Privacy Enhanced Group Communication in Clinical Environment

Mingyan Li[a], Sreeram Narayanan[b] and Radha Poovendran[a]

[a] Department of Electrical Engineering, University of Washington, Seattle, WA 98195.
[b] Department of Radiation Oncology, University of Washington, Seattle, WA 98195.

ABSTRACT

Privacy protection of medical records has always been an important issue and is mandated by the recent Health Insurance Portability and Accountability Act (HIPAA) standards. In this paper, we propose security architectures for a tele-referring system that allows electronic group communication among professionals for better quality treatments, while protecting patient privacy against unauthorized access. Although DICOM defines the much-needed guidelines for confidentiality of medical data during transmission, there is no provision in the existing medical security systems to guarantee patient privacy once the data has been received. In our design, we address this issue by enabling tracing back to the recipient whose received data is disclosed to outsiders, using watermarking technique. We present security architecture design of a tele-referring system using a distributed approach and a centralized web-based approach. The resulting tele-referring system (i) provides confidentiality during the transmission and ensures integrity and authenticity of the received data, (ii) allows tracing of the recipient who has either distributed the data to outsiders or whose system has been compromised, (iii) provides proof of receipt or origin, and (iv) can be easy to use and low-cost to employ in clinical environment.

Keywords: HIPAA, Security, Privacy, Confidentiality, Tracing, Group communication, Watermarking, Web application, Medical imaging

1. INTRODUCTION

Advances in computer systems and network technologies facilitate communication between health care professionals, and expedite high-quality treatments. At the same time, patient information can often be easily accessible and transmitted over an unprotected channel. This poses a great challenge for security and privacy protection of patients' records.

As the privacy protection of medical records is mandated by the recent Health Insurance Portability and Accountability Act (HIPAA),[1] research efforts[2,3,4] have been made to meet the HIPAA standards, which require the healthcare providers and professionals to ensure confidentiality, integrity and authenticity of the patient information. However, current security measures focus on the confidentiality of data in storage and during transmission only, before the data is accessed by authorized recipients.[5] The privacy of patient data can be breached by a recipient delivering the medical records to unauthorized parties. At present, the Digital Imaging and Communication in Medicine (DICOM)[2] standard does not address the issue of the privacy protection of patient data after the reception of the data. To enhance the patient's privacy at the recipients' end, we have proposed to enable tracing medical records by using watermarking techniques.[5]

In this paper, we design a tele-referring system that ensures the security and privacy of patient data *before and after* the data is accessed by an intended recipient, in an electronic group communication environment. Figure 1 illustrates a typical treatment scenario that is considered. After a patient visits his/her primary physician, the physician forms a team of physicians to collaborate on the patients case. Together they constitute a referrer group that implements the referring procedure as follows. The primary physician retrieves the patient's related Electronic Health Record (EHR) from a database, including images, and transmits EHR to other physicians for diagnosis reports. Each physician writes his/her comments in a report and broadcasts the report to the entire group. On the receipt of all the reports, the primary physician will finalize the treatment for the patient.

Corresponding author: Professor Radha Poovendran
E-mail: myli, radha@ee.washington.edu, sram@u.washignton.edu.

