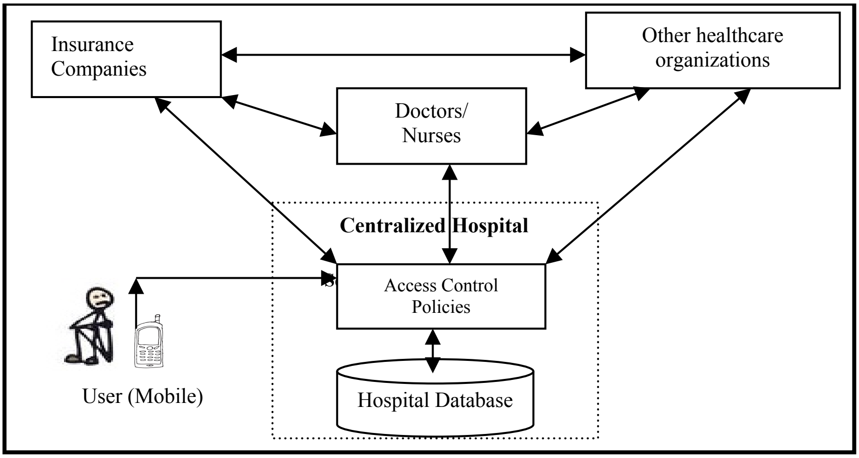


Figure 1: E-Health Scenario

Although a lot of work has been done in the design of Internet-based health care systems, little has been done on tailoring these systems to mobile devices yet, to date, mobile phones are one of the most widely used computing devices in the world.

Furthermore, mobile phones are increasingly becoming cheaper and affordable especially to the population in developing countries particularly in Africa. Given the fact that most parts of Africa are characterized by general poor infrastructure such as bad roads, poor transport systems, non-existent electricity in rural areas, lack of centralized services and frequent power outages in urban areas, mobile phones could provide a better alternative way to access EHRs. However, as in conventional Internet-based systems, mobile health records raise questions pertaining to security and privacy (Fisher and Madge, 1996). Users want the convenience of data access and availability but are also concerned about cases of unauthorized access (Annas, 2003; Li et al, 2005).

Securing and guaranteeing availability of mobile health records is a complex and difficult task to accomplish. One of the methods of guaranteeing privacy in E-health systems is via access control (Benaloh et al, 2009). Access control mechanisms are designed to secure data at the server to verify that patients' records are accessed by authorized users. In many cases, this has been a fairly effective approach. However, when the server fails or becomes unavailable for example due to power outages that is common in developing countries, access control decisions cannot be made, making EHRs unreachable. In addition, access control approaches such as traditional RBAC model are not designed to provide fine-grained access control. For instance, in mobile health record systems, it is difficult to configure a policy that permits a patient to selectively share personal records to healthcare workers. In addition, although there several XML-based standards such as Clinical Document Architecture (CDA) that calls for protecting EHRs, none of the standards provide enough guidelines for protecting and transporting EHRs (HL7 web site, 2011). Therefore, a mobile access control framework that protects and selectively shares EHRs using a mobile phone is a good way of ensuring secure and on-demand access to EHRs. The aim of the framework is to empower patients to grant access to specific potions of their data without the need for a single centralized server. As well, the proposed framework supports the availability of EHRs even when hospital servers are offline. This reduces the need to rely on server based access control authorizations for the provision of EHRs.

The rest of the paper is structured as follows. In Section 2, the background work on role-based access control schemes for enforcing security and privacy of mobile health data is presented. In Section 3, the proposed access control framework that is inspired by the concept of attribute-based encryption is introduced, followed by an example scenario in healthcare environment in section 4. Finally, in Section 5, conclusions are given and future work is discussed.

2. Related Work

In this section, a survey of related work that motivates this paper is discussed, first by providing an overview of the existing access control architecture for patient centered health record systems and then examine some of the techniques that investigate the problem of enforcing access control policies for selective sharing of EHRs.

