Journal of King Saud University – Computer and Information Sciences (2014) **26**, 170–180

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations

Sangram Ray [*], **G.P. Biswas**

Department of Computer Science & Engineering, Indian School of Mines, Dhanbad 826004, India

Received 12 February 2013; revised 17 May 2013; accepted 2 October 2013
Available online 9 October 2013

KEYWORDS

Health Insurance Portability and Accountability Act (HIPAA);
Certificate Authority (CA);
Protected health information (PHI);
E-health security;
Medical center server (MCS);
Public key infrastructure (PKI)

Abstract The Health Insurance Portability and Accountability Act (HIPAA) passed by the US Congress establishes a number of privacy/security regulations for e-healthcare systems. These regulations support patients' medical privacy and secure exchange of PHI (protected health information) among medical practitioners. Three existing HIPAA-based schemes have been studied but appear to be ineffective as patients' PHI is stored in smartcards. Moreover, carrying a smartcard during a treatment session and accessing PHI from different locations results in restrictions. In addition, authentication of the smartcard presenter would not be possible if the PIN is compromised. In this context, we propose an MCS (medical center server) should be located at each hospital and accessed via the Internet for secure handling of patients' PHI. All entities of the proposed e-health system register online with the MCS, and each entity negotiates a contributory registration key, where public-key certificates issued and maintained by CAs are used for authentication. Prior to a treatment session, a doctor negotiates a secret session key with MCS and uploads/retrieves patients' PHI securely. The proposed scheme has five phases, which have been implemented in a secure manner for supporting HIPAA privacy/security regulations. Finally, the security aspects, computation and communication costs of the scheme are analyzed and compared with existing methods that display satisfactory performance.

1. Introduction

E-healthcare is an online approach that includes patient treatment, generation of diagnostic reports (PHI), secure storage and access to PHI data such that only authenticated entities can retrieve and update the data through the Internet. The medical practitioners generally retrieve old PHI data during a new treatment session, and the currently generated PHI is restored and updated with new medical information (Aljumah et al., 2013; El-Sappagh and El-Masri, 2013). The protection of patients' privacy is also considered in an e-health system. However, the deployment of an e-health system fulfilling all these requirements is a challenging job. Several bills by different health agencies and authorities have been proposed, and HIPAA (Health Insurance Portability and Accountability Act) (Collmann et al., 2004; HIPAA, 1996a,b; Yanga et al., 2006) was voted into federal law by the United States Congress

[*] Corresponding author. Mobile: +91 8797369171.
E-mail addresses: sangram.ism@gmail.com (S. Ray), gpbiswas@gmail.com (G.P. Biswas).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

1319-1578 © 2013 Production and hosting by Elsevier B.V. on behalf of King Saud University.
http://dx.doi.org/10.1016/j.jksuci.2013.10.001

in 1996 for the US healthcare industry. In fact, HIPAA mentions a set of conceptual guidelines to be strictly maintained and followed by all healthcare organizations for improving healthcare services, including qualities and overall efficiency of an e-health system. In addition, HIPAA highlights patients' privacy (Federal Register, 2002; Huanga et al., 2009; Jin et al., 2011) and provides direction to other countries considering HIPAA guidelines along with their respective domestic laws. Although this direction can help facilitate the initiation of other countries deploying e-health systems, no specific procedures in HIPAA are provided for maintaining patients' privacy and security regulations.

The detailed specifications of HIPAA are available in Collmann et al. (2004), HIPAA (1996a,b) and Yanga et al. (2006). These specifications have been summarized and used in many e-healthcare schemes (Hu et al., 2010; Huang and Liu, 2011; Lee and Lee, 2008; Lee et al., 2011; Li et al., 2008). For the sake of clarity, the summarized outcome requirements of HIPAA in regard to privacy and security regulations (Hu et al., 2010; Huang and Liu, 2011; Lee and Lee, 2008), which have also been used in our e-health scheme, are briefly stated below.

1.1. Privacy regulations

Privacy regulations (Hu et al., 2010; Huang and Liu, 2011; Lee and Lee, 2008) define a patient's right to understand and control the use/disclosure of his PHI, comprising the patient's name, address, contact number and medical records.

1.2. Security regulations

The security regulations of HIPAA (Hu et al., 2010; Huang and Liu, 2011; Lee and Lee, 2008), which mainly consist of five terms, are as follows:

(1) *Patients' understanding*: The patients' right to understand how their PHI will be used and kept must be maintained.
(2) *Confidentiality*: Various software safeguards such as encryption and decryption authentication are described to protect health data during storage and transmission.
(3) *Patients' control*: Patients must have control in accessing and using their PHI data.
(4) *Data integrity*: Patients' electronic health information should be protected from medical omissions, tampering and unauthorized destruction.
(5) *Consent exception*: In life-saving and other exceptional situations, access to PHI without patient's authorization is allowed.

A HIPAA based e-health system was initially proposed by Lee and Lee (2008), which was followed by Hu et al. (2010) and Huang and Liu (2011). We studied these proposals thoroughly and will now present their outcomes. In 2008, Lee and Lee (2008) proposed a health data card-based e-healthcare scheme, where a smart card is used by a patient for secure storing and/or retrieving of PHI during a treatment session. A symmetric encryption-decryption with a session key generated with the healthcare provider is used for confidentiality of the PHI data. Thus, it becomes a session-based e-health scheme, which means that each patient come in direct contact with medical staff during a treatment session and produces his smart card for accessing/updating PHI data. This creates certain limitations such as PHI is available only when both patient and the smart card are physically present at the healthcare provider, and hence, it is not possible to access the smartcard from a distant location through the Internet. In addition, the multiple accessing of a patient's PHI may not be feasible simultaneously, such as when different expert opinions are needed and for pathological tests and analyses. The smartcard-based approach also adds additional overhead if the laboratories for different medical test-sample analyses are located in a wide geographical distribution. Finally, a security flaw may exist in a smart card with a PIN-based system, where instead of the owner, the presenter of the smartcard is authenticated if the PIN is compromised.

Some contract-based e-health systems are also available in literatures (Agrawal et al., 2005; Agrawal and Johnson, 2006; Bhatti et al., 2007; Hu and Han, 2009; Lambrinoudakis and Gritzalis, 2000; May, 1998; Yu et al., 2006), where patient's PHI is entirely left to a medical service provider (MSP) for storage. In these systems, a patient signs for a fixed contract-period with the MSP, and any medical staff can access the same during this contract period. However, it may be noted that every access to the patient's PHI is controlled and protected by the MSP. An existing contract-oriented e-health system based on HIPAA privacy/security regulations is described now.