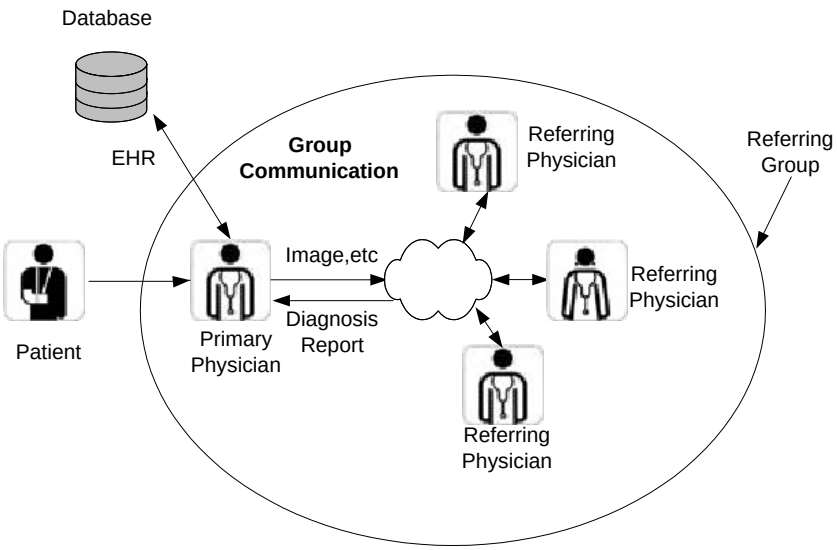

Figure 1. A group communication scenario in clinical environment

Security threats that breach the privacy of patients' records range from passive eavesdropping to malicious attacks. Contrary to the belief that most of security breaches are due to external intruders, most security threats occur from inside due to "accidental disclosure, insider curiosity, and insider subornation (releasing health information to outsiders for revenge, spite, or profit)".[6] The following scenarios are a few examples to demonstrate how easily the patients' privacy can be compromised.

Example 1: Physician A sends referring physician B a patient's information and medical images by email without encryption. An eavesdropper can tap into the message and obtain the patient's record.

Example 2: Physician A belongs to more than one referrer groups. The physician accidently forwards patient information from one group to another unintended group.

Example 3: Physician B denies reception of a patient's records from physician A, and physician A has no proof that physician B received the records. Then physician B is exempted from the responsibility of keeping the patients' records private.

Education alone is insufficient to prevent violation of privacy, and adequate security measures to enforce it are needed.[6] Hence, a tele-referring system that facilitates physician referring procedure and automates security safeguard against privacy disclosure is needed. In this paper, we present our security architecture design for the tele-referring system that incorporates safeguards against internal users from leaking privacy information accidentally or intentionally.

Compared to the state of the art medical security systems,[34] we introduce two new features into our architecture design: (i) privacy protection after the reception of patients' data is enhanced by enabling tracing to the recipient whose received data are leaked to unintended recipients, using watermark technique; (ii) multicast communication mode is proposed in our distributed architecture design. In contrast to unicast employed by most medical security systems, multicast mode reduces a sender's computation and saves the network resources.

The structure of the rest of the paper is as follows. Section 2 defines design goals, including all the security properties we aim to achieve in our design. In Section 3, we propose two designs of the tele-referring system: a distributed approach and a centralized approach, and discuss how security properties are satisfied. We finally conclude our paper in Section 4.

2. DESIGN GOALS

To protect patients' privacy during and after the transmission of medical data with minimal overhead, we need to ensure the following properties in our tele-referring system:

- **Confidentiality** is the ability of preventing anyone but intended medical professionals from reading the transmitted patients' data. Confidentiality is often enforced by encryption. Using encryption, the scenario described in Example 1 can be avoided.
- **Authentication** is to ensure medical records are originated from the correct sources to the claimed receivers. Authentication is of special importance since confidentiality cannot be guaranteed without first verifying who is at the other end of a communication channel.
- **Message Integrity** is an assurance given to recipient that the patients' data has not been changed by unauthorized parties.
- **Non-repudiation** is the ability of a recipient (sender) proves to the Trust Third Party (TTP) that the sender (recipient, respectively) did send (receive) the message earlier, the evidence used is called proof of transmission (reception). The proof of reception serves as a solution to the scenario described in Example 3.
- **Tracing** is the ability of tracking the authorized recipient who either distributed the data outside of the intended group or whose system has been compromised. Incorporating this property into system provides a deterrent to preclude the scenario in Example 2 from happening.
- **Audit Log** is the ability of recording events, such as EHR access and modification, which can be used as security evidence or for system usage statistics.
- **Service Availability** is the reassurance that service is available and medical records are accessible upon requested by authorized users.
- **Efficient** in terms of communication cost, computation complexity and storage. This leads to timely health care delivery and efficient utilization of user and network resources.
- **Easy to operate**. Additional operations required from medical professionals should be minimal, ideally, all the security functions being transparent to users.
- **Easy to deploy**. This ensures low-cost installation.