Szolovits et al (1994) introduced the concept of patient centered health information systems that integrate personal health information across institutions. Szolovits's concept was extended by Simons et al, (2005) to build the PING architecture which enables a patient to maintain electronic copies of his/her records that are encrypted at a storage site of the patient's choice. The PING server handles encryption and performs the authentication as well as authorization of users. Similar to PING is Indivo (Mandl et al, 2007). Indivo is an online system that keeps patient's health data encrypted at the Indivo server. Access control decisions are mediated by the Indivo server according to institutional defined security policies. This approach violates the design goal described above, since the trusted Indivo server must be kept online in order to mediate access control decisions.

Gupta et al (2006) developed a criticality-aware access control model which regulates access control for pervasive applications. However, their model did not provide a fine grain control on when and who can exercise the extra privileges needed for an emergency situation. Ardagna et al (2010) extended the criticality-aware access control model (Gupta et al (2006)) to provide a break-the-glass model where policies are separated into different categories starting with access control policies, emergency policies and a break-the-glass policy. When a user requests an access, the system checks regular access control policies and if the request is denied, the system overrides the decision by break-the-glass policy. The drawback of this approach is that the override depends on a fixed decision procedure that does not consider reasons for denial. Literature also reveals other access control models based on purposes (Byun et al (2005) and Yang et al (2007)). However, according to Jin et al (2009), purpose based access control alone cannot meet all the patient's privacy protection requirements.

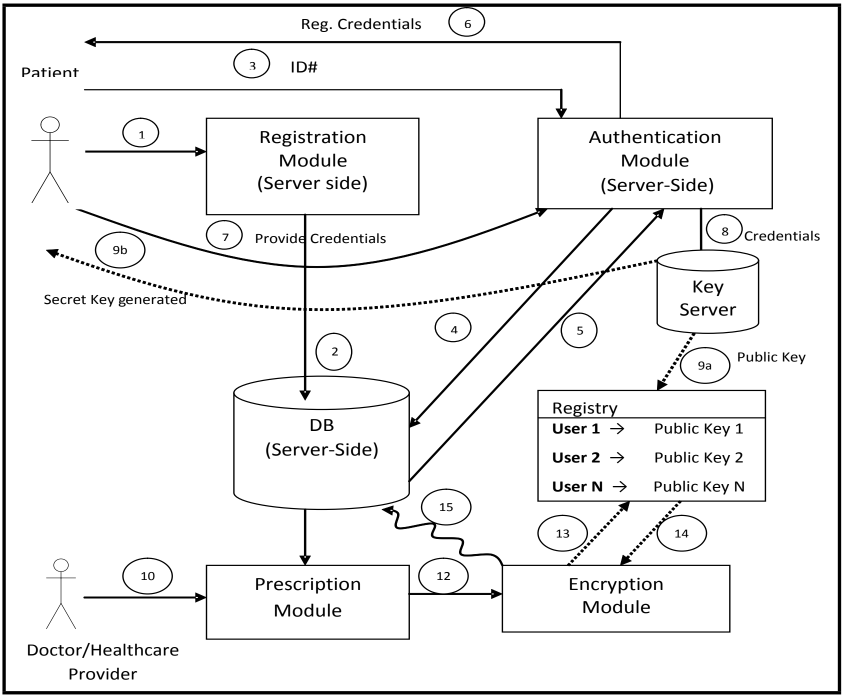
The Role based access control (RBAC) model is commonly used in E-health systems for securing access to EHRs (Sandhu et al, 2002; Eyers et al 2006). Solutions proposed by Becker and Sewell (2004), Bhatti et al (2006), Georgakakis et al (2011) and Eyers et al (2006) use RBAC mechanism to address organizational security management and provide meaningful access control decisions for EHR systems. However, none of them support selective sharing of EHRs and thus cannot support a more fine-grained access control.