In 2010, Hu et al. proposed an e-health system for HIPAA privacy and security regulations where a hybrid security scheme based on public key infrastructure (PKI) and a Medicare smartcard is used. In this scheme, a patient initially collects his smartcard from a smartcard trust center (STC) and uses the same card for signing a contract with an MCS (medical center server) for certain duration. The smartcard, which contains the patient's information and valid public–private key pair collected from the patient's PKI digital certificate, is used for authenticated negotiation of a contract key with the MCS. The patient's PHI is stored in the MCS in plaintext form, and medical staff, without prior consent of the patient, can access the PHI data securely. On request, the MCS sends both contract key and PHI data to medical staff, where the contract key and the PHI are encrypted by the public-key of the medical staff and contract key of the patient, respectively. After completion of the contract period, the PHI data are finally deleted from MCS. This scheme has certain limitations as described now. First of all, it violates the HIPAA privacy/security regulations as no patient-consent during storage/retrieval of PHI to/from MCS is required. As the patient's PHI is only kept in the MCS and deleted after the contract period, the patient has no way to acquire a copy of his/her PHI for subsequent treatment processes. Moreover, this scheme does not account for legal requirements involved with patient's consent exception cases. Therefore, if an emergency situation exists, it cannot be handled without legal complications.

Similar to Lee and Lee's scheme (2008), an e-health scheme based on a smart card to satisfy HIPAA privacy and security regulations is proposed by Huang and Liu (2011). In this scheme, elliptic curve cryptography (ECC) is used for different security operations such as password protection/update, signature generation for signing contract agreement and verification and encryption-decryption of

PHI data. One of the advantages over Lee and Lee's scheme (2008) is that for comparable security it requires, ECC being an additive group method, a smaller key length than the key-size required in multiplicative group based-PKI (Koblitz, 1987; Miller, 1985). As a result, the computation-communication costs for registration, signature generation-verification, encryption-decryption processes and storage requirements are significantly reduced. In addition, the scheme has a provision for allowing patients to freely choose and update their passwords. However, this scheme, because of the use of a smartcard, also possesses all the aforementioned limitations in the analysis of the Lee and Lee's scheme (2008). The Huang and Liu scheme also has the limitations associated with supporting session-based e-health services as discussed in the earlier analysis that revealed that a contract-oriented e-health scheme is better than a session-based system (Agrawal et al., 2005; Agrawal and Johnson, 2006; Bhatti et al., 2007; Hu and Han, 2009; Lambrinoudakis and Gritzalis, 2000; May, 1998; Yu et al., 2006).

This paper addresses all these issues and presents a unified e-health system for HIPAA privacy and security regulations that not only incorporates all the merits of the different schemes analyzed but also uses existing PKI for efficient implementation and use. Our e-healthcare scheme is a contract-oriented scheme that allows a patient to sign a contract and register with an MCS, where a CA-based digital certificate is used for initial authentication. Similarly, each medical staff registers with the MCS and negotiates (including patients) a contributory registration key with the MCS. This key is used for subsequent authentication and negotiation of a session key prior to each new treatment session. In this scheme, instead of a smartcard, the MCS connected through the Internet is used for secure storage/retrieval of PHI, where symmetric encryption based on a session key is used. At the end of the contract period, a copy of PHI is securely sent to a patient; however, the PHI is never deleted from the MCS. In addition, our scheme allows for a patient to extend the current contract period or re-register with the MCS, especially when the previous registration key is compromised. The main contributions of this work are as follows. (1) It supports a contract-oriented approach and uses an MCS for PHI data storage, which thus avoids all drawbacks that exist in session- and smartcard-based systems. (2) All entities initially follow CA-based authentication for registration with the MCS; however, a negotiated session key is used for subsequent authentication and securing different operations required in the proposed e-health system. The system thus avoids additional overhead involved in maintaining and processing of the CA-based certificate. (3) As PHI is loaded into the MCS system, any actor with prior registration to the MCS can access patients' PHI data over the Internet from any geographical locations. (4) Finally, a patient receives updated PHI data at the end of his/her contract period.

The remaining parts of this paper are organized as follows. Section 2 provides the proposed CA-based e-health system, where each of the six phases is described with flow diagrams and algorithmic steps. As a performance study, the fulfillment of HIPAA security and privacy regulations, implementation feasibility and applications and comparisons in terms of some characteristic features with three existing schemes are presented in Section 3. Finally, Section 4 concludes the paper.

2. Proposed CA-based e-health system

In this section, an e-health system for satisfying HIPAA privacy/security regulations is presented. It uses existing PKI, in which a CA acts as a trusted agency to issue public-key certificates for verification and validation of a user's public key (Elgamal, 1985; Levi et al., 2004; NIST, 2001; Stallings, 2009; Weise, 2001). The PKI is a hierarchical tree structure of CAs with a root CA that creates, distributes, verifies and revokes users' public-key certificates based on the X.509 standard (Elgamal, 1985; Levi et al., 2004; NIST, 2001; Stallings, 2009; Weise, 2001). In fact, a public-key certificate combines a user's identity with a public key, and thus, users, upon exchange of their certificates among themselves, become authenticated to each other and receive authenticated public keys as well.

In our system, all patients, doctors and other medical staff obtain their public-key certificates from a CA. A patient, who wishes to use an e-healthcare service, must register with a medical center server (MCS). Similarly, the doctors and other medical staff are also registered with the MCS, which contains all healthcare information, including the patient's PHI. The patient's PHI generated after the completion of a treatment session is uploaded to the MCS, and a copy of the same is securely sent to the patient. The patient's PHI stored in the MCS is accessible online and if necessary, any foreign MCS (FMCS) can access PHI with prior registration with the MCS. However, for authentication, each FMCS must receive a certificate from a CA for validation of its public key. The details of our proposed scheme are given below, and the following common notations are used:

$h(\_)$	a secure one-way hash function (e.g., SHA1, MD5, etc.)
E	encryption
D	decryption
P	patient
MCS	medical center server
$\mathrm{ID_P}$	identity of a patient
$\mathrm{ID_{DOC}}$	identity of a doctor
$\mathrm{R_{MCS}}$	a random challenge generated by the MCS
$\mathrm{U_{MCS}}$	another random challenge generated by the MCS
$K_{\mathrm{REG_P}}$	registration key of a patient
$K_{\mathrm{REG_D}}$	registration key of a doctor
K_S	a random secret session key generated by a doctor
$\mathrm{CA_P}$	public key certificate of a patient
$\mathrm{CA_{DOC}}$	public key certificate of a doctor
$\mathrm{CA_{MCS}}$	public key certificate of MCS
$(\mathrm{PR_P}, \mathrm{PU_P})$	patient's private/public key pair
$(\mathrm{PR_{DOC},} \mathrm{PU_{DOC}})$	doctor's private/public key pair
$(\mathrm{PR_{MCS},} \mathrm{PU_{MCS}})$	MCS's private/public key pair

The proposed CA-based scheme consists of six phases, namely registration, PHI generation, PHI upload, PHI retrieval, handling emergency situations and foreign access, each of which is addressed below.