3. ARCHITECTURE DESIGN: A DISTRIBUTED APPROACH AND A CENTRALIZED APPROACH

We will present two security architecture designs: one is a distributed approach, in which a central server is required for the periodic key distribution and update, the other is a centralized web-based approach, in which a web server is required to be available all the time. For a better understanding of our designs, we will first introduce security primitives and define our notations.

3.1. Security primitives and notations

There are two classes of encryption algorithms: *symmetric* and *asymmetric* (public).[7] In symmetric key algorithms, both encryption and decryption keys are the same and should be kept secret. In a public key cryptosystem, such as RSA,[8] there is a key pair: public key and private key. The private key is held by a user secretly and the public key is published. The data encrypted by public key can be decrypted only by the one who holds the corresponding private key.

A cryptographic *hash* function $h(\cdot)$ is a one way function,[7] which is easy to compute in one direction, but its inverse is computationally intractable. A Message Authentication Code (MAC)[7] is a one-way hash computed from a message using a symmetric key, and it allows for message integrity check. A *digital signature*[7] is a public key based technique to ensure authenticity and message integrity of a message. A digital signature generated

by computing the hash value of a message and encrypting the hash using the private key of an entity. Given a message and a digital signature on the message, anyone can verify that the integrity of message is preserved and the message is from the claimed sender by using the public key of the sender.

We use K_A, K_A^{-1} to denote an asymmetric key pair, the public key, and the private key of entity A. $E_K(m)$ denotes the encryption of message m using key K, where the K can be a symmetric key or one entity's public key. $sig_{K_A^{-1}}m$ denotes the digital signature generated by A on message m, using its private key K_A^{-1}.

3.2. Architecture design: a distributed approach

For the distributed approach, we assume that everyone in the referring group has an asymmetric key pair with the certified public key published. In fact, DICOM requires that every communication entity has an asymmetric key pair.[2] Figure 2 illustrates the system architecture when using the distributed approach.

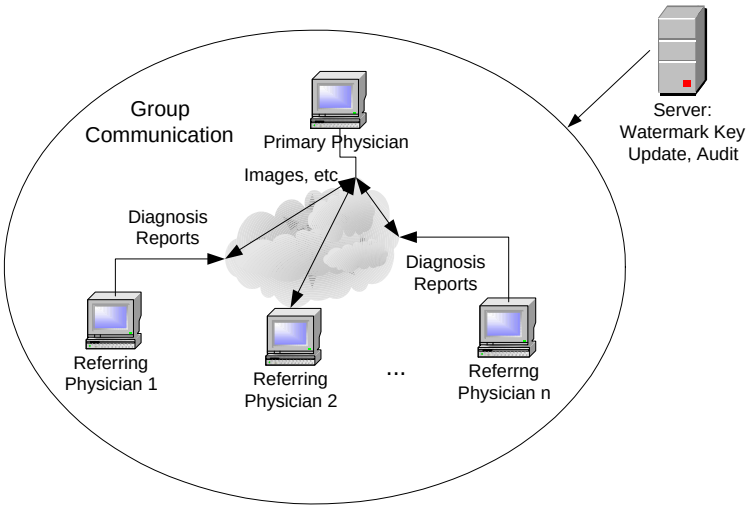

Figure 2. System architecture: the distributed approach

In the first stage, the primary physician sends the patient's medical images X to referring specialists. We use P to denote the communication node of primary physician. There are n referring specialists: $R_1, R_2, ..., R_n$, $R = \{R_1, R_2, ..., R_k\}$ denotes all the specialists, and R_* denotes any one of them.

Stage 1: Transmission of a patient' medical record X.

Step 1: P chooses a symmetric session key SK, encrypts the patient's medical record X, multicasts the encrypted message $C = E_{SK}(X)$, along with its digital signature $sig_{K_P^{-1}}(C)$.