Benaloh et al (2009) explored the challenges of preserving patient's privacy and advocated that security in EHR systems be enforced via encryption in addition to access control policies. They proposed hierarchical identity based encryption (HIBE) and searchable encryption to construct a privacy preserving EHR system. The system allows a patient to selectively share the records among doctors and healthcare providers without the need to rely on an online server for access control decisions. Selective sharing is based on hierarchical encryption. Patient's records are partitioned into hierarchical structure and each portion is encrypted with a corresponding key. Private sub keys are derived from root private key by the patient. The drawback of hierarchical based encryption is the limitation of flexibility in the access structure that is, it does not allow more expressiveness in the access structure.

3. Access Control Framework

The framework utilizes the recent development of dual-policy attribute based encryption which combines ciphertext-policy attribute based encryption and Key-policy attribute based encryption to support more expressiveness in the access structure (Attrapadung and Imani 2009). Dual-policy attribute based encryption was built on the concept of attribute based encryption (ABE) introduced by Sahai and Waters (2005). In an ABE system, user's keys and ciphertexts are labeled with a set of descriptive attributes. A particular key can be used to decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key (Goyal et al, 2006; Bethencourt et al, 2007; Waters, 2008). ABE system enables an access control mechanism over encrypted data by specifying access policies among private keys and ciphertexts. ABE is typically described in two flavors; ciphertext-policy ABE and key-policy ABE. In ciphertext-policy ABE, each ciphertext is bound together with a policy describing who is entitled to decrypt it (Bethencourt et al, 2007). The user's private key will be associated with an arbitrary number of attributes expressed as strings. In the proposed framework, when the hospital data clerk enters records for encryption, he also specifies an associated access structure over attributes. A user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertext's access structure. The roles of the users in the healthcare organization are defined by the user attributes, which in turn specify the permissions that the user can be assigned. Users with a given role can access the records using role key.

The second flavor of ABE is key-policy ABE (Goyal et al, 2006; Sahai and Waters, 2005). With key-policy ABE, individual patient records are tagged with XML specific attributes and access to these records are granted by generating private keys that are embedded with access policies determining which records may be accessed. In the proposed framework, key-policy system provides keys to temporary users such as researchers that have limited access to EHRs database. Individual keys then specify a particular policy defining which records the key can access.



Registry	
User 1 →	Public Key 1
User 2 →	Public Key 2
User N →	Public Key N

Figure 2: An Access Control Framework

Figure 2 above provides an overview of the components of the framework. When the record is created, the prescription module parses the record into an XML hierarchical structure where sensitive parts are selected for encryption under a policy that is appropriate for the record. The marked parts can then be encrypted using ciphertext-policy ABE (where the role of the parties is taken by the attributes and the access structure contains authorized sets of attributes) or key-policy ABE scheme under a set of attributes such as patient age, date of birth or any other non sensitive attributes that are related to the record. Once the records have been encrypted, it can be stored at the hospital server (Figure 2 (2)) and can also be exported to a patient's mobile phone.

The provider can continue accessing the locally stored records using the existing access control of the records. However, anyone without an appropriate ABE private key that satisfies the policy will not be able to decrypt the records.

A trusted master controller (key server Figure 2 (8)) manages ABE decryption keys and RSA public and private keys. The RSA public and private key pair enables patients to securely download and receive key updates. The keys are manually delivered onto patient's mobile phones (e.g. through the use of a USB) in order to prevent the most likely online attacks. This narrows the attack model of the key server to attackers who have only physical access. Both individual hospital employees and the patients obtain their ABE decryption keys from an offline key server. The patients can view their records by using a mobile health application browser to access the records. The application should access appropriate hospital server storage to download the ciphertext-policy ABE encrypted records. The encrypted records can then be stored on the patient's mobile phone for portability.