2.1. Registration phase

As stated earlier, the proposed e-health system requires registration with an MCS for all patients and medical staff, including doctors, and in this section, the proposed registration procedure for a patient is discussed. The validity of the registration depends on the signed agreement w, sent by the patient. Any medical staff that are directly/indirectly involved must follow the same registration procedure for MCS registration. The registration procedure comprises the four messages given in Fig. 1, which are described below.

***Step* 1:** Patient → MCS: $\mathrm{ID_P}$, *Signed agreement w*, $\mathrm{CA_P}$
Patient initially sends a *registration request* with his public key certificate, identity and a signed agreement w to the MCS. After receiving the request, the MCS validates the patient's certificate and retrieves the valid public key of the patient.

***Step* 2:** MCS → Patient: $E_{\mathrm{PU_P}}\ (R_{\mathrm{MCS}}),\ \mathrm{CA_{MCS}}$
In response to the patient's request, the MCS generates a random number R_{MCS} with k-bit security level, designated a challenge, to the patient and encrypts it using the patient's public key. The MCS then sends the encrypted message along with its public key certificate to the patient in message 2. Note that the public key certificates of the patient and MCS are exchanged for their authentication purposes as well as to obtain their valid public keys.

***Step* 3:** Patient → MCS: $E_{\mathrm{PU_{MCS}}}\ (R_{\mathrm{MCS}} \| g^{k_1})$
The patient validates the MCS's certificate and retrieves the valid public key of the MCS. Then, the patient decrypts the message sent by the MCS using his private key and correctly obtains the challenge R_{MCS}. The patient now selects a random number k_1 $(0 \leqslant k_1 \leqslant p-1)$ and calculates a public value g^{k_1} mod p, where p is a large prime number, and g is a generator of order $p-1$ in the group $< Z_p^*, \times >$, and both are public. Then, the patient concatenates R_{MCS} with g^{k_1}, encrypts the concatenated message using the public key of the MCS and finally sends the encrypted message to the MCS.

***Step* 4:** MCS → Patient: $w,\ E_{\mathrm{PU_P}}\ (R_{\mathrm{MCS}} \| g^{k_2}),\ E_{\mathrm{PR_{MCS}}}\ (h(w))$
After receiving the message, the MCS decrypts the message using its private key and extracts the challenge R_{MCS} and the public value g^{k_1}. Then, the MCS compares the received challenge with its own challenge, sent to the patient and if the comparison passes, it selects a random number k_2 $(0 \leqslant \mathrm{k}_2 \leqslant p-1)$ and calculates the corresponding pubic value g^{k_2} mod p in the same group. The MCS also generates the patient's registration key as $K_{\mathrm{REG_P}} = (g^{k_1})^{k_2} = g^{k_1 \cdot k_2}$ mod p and stores it in its database corresponding to the patient's identity. Then, the MCS concatenates its public value with the same challenge R_{MCS}, encrypts the concatenated message using the patient's public key and finally sends the encrypted message to the patient along with the agreement w and its signed copy $E_{\mathrm{PR_{MCS}}}\ (h(w))$ for integrity purposes.

After receiving the MCS's message, the patient decrypts the encrypted message using his private key and obtains the MCS's public value and R_{MCS}. He then compares the newly received R_{MCS} with the previously received R_{MCS} in message 2. If the comparison passes, the patient then calculates his registration key $K_{\mathrm{REG_P}} = (g^{k_2})^{k_1} = g^{k_1 \cdot k_2}$ mod p, which is same as the registration key obtained by MCS. To verify the integrity of the signed agreement w, the patient decrypts the signed message using the MCS's public key and obtains $h(w) = H$ (say). He then generates the hash digest of the publicly received w as $h(w) = H'$ (say) and checks H' = H? If he confirms the relationship, he saves the signed agreement and his registration key for future use.

2.2. PHI generation, upload and retrieval phases

PHI generation, along with its upload and retrieval procedures, is described in this section. In our proposed scheme, a patient physically visits a doctor whenever treatment is required, and then the doctor treats the patient and generates the patient's diagnosis data, designated PHI. The PHI consists of two categories, namely *text-data* and *image-data*. *Text-data* consists of sensitive textual data, including name, address and medical text results, among other data, and *image-data* consists of large-size medical images. In our scheme, the total PHI data are uploaded to the MCS by the doctor, and the patient only obtains a copy of his *PHI text-data* from the MCS to learn treatment results. The patient obtains only his

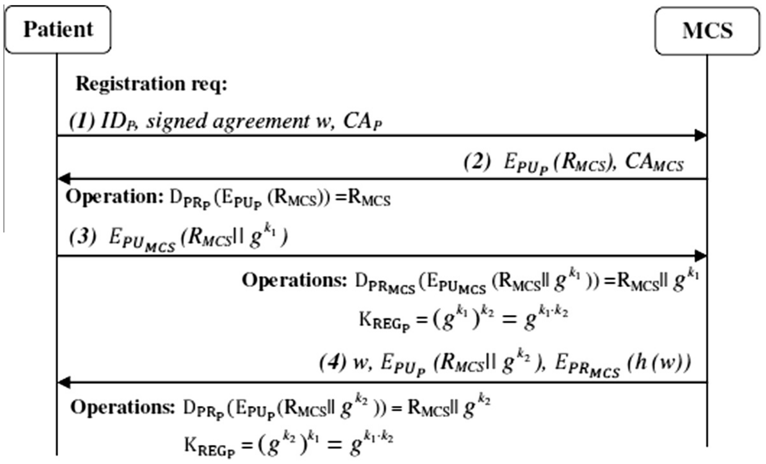
Patient
MCS
Registration req:
(1) ID_P, signed agreement w, CA_P
(2) $E_{PU_P}(R_{MCS}), CA_{MCS}$
Operation: $D_{PR_P}(E_{PU_P}(R_{MCS})) = R_{MCS}$
(3) $E_{PU_{MCS}}(R_{MCS} \| g^{k_1})$
Operations: $D_{PR_{MCS}}(E_{PU_{MCS}}(R_{MCS} \| g^{k_1})) = R_{MCS} \| g^{k_1}$
$K_{REG_P} = (g^{k_1})^{k_2} = g^{k_1 \cdot k_2}$
(4) $w, E_{PU_P}(R_{MCS} \| g^{k_2}), E_{PR_{MCS}}(h(w))$
Operations: $D_{PR_P}(E_{PU_P}(R_{MCS} \| g^{k_2})) = R_{MCS} \| g^{k_2}$
$K_{REG_P} = (g^{k_2})^{k_1} = g^{k_1 \cdot k_2}$

Figure 1 Registration protocol.

PHI text-data portion because it is of the smaller data size in comparison with *PHI image-data*. Thus, it is feasible to store the *text-data* in a patient's external drive.