$P \rightarrow R$: $E_{SK}(X)$, and $sig_{K_P^{-1}}(C)$, where $C = E_{SK}(X)$.

Step 2: On the receipt of C, recipient R_* computes its signature on H and sends it to the sender P.

$R_* \rightarrow P$: $sig_{K_{R_*}^{-1}}(C)$.

Step 3: On the receipt of the signature of recipient R_* on C, P sends R_* the session key SK encrypted using the public key of R_*, so R_* can decrypt SK and the patients' record X from C.

$P \rightarrow R_*$: $E_{K_{R_*}}(SK)$.

In the second stage, a referring physician finishes his/her diagnosis report F and broadcasts it to the rest of the group for review.

Stage 2: Transmission of a diagnosis report F.

R_* encrypts the report with the session key SK, signs on the encrypted report, and broadcasts it to the rest of the group.

$R_* \rightarrow P$ and all other referrers as: $E_{SK}(F)$, $sig_{K_{R_*}^{-1}}(E_{SK}(F))$.

We note that the report from each physician is saved in a separate file. If multiple medical professionals are allowed work on a single file, then the comments made by one physician are subject to undetectable illegal modification and deletion by others.

Now we discuss how the security requirements listed in Section 2 are fulfilled.

3.2.1. Achieving confidentiality, authentication and message integrity

The session key SK is encrypted using each intended recipient's public key, so that only the authorized recipient can decrypt the key SK. Since the medical record X and the report F are encrypted using the key SK, the confidentiality of X and F is ensured. In both transmissions of the medical record and a diagnosis report, the encrypted message is broadcast along with the digital signature using sender's private key, and thus the integrity and authenticity of the message can be verified by using the public key of the sender.

Instead of using recipients' public keys, the medical record X in Step 1 is encrypted with the session key SK to: (i) reduce the computation of P and the length of the message by a factor of n, (ii) enable multicast communication mode, in which identical data is transmitted to multiple recipients, to reduce network bandwidth consumption, and (iii) provide proofs of reception. If the message X is encrypted using a recipient's public key, then the primary physician gives decodable messages in the first place and may not be able to collect proofs of reception.

3.2.2. Achieving non-repudiation

The $sig_{K_P^{-1}}(C)$ in Step 1 serves the proof of transmission at the recipient end, and $sig_{K_{R_i}}\{C\}$ for $i = 1, .., n$ in Step 2 are the proofs of receipt held by the sender P. There is, however, one potential problem with using $sig_{K_{R_*}^{-1}}(C)$ as the receipt. If the encrypted key in Step 3 is lost, then the sender has the proof from Step 2, but the recipient does not actually receive the key to decrypt and obtain the record X. In this case, the recipient will request retransmission, otherwise the encrypted medical data C is of no use to it. If it does not request for retransmission after some time, we can safely assume that it gets the encrypted session key, and $sig_{K_{R_*}^{-1}}(C)$ can always be used as the proof of reception of the encrypted X.

3.2.3. Tracing medical images

Encryption can only present external access to the patients' records being transmitted, but offers no privacy protection after a recipient has received data. The violation of patient privacy by a recipient can happen due to, for example, accidental disclosure, and system compromise under attack. To provide a deterrent to preclude an individual from being careless or even attempting the privacy breach by leaking medical images to unauthorized users, we enable tracing in our system by using watermarking. Watermarking[9] is a technique to embed identification codes, called watermarks, into media in form of text, image, audio, video data. When used for tracing purposes, a unique watermark per user is required.