To prevent malicious users from accessing the key on the mobile phone, a random passphrase provided by the user will be used to encrypt the key on the patient's mobile phone using SQL Cipher encryption scheme (Android web site, 2011). The scheme is an SQLite extension in Android that provides transparent 256-bit AES encryption on a mobile phone (Android web site, 2011). "The data protected by this type of encryption and stored by Android apps is less vulnerable to access by malicious apps, protected in case of device loss or theft, and highly resistant to mobile data forensics tools that are increasingly used to mass copy a mobile device during routine traffic stops" (Android web site, 2011).

3.1. Key Revocation

User revocation is an important yet difficult issue in E-health systems. One major limitation in dealing with revocation of users in any system is that access to data that users have already seen cannot be revoked. Luan et al (2009) proposed an architecture that deploys an online mediator for every decryption such that revoked users cannot be authenticated. The drawback of this architecture is that the mediator must be kept online in order for users to decrypt thus violates the main design goal of this study. The proposed framework enforce revocation by associating user's secret key with an expiration date say Y. Records are encrypted on some date Z such that users can decrypt only if Y>=Z. The access privilege of users will be automatically revoked after the expiration date. To enable earlier revocation of users, we adopt (Yu et al (2008)) architecture that supports revocation by broadcasting an update message to update CP-ABE public and private keys. The hospital administrator simply encrypt the patient's new ABE key with the patient's RSA public key and make them available in a key chain for downloads.

3.2. Granting Access

Authorized hospital employees and patients obtain their keys from the hospital's ABE master controller (key server). In the proposed framework, two types of keys can be generated; a ciphertext-policy key or role key; each key corresponds to user roles and is embedded with fixed attributes that are related to the user. For example, patient age/name, user type (doctor, Lab technologist, patient, counselor), department and key expiration date.

3.3. Access Policy

The access policy of the framework consist of monotone Boolean formula that use only logical 'and' and logical 'or' gates referencing a list of attributes that are embedded into user's private key. For instance, given the attributes Doctor, Nurse, and health centre 3 (HC3), the hospital may specify a policy to allow a record to be read by a Doctor or Nurse or a consultant with ID = CID005, all attached to HC3.

$$((\text{Doctor} \vee \text{Nurse}) \wedge \text{HC3}) \vee \text{ID: CID005})$$

The ciphertext-policy and the key-policy ABE approaches can be combined into a single scheme referred to as dual-policy ABE scheme (Attrapadung and Imani, 2009). The scheme enables multiple users to access similar/the same medical record provided the users satisfy the authorization constraints. Our framework combines the two approaches. The encryptor (hospital administrator/data clerk) associate the record simultaneously with both a set of attributes that annotate the record itself and an access policy that states the type of users that will be able to decrypt the record. Similarly, a user is given a private key assigned simultaneously for both a set of attributes that annotate user's credentials and an access policy that states the type of record the user can decrypt.

4. Example Scenario

Consider the case of a hospital where Grace is a data clerk and John a patient. When Grace submits a new or modified record for storage at the hospital server, the record is parsed into an XML structure where sensitive parts are selected for encryption by encryption module under an appropriate role based access policy. Users (Patients and healthcare workers) whose attributes satisfy the access policy are able to decrypt the records with their secret attribute keys. The policies are initially specified by the hospital in order for the system administrator to make meaningful access control decisions. The encrypted records are then transferred to the hospital's own server for storage and can also be exported to a patient's mobile phone to facilitate offline access.

John (patient) presents the appropriate credentials to the hospital. Since some nations in developing countries do not have national IDs, John's credentials may be *(e.g. Passport, driving permit, National social security card (NSSF) e.t.c.)* for proper authentication. After John has been authenticated, the hospital ABE master controller (key server) generates John's ABE private key and subsequently send it to John's mobile phone. John then uses the mobile health application browser to interface with the hospital server and download the ciphertext-policy ABE encrypted records as shown in Figure 3.