To upload and retrieve a patient's PHI data from the MCS, i.e., prior to start of any treatment session, a doctor must negotiate a temporary secret session key with the MCS. The session key is temporary because it is deleted after completion of a treatment session, and a new session key is negotiated for a new treatment session. The generation of a secret session key, upload and retrieval of a patient's PHI in both normal and emergency conditions are described in the following subsections.

2.2.1. Secret session key negotiation procedure

In this subsection, the mutual authentication and secret session key negotiation procedure between a doctor and MCS is described. The detail key negotiation procedure, comprising three steps, is given in Fig. 2 and described below.

***Step* 1:** Doctor → MCS: $\mathrm{ID}_{\mathrm{DOC}}$, $E_{K_{\mathrm{REG_D}}}\ (K_S \| h(\mathrm{ID}_{\mathrm{DOC}}))$
The doctor randomly selects a secret number K_S, concatenates it with the calculated hash digest of his identity, encrypts the concatenated message using his registration key $K_{\mathrm{REG_D}}$, and then sends the encrypted message along with his identity $\mathrm{ID}_{\mathrm{DOC}}$ to MCS.
***Step* 2:** MCS → Doctor: $E_{K_S}\ (U_{\mathrm{MCS}})$
After receiving the message, the MCS obtains the doctor's registration key K_{REG_D} corresponding to the doctor's identity from its database, uses it to decrypt the message sent by doctor and obtains the secret number K_S and the hashed digest of doctor's identity $h(ID_{\mathrm{DOC}}) = H$ (say). For authentication, the MCS calculates the hash digest of the openly received doctor's identity as $h(ID_{\mathrm{DOC}}) = H'$ (say) and checks $H' = H$? If the result is true, the doctor is authenticated to the MCS, and the received random secret K_S becomes the secret session key for that session. For confirmation, the MCS generates a random challenge U_{MCS}, encrypts it using the secret session key K_S and sends to the doctor.
***Step* 3:** Doctor → MCS: $E_{\mathrm{PR_{DOC}}}\ (h(U_{\mathrm{MCS}}))$
In response to the MCS's challenge, the doctor decrypts the encrypted message using the secret session key K_S, receives the challenge U_{MCS}, signs on it using his private key and then sends it to the MCS.

If the challenge is answered, i.e., if the verification of the doctor's signature is successful, then the session between the doctor and MCS is established with session key K_S. Otherwise, the request is rejected.

Note that any doctor before attending a patient must negotiate a secret session key with the MCS using the above protocol, and at the end of the treatment procedure, the session key is deleted. After negotiating a session key, the doctor may retrieve/upload the patient's PHI both in normal and emergency circumstances from/to MCS, the details of which are addressed now.

2.2.2. PHI upload procedure

The patient's PHI upload procedure involves the exchanges of two messages – (1) from doctor to the MCS for uploading and (2) from the MCS to the patient when he wants to obtain a copy of his *PHI text-data*. The details of these exchanges are given in Fig. 3and explained below.

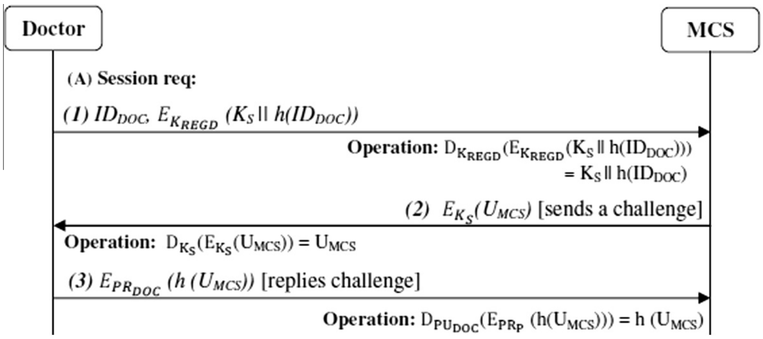
Doctor
MCS
(A) Session req:
(1) ID_{DOC}, $E_{K_{REGD}}$ (K_S || $h(ID_{DOC})$)
Operation: $D_{K_{REGD}}(E_{K_{REGD}}(K_S \| h(ID_{DOC})))$
$= K_S \| h(ID_{DOC})$
(2) $E_{K_S}(U_{MCS})$ [sends a challenge]
Operation: $D_{K_S}(E_{K_S}(U_{MCS})) = U_{MCS}$
(3) $E_{PR_{DOC}}$ $(h(U_{MCS}))$ [replies challenge]
Operation: $D_{PU_{DOC}}(E_{PR_P}(h(U_{MCS}))) = h(U_{MCS})$

Figure 2 Secret session key negotiation protocol.

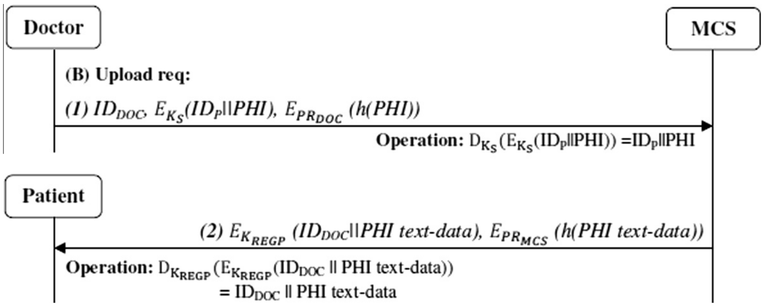
Doctor
MCS
(B) Upload req:
(1) ID_{DOC}, $E_{K_S}(ID_P \| PHI)$, $E_{PR_{DOC}}$ $(h(PHI))$
Operation: $D_{K_S}(E_{K_S}(ID_P \| PHI)) = ID_P \| PHI$
Patient
(2) $E_{K_{REGP}}$ (ID_{DOC}||PHI text-data), $E_{PR_{MCS}}$ (h(PHI text-data))
Operation: $D_{K_{REGP}}(E_{K_{REGP}}(ID_{DOC}$ || PHI text-data))
$= ID_{DOC}$ || PHI text-data

Figure 3 PHI uploading protocol.

***Step* 1:** Doctor → MCS: $\mathrm{ID_{DOC}}$, E_{K_S} $(\mathrm{ID_P}\|PHI)$, $E_{\mathrm{PR_{DOC}}}$ $(h(PHI))$
The doctor concatenates the patient's identity and PHI, encrypts the concatenated message using the secret session key K_S and sends the encrypted message along with the doctor's identity to the MCS. To support the integrity of the PHI, the doctor generates the hash digest of the patient's PHI, signs on it using his private key, and then sends the signed message to MCS.