It is a challenging problem to enable tracing while utilizing multicast communication in which identical data is delivered to multiple recipients, since unique watermarked copy for each recipient is required for tracing purpose. Recently, we proposed an efficient solution[10] as illustrated in Figure 3. We assume that each user in the group is assigned a *watermark key* for watermarks embedding and decoding. Our main idea is to embed an original image X from the primary physician with a strong watermark, so the resulting "noisy" image X' cannot be diagnosed directly. The medical record transmission protocol is executed to multicast the encrypted X', i.e., $E_{SK}(X')$ to the group. A recipient first decrypts X'. To achieve diagnostic value of the image, a recipient has to eliminate part of the watermark using its pre-assigned watermark key. This process ensures the watermark of the recipient will be imprinted into the image. Therefore, the usable image $\bar{X}$ obtained by each recipient is a unique watermarked copy. The solution requires a central server in charge of watermark key distribution and update.

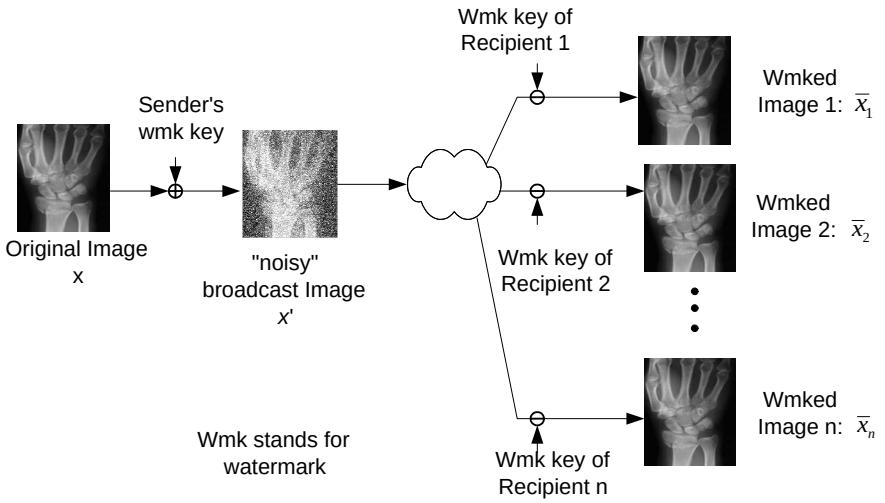

Figure 3. A multicast watermarking model with one sender and n recipients

3.2.4. Ensuring log and service availability

Audit log is a critical component in medical information system for security and privacy check. But in a distributed system, it is challenging to maintain logs from all the distributed nodes in a timely and secure fashion. A distributed architecture provides better service availability since it does not heavily depend on a server for a service, and hence suffers less from a single point failure than a centralized architecture.

3.3. Architecture design: a centralized approach

Although the distributed approach does not require the server to be on-line most of the time, a certified private and public key pair has to be assigned for each participating physician to ensure authentication. Additionally, special software has to be installed in the physicians' terminal to make all the encryption/decryption and watermarking/decoding transparent to the physicians. However, using a centralized architecture, most of the processes are performed by a server and the only software required for each physician's terminal is a standard Internet browser. Therefore, the centralized web-based approach is easy to implement and deploy. Now we describe our centralized web-based architecture design of the tele-referring system.

3.3.1. System architecture

The web-based tele-referring system aims to provide a web site where a team of medical professional can securely access a patient's medical record and collaborate on the treatment: the primary physician can deposit EHR of a patient, including medical images, assign referring specialists, and read diagnostic reports from referring physicians; and referring physicians can login, retrieve the medical images, and write the diagnosis. The system structure and data flow are shown in Figure 4. A web server provides services including user authentication, events auditing, data retrieval and display. A database is used to store the medical images and reports, account management information, and watermarks for tracing. The web server also communicates with Simple Mail Transport Protocol (SMTP) server, as emails are used to notify the physicians when there is a patient's case or when a diagnosis report is completed.

3.3.2. Functions performed by a primary physician and a referring physician

In the web-based tele-referring system, there are three functional roles based on the trust level: an administrator, a group initiator (corresponding to a primary physician) and group members (corresponding to referring specialists).