The hospital server supports only read access to the encrypted individual health records and the encrypted records can be exported on John's mobile phone for portability. In order to enable offline access, John uses ABE private keys stored on the mobile phone to decrypt the records. John may decide to share encrypted records using Bluetooth technologies or decrypt the records and share them with a physician through the exchange of mobile devices. We recognize this as a limitation and an open problem for future research.

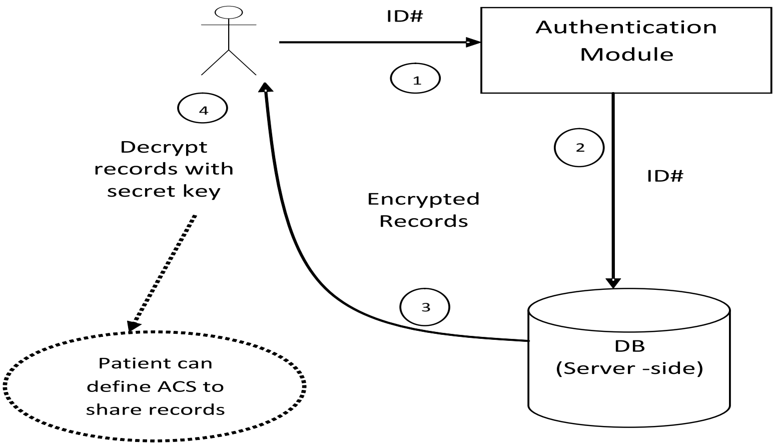

ID#
Authentication Module
1
4
Decrypt records with secret key
2
ID#
Encrypted Records
3
DB (Server -side)
Patient can define ACS to share records

Figure 3: Patient Downloads the Records

5. Conclusion and Future Work

Controlling access to EHRs is a key requirement of mobile health systems. Access control models such as RBAC can be used to authorize access to various healthcare resources. However, RBAC is not equipped to support selective sharing of composite EHRs and so cannot support fine-grained access control. Additionally, when hospital servers are unavailable, access control decisions cannot be made, making EHRs unreachable. In this paper, an access control framework that makes use of Attribute Based Encryption (ABE) is proposed. ABE is used to provide fine-grained based encryption restricting access of EHRs. Furthermore, it provides an access control mechanism over encrypted data by specifying access policies among private keys and ciphertexts.

In order to assess the usability and practical importance of our framework, a system implementation appears an interesting future work.

6. References

Android Web Site (2011). http://giv.to/cP9Lnu. (Accesses 4th June 2011).

Annas, G. J. (2003), "HIPAA Regulation - A New Era of Medical Record Privacy", *The New England Journal of Medicine* 348:1486-1490.

Ardagna, C., Vimercati, S., Foresti, S., Grandison, T., Jajodia, S. and Samarati, P. (2010), "Access control for smarter healthcare using policy spaces", *Computers & Security* Vol. 29, pp. 848-858, 2010.

Attrapadung, N. and Imani, H. (2009), "Dual-Policy Attribute Based Encryption", *in Proc. ACNS,* 2009, pp.168-185.

Becker, M. Y. and Sewell, P. (2004), "Cassandra: Flexible trust management applied to electronic health records", *In Proc. of IEEE 17th Computer Security Foundations Workshop*, pages 139–154.

Benaloh, J., Chase, M., Horvitz, E. and Lauter, K. (2009), "Patient controlled encryption: Ensuring privacy in medical health records", *In ACM CCSW* 2009.

Bethencourt, J., Sahai, A. and Waters, B. (2007), "Ciphertext-policy attribute-based encryption", *In Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 321-334. IEEE Computer Society.

Bhatti, R., Moidu, K. and Ghafoor, A. (2006), "Policy based security management for federated healthcare databases (or RHIOs)", *In Proc. of the international workshop on Healthcare information and knowledge management*, pages 41–48.

Byun, J. W., Bertino, E. and Li, N. (2005), "Purpose based access control of complex data for privacy protection", *In Proc. of 10th ACM symposium on Access control models and technologies (SACMAT)*, pages 102–110.