After receiving the message, the MCS obtains the session key K_S from its database corresponding to the doctor's identity, uses it to decrypt the encrypted message and obtains the patient's identity and PHI. Then, to verify the integrity of the PHI, the MCS calculates the hash digest of the received PHI as $h(PHI) = H$ (say), decrypts the signed hash digest, sent by the doctor, using the doctor's public key, gets $h(PHI) = H'$ (say) and verifies $H' = H$? If the message passes verification, the MCS stores the patient's PHI in its database corresponding to the patient's identity and sends a copy of the PHI text-data by following step 2.

***Step* 2:** MCS → Patient: $E_{K_{\mathrm{REG_P}}}$ $(\mathrm{ID_{DOC}}\|PHI\ text-data)$, $E_{\mathrm{PR_{MCS}}}$ $(h(PHI\ text-data))$
The MCS concatenates the doctor's identity with the patient's PHI text-data, encrypts the concatenated message using the patient's registration key $K_{\mathrm{REG_P}}$ and then sends the encrypted message to the patient. Signed *PHI text-data* are also sent to the patient to support the integrity of the *PHI text-data.*

After receiving the message, the patient decrypts the encrypted message using his own registration key $K_{\mathrm{REG_P}}$ and obtains the PHI text-data and the identity of doctor who treated him. If the patient is sure about the identity of the treating doctor, then he verifies the integrity of the *PHI text-data* as discussed in *step 1* and if the verification is successful, he stores his *PHI text-data.*

2.2.3. PHI retrieval procedure

In this subsection, a patient's PHI retrieval procedure is introduced. As stated earlier, a doctor must negotiate a secret session key with the MCS before starting a new treatment session. This session key is then used to retrieve the patient's previous PHI (if any) from the MCS for ready reference and better treatment of the patient. The PHI retrieval procedure, consisting of two-message exchanges, is given in Fig. 4 and discussed below.

***Step* 1:** Doctor → MCS: $\mathrm{ID_{DOC}}$, E_{K_S} $(\mathrm{ID_{DOC}}\|\mathrm{ID_P})$
The doctor concatenates his identity with the patient's identity, encrypts the concatenated message using the secret session key K_S, and then sends the encrypted message and his identity as a PHI retrieval request to the MCS.

After receiving the request, the MCS obtains the doctor's identity, determines the session key K_S from its database, uses it to decrypt the encrypted message and obtains the identity of patient and doctor. Then, the MCS compares the extracted doctor's identity with the openly received identity and if the verification is successful, the MCS accesses the patient's PHI from its database based on the patient's identity and proceeds to the following step.

***Step* 2:** MCS → Doctor: E_{K_S} $(\mathrm{ID_P}\|PHI)$
The MCS concatenates the patient's identity with the patient's PHI, encrypts the concatenated message using the secret session key K_S, and then sends the encrypted message to the doctor.

After receiving the message, the doctor decrypts the message using K_S and obtains the patient's identity and PHI, verifies the patient's identity in regard to whose PHI is being requested and if everything is satisfactory, then the doctor uses the PHI for the patient's treatment.

Note that, for easy reference and quick diagnosis, the patient may provide his *PHI text-data* directly to the doctor by providing his external drive. However, this method is totally optional, but may be followed if there are any types of communication errors with the MCS.

2.2.4. PHI retrieval in patient's emergencies

In patient's emergency situations, e.g., when the patient is unable to provide consent for his treatment, a doctor initiates treatment immediately, and no formalities, such as identification of the patient or retrieval of PHI, are required. However, for better treatment and quicker diagnosis, the doctor may retrieve the patient's previous PHI from the MCS. To handle this situation, the doctor sends an emergency session request to the MCS and negotiates a secret session key for the particular emergency session as discussed in Section 2.2.1. The details of the patient's PHI retrieval procedure in an emergency situation is given in Fig. 5 and described below.

***Step* 1:** Doctor → MCS: $\mathrm{ID_{DOC}}$, E_{K_S} $(\mathrm{ID_{DOC}}\|\mathrm{ID_P})$
The doctor concatenates his identity with the patient's identity, encrypts the concatenated message using the secret session key K_S, and then sends the encrypted message along with his identity as *emergency retrieval request* to the MCS.

After receiving the doctor's emergency retrieval request, the MCS obtains K_S from its database based on the doctor's identity, decrypts the encrypted message using K_S

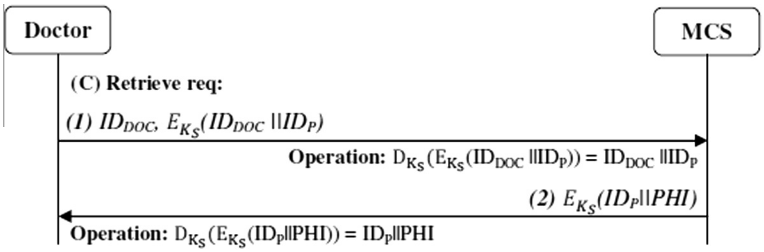
Doctor
MCS
(C) Retrieve req:
(1) ID_{DOC}, $E_{K_S}(ID_{DOC}\|ID_P)$
Operation: $\mathrm{D_{K_S}(E_{K_S}(ID_{DOC}\|ID_P)) = ID_{DOC}\|ID_P}$
(2) $E_{K_S}(ID_P\|PHI)$
Operation: $\mathrm{D_{K_S}(E_{K_S}(ID_P\|PHI)) = ID_P\|PHI}$

Figure 4 PHI retrieval protocol.

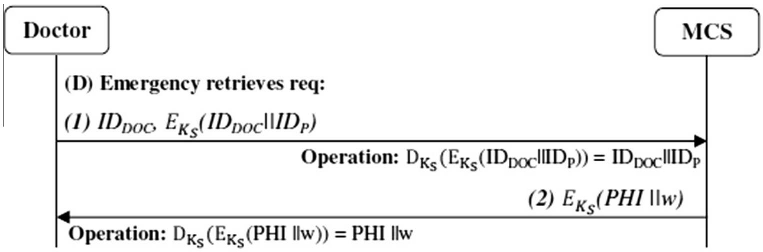
Doctor
MCS
(D) Emergency retrieves req:
(1) ID_{DOC}, $E_{K_S}(ID_{DOC}||ID_P)$
Operation: $D_{K_S}(E_{K_S}(ID_{DOC}||ID_P)) = ID_{DOC}||ID_P$
(2) $E_{K_S}(PHI\,||w)$
Operation: $D_{K_S}(E_{K_S}(PHI\,||w)) = PHI\,||w$

Figure 5 PHI retrieval protocol in patient's emergency situation.

and obtains the identities of the doctor and patient. The MCS then checks the integrity of the doctor's identity by comparing the decrypted identity with the openly received identity. If both are the same, the MCS accesses the patient's PHI from its database based on the patient's identity and follows the step discussed below.

***Step* 2:** MCS → Doctor: E_{K_S} $(PHI||w)$

The MCS concatenates the patient's PHI with the patient's signed agreement w, encrypts the concatenated message using the secret session key K_S, and then sends this encrypted message to the doctor.