In addition to the functions performed by a group initiator and group members, an administer can perform the following additional functions: configure the tele-referring system, access and modify the database, disable a

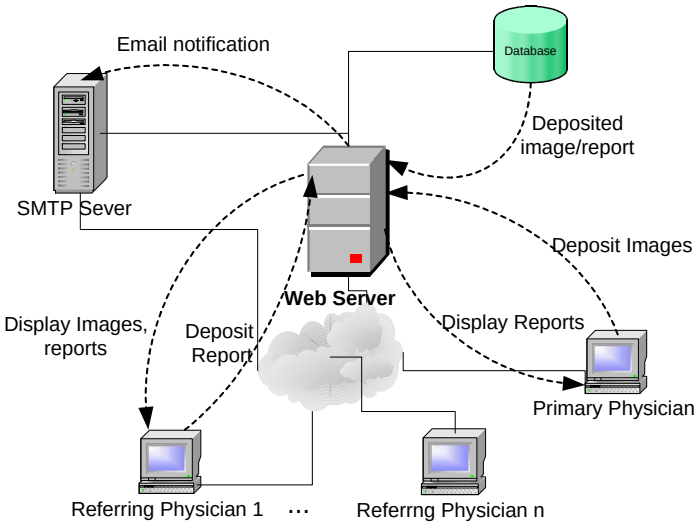

Figure 4. System architecture and data flow: the centralized approach. The solid line indicate network infrastructure and the thick dotted line indicate data flow.

group initiator and delete a group. Since an administrator has the highest level of trust, number of people who can access as an administrator should be highly limited. The primary physician as the group initiator is allowed to perform the following tasks:

- create a new group
  - name the group
  - deposit EHR of a patient
  - add referring physicians: email addresses, initial passwords
- view the list of groups where he/she is the group initiator
- manage the existing groups where he/she is the group initiator
  - view the list of group members
  - membership management
    - view the profile of a group member
    - add a group member
    - delete a group member
  - view all the reports from group members
  - search the report from a particular member
  - send reminders

A referring physician as a group member has the ability to perform the following

- edit his/her profile
- change his/her password
- view the list of groups that he/she belongs to
- post a report for a group he/she belongs to
- view all the posted reports for a group he/she belongs to

We now describe how security features defined in Section 2 are achieved.

3.3.3. Achieving confidentiality during transit and in storage

Secure Socket Layer (SSL) is the standard protocol to secure the communication[11] between client browsers and the web server. It requires a server authentication certificate, which contains certified public key for the server, to be installed on the web server. SSL establishes a symmetric session key during the handshaking, and uses the session key to encrypt the subsequent messages. In our tele-referring system, all the medical images and diagnosis reports are sensitive data and their transmission should be protected using SSL. This implies client browsers can only access the web via HyperText Transport Protocol (Secure) (HTTPS), which is actually HTTP over SSL. Communication between the web server and the database should be conducted using a private channel. In practice, Internet Protocol Security (IPSec) can be used to ensure the confidentiality between the servers.[12] To prevent external, unauthorized access to the database and the web server from the Internet, a firewall should be installed to separate the servers from the Internet and filter incoming/outgoing messages.

We require that the web server and the database are physically tamper resistant. To safeguard against the compromise of data confidentiality in storage due to theft, the data is avoided being stored in cleartext whenever it is possible.[4] When only the verification of data is needed, such as password verification, the hash of data is stored in the database. Furthermore, access control is enforced to protect confidentiality. Whenever a medical record is retrieved, the server should authenticate the user, check his/her access right based on the group ID (which group he/she belongs to) and role of the user (a primary physician or a referring physician).

3.3.4. Achieving authentication and message integrity

We employ password-based user authentication, which allows a physician the freedom to connect to the tele-referring site from a machine that has no specific configuration information of the physician. Since the efficiency of password-based authentication in thwarting unauthorized access depends on the quality of passwords selected and the frequency of the passwords being changed,[13] the physicians should choose strong passwords that are hard to guess or uncover by brute force search. To prevent an adversary from trying passwords on-line, a lockout is utilized after a certain number of login failures, and at the same time an audit message is generated. Message integrity is guaranteed by SSL using MAC.