Eyers, D. M., Bacon, J. and Moody, K. (2006), "OASIS role-based access control for electronic health records", *In IEEE Proceedings*, pages 16–23.

Fisher, F. and Madge, B. (1996), "Data Security and Patient Confidentiality: The Manager's Role", *The International Journal of Bio-Medical Computing*.

Georgakakis, E., Nikolidakis, S. A., Vergados, D. D. and Douligeris, C. (2011) "Spatio temporal emergency role based access control (STEM-RBAC): A time and location aware role based access control model with a break the glass mechanism" *ISCC* 2011, pp. 764-770

Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006), "Attribute-based encryption for fine-grained access control of encrypted data", *In Proceedings of the 13th ACM conference on Computer and communications security*, pages 89-98.

Gupta, S., Mukherjee, T. and Venkatasubramanian, K. (2006) "Criticality aware access control model for pervasive applications, *In Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communications*, Pisa, Italy, 2006.

HL7 Web Site (2011). http://www.hl7.org/. (Accesses 24th March 2012).

Hu, J., Chen, H. and Hou, T. (2009), "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", Computer Standards and Interfaces, 32 (5-6): 274–280.

Jin, J., Ahn, G. J., Hu, H., Covington, M. J. and Zhang, X. (2009), "Patient centric authorization framework for sharing electronic health records", *SACMAT'09,* June 3–5, 2009, Stresa, Italy

Li, M., Poovendran, R. and Narayanan, S. (2005), "Protecting Patient Privacy against Unauthorized Release of Medical Images in a Group Communication Environment", *Computerized Medical Imaging and Graphics,* 2005.

Luan, I., Milan, P., Svetla, N., Pieter, H. and Willem, J. (2009) "Mediated ciphertext-policy attribute-based encryption and its application", *In WISA*, 2009.

Mandl, K., Simons, W., Crawford, W and Abbett, J. (2007), "Indivo: a personally controlled health record for health information exchange and communication", BMC Medical Informatics and Decision Making, 7(1): 25.

Markle Foundation (2004), "Connecting for Health. Connecting Americans to their healthcare. Final report of the working group on policies for electronic information sharing between doctors and patients", New York: www.connectingforhealth.org/resources/final_phwg_report1.pdf. (Accessed 5th Nov 2011)

National Committee on Vital and Health Statistics Web site (2006). Personal health records and personal health record systems: A report and recommendations. Washington: Department of Health and Human Services. http://www.ncvhs.hhs.gov/0602nhiirpt.pdf. (Accessed 6th November 2011)

Sahai, A. and Waters, B. (2005), “Fuzzy identity-based encryption”, *In Advances in Cryptology, EUROCRYPT*, pages 457-473, 2005.

Sandhu, R., Coyne, E., Feinstein, H. and Youman, C. (1996), “Role-based access control models”, *IEEE Computer*, 29 (2):38-47, 1996.

Simons, W.W., Mandl, K. D. and Kohane, I. S. (2005), “The PING Personally Controlled Medical Record System”, Technical architecture. *Journal of the American Medical Informatics Association.* 12(1):263-268.

Szolovits, P., Doyle, J., Long, W. J., Kohane, I. and Pauker, S. G. (1994), “Guardian angel: Patient-centered health information systems”, Technical report, 1994.

Waters, B. (2008), “Ciphertext-policy attribute based encryption: An expressive, efficient, and provably secure realization”, *Cryptology ePrint Archive*, Report 2008/290.

Yang, N., Barringer, H. and Zhang, N. (2007), “A purpose based access control model”, *In Proc. of 3rd International Symposium on Information Assurance and Security (IAS)*, pages 143–148.

Yu, S., Ren, K. and Lou, W. (2008), “Attribute-Based Content Distribution with Hidden Policy”, *In Proc. Of NPSEC’08*, Orlando, Florida, USA, 2008.