After receiving the message, the doctor decrypts the message using the secret session key K_S and obtains the patient's PHI and w, from which he obtains all the information on the patient. At the end of the treatment session, when the patient becomes physically fit and the proper consent from the patient is received, the doctor uploads the patient's updated PHI to the MCS as described in Section 2.2.2.

2.2.5. *Foreign access to patient's PHI*

For treatment in foreign areas, i.e., the areas of a patient's home country that are not covered by the MCS in which the patient has registered as well as any foreign country, a patient has to approach a doctor, who has already registered with a local MCS and has negotiated a secret session key with it. Then, two cases may apply. (1) All MCSes in a country are interconnected through the Internet, or (2) All national-level MCSes (a root MCS of a hierarchical tree structure of MCSes of a country) in different countries are interconnected through the Internet. If case 1 applies, then a patient obtains treatment from any local MCS of his home country using his same registration key negotiated with his home MCS and the treatment of him/her in home country is transparent as all the protocols proposed earlier are equally applicable, and the uploading/retrieval of the PHI to/from the home MCS can be performed through any local MCS. On the other hand, treatment in a foreign country in case 2 is only possible with the following:

1) A patient must register with a foreign MCS and receive a secret registration key. The registration procedure as discussed in Subsection 2.1 can be used for this purpose.
2) After completion of diagnosis and receipt of medical advice, the generated PHI needs to be uploaded to the MCS and a complete copy of the same has to be provided to the patient. The protocols described in Subsections 2.2.1, 2.2.2 and 2.2.3 are followed for these procedures.
3) Finally, the PHI generated in foreign countries is uploaded to the patient's home MCS with the help of any doctor of the patient's home country.

3. HIPAA regulation fulfillment and performance analysis of the proposed scheme

In this section, we discuss the major contributions, validity and acceptance of our scheme. An analysis was conducted to determine how the proposed scheme fulfills the HIPAA privacy/security regulations, and the results of that analysis are shared in this section. Moreover, feasibility analysis is also discussed to demonstrate the practical applicability of the proposed scheme. Finally, the results of a performance evaluation of the proposed scheme in comparison with other existing schemes are also discussed to support our claims.

3.1. *Fulfillment of HIPAA regulations*

To illustrate and justify the fulfillment of HIPAA privacy and security regulations (Collmann et al., 2004; HIPAA, 1996a,b; Yanga et al., 2006), the following summarized HIPAA regulations given in Hu et al. (2010), Huang and Liu (2011) and Lee and Lee (2008) have been considered and implemented in this paper.

3.1.1. *Patient's understanding*

HIPAA requires a patient's understanding regarding the clear specification of the whole treatment process, which must be known and agreed upon by the patient. The contents of the agreement mainly are about the secure storing and retrieval of patient's PHI, complete information of patient and related information.

In our scheme, the patient's understanding is included via an electronically signed agreement w, which is sent to the MCS with the registration request, and the same agreement is signed and returned to the patient at the end of the registration phase. A copy of the final signed agreement is also kept in the MCS with the patient's PHI for future reference.

3.1.2. *Confidentiality*

According to HIPAA, various software safeguards, such as encryption-decryption, may be used to provide confidentiality of patient's PHI during storage and transmission over open channels.

To provide confidentiality of important data such as the patient's PHI, a public key certificate-based authentication protocol has been proposed in the registration phase for negotiating the secret registration key of patients, doctors and other medical staff. This key is then used as a master secret key for providing consent/authorization of the owner in different phases and negotiating a secret session key for encryption/decryption of important messages. The public-key certificate is used here for providing the initial security association for subsequent operations. The negotiated secret session key is used to send the encrypted patient's PHI during uploading and retrieval phases of the patient's treatment.

3.1.3. Patient's control

According to the HIPAA privacy and security regulations, a patient must have control of accessing his PHI.

Our scheme supports patient's consent both in uploading and retrieval of patient's PHI. A both-side signed agreement exists between the patient and the MCS during registration to obtain consent for accessing the patient's PHI data by any registered medical practitioner in the whole valid registration period.

3.1.4. Data integrity

According to HIPAA, the surety of data integrity must be kept, i.e., patient's PHI must be protected from medical omissions, tampering, unauthorized destruction and other such undermining of data integrity during transmission.

In our scheme, a signature is generated on the patient's PHI, and the signed PHI is transmitted along with the encrypted PHI. The signed PHI is used to verify the data integrity at the receiving end. Thus, data integrity is preserved in our scheme.

3.1.5. Consent exception

HIPAA privacy/security regulations support consent exception situation i.e., for life-saving purposes and other exceptional situations, access to a patient's PHI without the patient's consent is allowed.

In our scheme, a patient's consent exception case is considered and discussed in Section 2.2.4 for handling a patient's emergency situation.

Thus, the proposed scheme ensures the patient's understanding, confidentiality, data integrity, patient's control and consent exception cases as required for fulfilling the privacy and security regulations of HIPAA.

3.2. Feasibility analysis of proposed e-health system

In this section, a feasibility analysis, i.e., the implementation aspects of the proposed scheme, is described. The key establishment and management with security, along with computational and storage performance of the proposed scheme are mainly included and evaluated.

3.2.1. Efficient key management

The proposed scheme involves typical public key certificates, which are already available, for establishing the initial security association among different entities. Then, based on a public-key certificate, a two-way authenticated symmetric secret key, known as a registration key, is generated using the Diffie–Hellman (DH) (Diffie and Hellman, 1976) technique, which involves the exchange of only two short messages between the participants. The registration key is considered as a master key, which is then used to generate a temporary secret session key in each treatment session. All operations thus far involved in our scheme are trivial except the storing and maintaining of a large number of registration keys in the MCS. The key generation, distribution, storage and recovery are briefly explained below.

(1) For key generation, the MCS and patient compute a contributory patient's registration key $K_{\mathrm{REG_P}} = (g^{k_1})^{k_2} = g^{k_1 \cdot k_2} \bmod P$ using $g^{k_1} \bmod P$ and $g^{k_2} \bmod P$ public values generated independently by the patient and MCS, respectively. In addition, a random number K_S, assumed by a doctor, is negotiated with MCS using his registration key $K_{\mathrm{REG_D}}$. This K_S is considered a secret session key and used in a session. At the end of each session, the existing K_S is deleted, and a new K_S for a new session is negotiated. Because all these key generation procedures are based on existing public key certificates, they are secure and cost efficient.

(2) As such, no key distribution is involved in our scheme except for maintaining a database in MCS for key storage and retrieval for different decryption/verification purposes. In addition, the patient's PHI is encrypted by the MCS using the patient's registration key when sending a copy of the same to the patient. In addition, the MCS requires a public key certificate for each patient/member of the medical staff, which results in additional costs for storing, maintaining and verifying their public keys. Thus, our e-healthcare scheme, instead of distribution costs, mainly has key storage costs.