3.3.5. Ensuring non-repudiation and auditing log

Requests to the servers need to be kept track of by generating audit message. An audit message contains the time, the username, the content, the IP address of the request. The log serves as the proofs to address the non-repudiation threat of users denying their actions. Regular analysis of the audit logging can help to predict an attack in advance and prove the suspicious actions of users, and hence constitutes an important part to ensure the proper operation of the entire system. Access control to log files need to be enforced, and file backup need to be performed regularly. Since the only legitimate access point to the tele-referring service from Internet is through the web server in the centralized approach, it is easier to log activities than in the distributed approach, where secure transmission of log files from distributed nodes to a server and time synchronization are major implementation issues.

3.3.6. Tracing medical images

To enable tracing medical images for enhanced privacy protection, a watermark is generated and assigned to each user per group. Because the information related to a watermark can be leaked with repeated use over many images, watermarks need to be updated periodically. The system stores all the watermarks and their effective periods in a database, in order to trace the authorized user whose received medical image is found outside of the intended group.

3.3.7. Ensuring service availability

The service availability of the web-based tele-referring system implies the availability of the web server and the database. A backup server and a duplicate database are required to protect the system from single point failure. Additional care has to be taken to ensure the security of the backup server and the duplicate database.

4. CONCLUSIONS

None of current medical security systems have addressed the patient privacy issue after the data has been accessed by an authorized recipient. In our design of a tele-referring system, we enable tracing medical images by using watermarks, to enhance the patient's privacy at the recipient end. We have proposed two different security architecture designs of the tele-referring system: a distributed approach and a centralized web-based approach, and demonstrate how these two designs can fulfill the security goals. Although the distributed approach has the advantage of not requiring a trusted server to be on-line all the time, it is easier to monitor and log the system events using the centralized approach, as the web server serves as the centralized gatekeeper. The centralized web-based approach also simplifies the deployment on the client side, since neither a special software (but an Internet browser) nor a private/public key pair is required on a client. The prototype implementation of the centralized system design is left as future work.

REFERENCES

1. United Stated Department of Health & Human Services, "HIPAA: medical privacy - national standards to protect the privacy of personal health information," *[Online], Available: http://www.hhs.gov/ocr/hipaa/* .
2. HEMA, "DICOM: digital imaging and communication in medicine," *[Online], Available:http://medical.nema.org/* .
3. F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a hipaa mandated pacs environment," *Computerized Medical Imaging and Graphics* **27**, pp. 185–196, 2003.
4. D. Slik, M. montour, and T. Altman, "A comprehensive security framework for the communication and storage of medical images," in *Medical imaging 2003: PACS and integreated medical information systems, proceddings of SPIE*, **5033**, pp. 212–223, 2003.
5. M. Li, S. Narayanan, and R. Poovendran, "Tracing medical images using multi-band watermarks," in *Proceedings of the 26th IEEE Engineering Medicine Biology Conference (EMBC)*, (San Francisco, CA), Sept. 2004.
6. T. Huston, "Security issues for implementation of e-medical records," *Communications of the ACM* **44**(9), pp. 89–94, 2001.
7. C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*, Prentice Hall PTR, 2nd ed., 2002.
8. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptogsystems," *Communications of the ACM* **21**(2), pp. 120–126, 1978.
9. H. M. Chao, C. M. Hsu, and S. G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedicine* **6**(1), pp. 46–53, 2002.
10. M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," under review, 2005.
11. *Building secure microsoft ASP.NET applications: authentication, authorization, and secure communication; patterns and practices*, Microsoft Press, 2003.
12. F. Swiderski and W. Snyder, *Threat modeling*, Microsoft Press, 2004.
13. L. Ravera, I. Colombo, M. Tedeschi, and A. Ravera, "Security and privacy at the private multispecialty hospital istituto clinico humanitas: strategy and reality," *International Journal of Medical Informatics* **73**(3), pp. 321–324, 2004.