(3) For key recovery, the proposed scheme does not require any key recovery operation because in emergency situations, a doctor can directly retrieve the patient's PHI from the MCS with prior registration with the MCS.

Hence, our scheme efficiently supports the generation, distribution and storage of keys and equally ensures the secrecy of these keys with minimum cost because of the use of the available public key infrastructure. Therefore, the proposed scheme has the feasibility to be implemented in practical applications.

3.2.2. Computational performance

The computational costs involved in different phases of the proposed scheme are discussed in this section. The main computational phases are the (1) registration phase, (2) session key negotiation phase, (3) PHI uploading phase, (4) PHI retrieval phase and (5) PHI retrieval in patient's emergency. Their cost requirements are given below.

3.2.2.1. Registration phase.

(i) The phase uses PKI for entity authentication, which involves the verification cost of a public key (Stallings, 2009), thereby requiring *one* hash operation (NIST, 2002) and *one* public-key decryption (Stallings, 2009) for each side.

(ii) For mutual authentication and generation of a registration key, *three* random number generations (Biswas, 2011), *four* modular exponentiation operations (Diffie and Hellman, 1976), *three* public key encryptions/decryptions, *one* signature generation/verification and *four* message exchanges are required.

3.2.2.2. Session key negotiation phase. The cost includes cost of the generation of *two* random numbers, *two* symmetric encryptions/decryptions, *one* signature generation/verification, and the exchange of *three* messages.

3.2.2.3. PHI uploading phase. The cost includes the cost of *two* symmetric encryptions/decryptions, *two* signature generations/verifications and the exchange of *two* messages.

3.2.2.4. PHI retrieval phase. The cost includes the cost of *two* symmetric encryptions/decryptions and the exchange of *two* messages.

3.2.2.5. PHI retrieval in patient's emergency. The cost includes the cost of *two* symmetric encryptions/decryptions and the exchange of *two* messages.

Hence, the proposed scheme is cost-effective as most of the phases have symmetric encryption/decryption operations, where each requires much less processing time than a public-key encryption/decryption. In addition, the communication cost of our scheme is lower, as comparatively fewer messages are exchanged. As for storage requirements, the patient stores only a copy of his own PHI text-data and a signed agreement *w*, and no storage requirement by any doctor is needed. Moreover, the patient's PHI, registration key, signed agreement and public key certificate are stored in the MCS, which has a sufficient database. Therefore, our scheme is efficient in terms of its storage requirements.

3.3. Comparison with existing schemes

In this section, a comparison with three existing schemes is provided as a performance evaluation of the proposed scheme. Lee and Lee (2008) proposed a session-based solution that requires the presence of a patient's smart card, as the card stores the patient's PHI and master key for authentication. As a result, this scheme suffers from several limitations. (1) The patient's PHI is available only when both patient and smart card are physically present at the healthcare provider, and there is also no possibility of accessing the patient's PHI from distant locations. (2) Simultaneous access to the patient's PHI is not feasible for such medical necessities because of gathering of different medical expert opinions and pathological analysis. (3) The smartcard-based approach also adds additional overhead if the laboratories analyzing different medical test-samples are located throughout a wide geographical distribution. (4) A security flaw may also exist with a PIN/password-enabled smart card, where instead of the owner, the presenter of the smartcard is authenticated when the PIN is compromised. (5) This scheme also requires a huge amount of PHI (both text-data and image-data) storage in a smart card, which may thus create burdens for patients in terms of storage and maintenance. (6) Finally, as discussed earlier, instead of a session-based scheme, the contract-based system supports the entire treatment session, which appears to be more suitable for an e-health system.

Our scheme eradicates these limitations in the following ways. (1) The patient's PHI is kept by the MCS, so it is possible to access patient's PHI through the Internet from a distant location. (2) Simultaneous access to the patient's PHI over Internet is also possible. (3) Different medical laboratories may access the PHI and directly upload the patient's test reports to the MCS through the Internet. (4) No one is allowed to access patient's PHI until an authenticated registration with the MCS is completed. (5) The MCS securely stores and maintains patients' PHI, and thus no burden is imposed on patients. (6) Lastly, a contract-oriented e-health system is presented in this work.

In 2010, Hu et al. proposed a contract-based scheme to address the HIPAA privacy and security regulations for e-health systems. In this scheme, a hybrid security scheme based on public key infrastructure (PKI) and a Medicare smartcard is used. This scheme has several limitations – (1) It violates HIPAA privacy/security regulations as no patient consent is incorporated during storage (retrieval) of PHI to (from) the MCS. (2) This scheme remains silent on the issue of patient's consent exception cases involved in handling patient's emergency situations. (3) A replay attack is possible during the uploading and retrieval of PHI as an attacker can impersonate a legitimate user by knowing information from previous communications. (4) Lastly, the scheme, similar to Lee and Lee (2008), suffers from the weaknesses inherent in using a smart-card based system.

The proposed scheme overcomes all these limitations in the following ways. (1) Prior to treatment, an agreement is made between a patient and the MCS, which stores the patient's consent (only registered medical staff can access the PHI). (2) A patient consent exception case is incorporated into our scheme to handle patient's emergency treatment. (3) The replay attack is defended against in the proposed scheme by a registration- and session-key negotiation-protocol containing nonce or random numbers to prevent forging of participant credentials. (4) Lastly, the proposed scheme uses a public-key certificate for initial authentication of the entities and is thus free from any smartcard-based weaknesses.

In 2011, Huang and Liu proposed a smart card-based e-health scheme to satisfy HIPAA privacy and security regulations, where ECC is used for key generation and management. As stated earlier, this scheme is a modification of Lee and Lee's (2008) scheme and because of the use of ECC, it requires a smaller key size and thus has less computation and communication costs for registration, signature generation-verification, and encryption-decryption than Lee and Lee's (2008) scheme. However, this scheme has all the limitations of Lee and Lee's scheme (2008) except for allowing patients to freely choose and update their passwords. Our scheme, similar to Lee and Lee's (2008) scheme, is free of all the limitations present in the Huang and Liu (2011) scheme.

A feature-based comparison of the proposed scheme with other three existing schemes is provided in Table 1 and shows the overall requirements and performance in terms of some characteristic features. As seen from Table 1, the proposed scheme exploits most of the efficient and usable tools in its implementation, and none of the existing schemes altogether supports the last six useful features. However, the proposed scheme uses PKI; thus, the additional overhead of maintaining and verifying public-key certificates is kept minimal by proposing the one-time use of PKI for initial verification of different actors in the scheme.

Table 1 Comparison of proposed scheme with three existing schemes.

Requirements/features	Lee and Lee (2008)	Hu et al. (2010)	Huang and Liu (2011)	**Proposed scheme**
Security architecture based on	Session	Contract	Session	**Contract**
Key type	Symmetric	Public–private	ECC	**Public–private**
Authentication based on	Smart Card	Smart Card	Smart Card	**Public-key certificate**
Medium used to access patient's PHI	Smart Card	Internet	Smart Card	**Internet**
Patient's PHI stored in	Smart Card	MCS	Smart Card	**MCS**
Simultaneous access of PHI	No	Yes	No	**Yes**
Access of PHI from distant locations	No	Yes	No	**Yes**
Protected from replay attack	No	No	No	**Yes**
Patient's consent to upload and retrieve PHI	Yes	No	Yes	**Yes**
Handles patient's emergencies	Yes	No	Yes	**Yes**
Communication and processing overhead	High	High	Low	**Low**

Regarding the practical applicability of our scheme, the proposed scheme has been built up with prior consultation with some professional physicians, and all have expressed their opinions in favor of our scheme. They also mentioned that it is very exciting to go through the workflows specified and interesting in terms of approaches considered for online e-healthcare implementation. However, they have commented that the proposed scheme is much more effective with chronic illness rather than the acute onset of any illness.

4. Conclusion

In this paper, a CA-based e-healthcare system has been proposed to satisfy HIPAA privacy and security regulations. It uses the existing PKI and public key certificate to set up a contract-based system with a MCS located at hospitals. In the scheme, the MCS stores the patients' PHI, which is securely retrieved/ updated by medical staff after the end of a contract period. A patient also receives his updated PHI from the MCS. The proposed e-health system consists of six phases, and all of them are implemented securely. A security analysis proves that the scheme is free from all relevant attacks. Lastly, a comparison table is provided that highlights the usefulness of the proposed scheme over three other existing schemes.

References

Agrawal, R., Johnson, C., 2006. Securing electronic health records without impeding the flow of information. Proceedings of the International Medical Informatics Association Working Conference Security in Health Information Systems.

Agrawal, R., Asonov, D., Bayardo, R., Grandison, T., Johnson, C., Kiernan, J., 2005. Managing Disclosure of Private Healthcare Data with Hippocratic Database. White paper, IBM.

Aljumah, A.A., Ahamad, M.G., Siddiqui, M.K., 2013. Application of data mining: diabetes health care in young and old patients. Journal of King Saud University – Computer and Information Sciences 25, 127–136.

Bhatti, R., Samuel, A., Eltabakh, M.Y., Amjad, H., Ghafoor, A., 2007. Engineering a policy based system for federated healthcare databases. IEEE Transactions on Knowledge and Data Engineering 19 (3), 1288–1304.

Biswas, G.P., 2011. Establishment of authenticated secret session keys using digital signature standard. Information Security Journal: A Global Perspective 20 (1), 9–16.

Collmann, J., Lambert, D., Brummett, M., DeFord, D., Coleman, J., Cooper, T., McCall, K., Seymour, D., Albert, C., Dorofee, A., 2004. Beyond good practice: Why HIPAA only addresses part of the data security problem. International Congress Series 1268, 113–118.

Diffie, W., Hellman, M., 1976. New directions in cryptology. IEEE Transaction on Information Theory 22, 644–654.

ElGamal, T., 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31 (4), 469–472.

El-Sappagh, S.H., El-Masri, S., 2013. A distributed clinical decision support system architecture. Journal of King Saud University – Computer andInformation Sciences, http://dx.doi.org/10.1016/j.jksuci.2013.03.005.

Federal Register, 2002. Standards for privacy of individually identifiable health information. Federal Register 67, 53181–53273.

HIPAA, 1996a. Health Insurance Portability and Accountability Act of 1996, 104th Congress, Public Law, 104–191.

HIPAA, 1996b. Health Insurance Portability Accountability Act of 1996 (HIPAA), Centers for Medicare and Medicaid Services, Available at: <http://www.cms.hhs.gov/hipaageninfo> (online).

Hu, J., Han, F., 2009. A pixel-based scrambling scheme for digital medical images protection. Journal of Network and Computer Applications 32 (4), 788–794.

Hu, J., Chen, H., Hou, T., 2010. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards and Interfaces 32, 274–280.

Huang, H.F., Liu, K.C., 2011. Efficient key management for preserving HIPAA regulations. The Journal of Systems and Software 84, 113–119.

Huanga, L., Chu, H., Lien, C., Hsiao, C., Kao, T., 2009. Privacy preservation and information security protection for patients' portable electronic health records. Computers in Biology and Medicine 39, 743–750.

Jin, J., Ahn, G., Hu, H., Covington, M.J., Zhang, X., 2011. Patient-centric authorization framework for electronic healthcare services. Computers and Security 30, 116–127.

Koblitz, N., 1987. Elliptic Curve Cryptosystem. Journal of Mathematics Computation 48 (177), 203–209.

Lambrinoudakis, C., Gritzalis, S., 2000. Managing medical and insurance information through a smart-card-based information system. Journal of Medical Systems 24 (4), 213–234.

Lee, W.B., Lee, C.D., 2008. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Transactions on Information Technology in Biomedicine 12 (1), 34–41.

Lee, C.D., Ho, K., Lee, W.B., 2011. A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations. IEEE Transactions on Information Technology in Biomedicine 15 (4), 550–556.

Levi, A., Caglayan, M.U., Koc, C.K., 2004. Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. ACM Transactions on Information and System Security 7 (1), 21–59.

Li, J., Lee, J., Chang, C., 2008. Preserving PHI in compliance with HIPAA privacy/security regulations using cryptographic techniques. Proceedings of International Conference on Intelligent Information Hiding and Multimedia, Signal Processing, 1545–1548.

May, T.T., 1998. Medical information security: the evolving challenge. Proceedings of 32nd Annual International Carnahan Conference on Security Technology, 85–92.

Miller, V., 1985. Use of elliptic curves in cryptography. Proceedings of Advances in Cryptology-CRYPTO' 85, LNCS 218, 417–426.

NIST, 2001. Introduction to Public Key Technology and the Federal PKI Infrastructure, National Institute of Standards and Technology.

NIST, 2002. Secure Hash Standard, National Institute of Standards and Technology, FIPS, 180–182.

Stallings, W., 2009. Cryptography and Network Security: Principles and Practices, Fourth ed. Prentice Hall, International Edition, pp. 420–430.

Weise, J., 2001. Public Key Infrastructure Overview, Sun PSSM Global Security Practice. Sun Blue Prints™.

Yanga, C.M., Lina, H.C., Changb, P., Jianc, W.S., 2006. Taiwan's perspective on electronic medical records' security and privacy protection: lessons learned from HIPAA. Computer Methods and Programs in Biomedicine 82 (3), 277–282.

Yu, W.D., Ray, P., Motoc, T., 2006. A RFID technology based wireless mobile multimedia system in healthcare. The 8th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2006, 1–8.