J Med Syst (2012) 36:631–638
DOI 10.1007/s10916-010-9527-7

ORIGINAL PAPER

# A Password-Based User Authentication Scheme for the Integrated EPR Information System

**Zhen-Yu Wu · Yufang Chung · Feipei Lai · Tzer-Shyong Chen**

Received: 20 March 2010 / Accepted: 7 May 2010 / Published online: 27 May 2010


**Abstract** With the rapid development of the Internet, digitization and electronic orientation are required in various applications of our daily life. For e-medicine, establishing Electronic patient records (EPRs) for all the patients has become the top issue during the last decade. Simultaneously, constructing an integrated EPR information system of all the patients is beneficial because it can provide medical institutions and the academia with most of the patients' information in details for them to make correct decisions and clinical decisions, to maintain and analyze patients' health. Also beneficial to doctors and scholars, the EPR system can give them record linkage for researches, payment audits, or other services bound to be developed and integrated into medicine. To tackle the illegal access and to prevent the information from theft during transmission over the insecure Internet, we propose a password-based user authentication scheme suitable for information integration.

**Keywords** E-medicine · Electronic patient records · Integrated EPR information system · Password · Authentication

Z.-Y. Wu · F. Lai
Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan

Y. Chung
Department of Electrical Engineering, Tunghai University, Taichung, Taiwan

F. Lai
Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan

T.-S. Chen
Department of Information Management, Tunghai University, Taichung, Taiwan

F. Lai
Graduate Institute of Biomedical Electronics and Bioinformatics, National Taiwan University, Taipei, Taiwan

*Present Address:*
Z.-Y. Wu (✉)
#1 Roosevelt Rd. Sec. 4,
Taipei, Taiwan 106, Republic of China
e-mail: d96922021@ntu.edu.tw

## Introduction

Recently, with the rapid development of the Internet, various technologies for applications are maturing and leading to digitization and electronic orientation in daily life such as e-commerce, e-banking, e-government, e-society, and e-medicine. Most hospitals or medical institutes have well-developed Electronic patient records (EPRs) for e-medicine during the last decade and the technology for EPRs remains as one of the most popular researches in e-medicine [1–5].

Traditionally, the written medical record of the patient is the most important data for a doctor during consultations. Most major medical institutions around the world relied on paper and pen for recording patients' medical problems. Patients obviously left behind their medical histories with each medical institution they visited, while medical institutions retained the rights to the medical records of their patients. Today, due to loss of medical integration or failure of medical-history retrieval from other institutions, diagnoses are often delayed or made incorrectly. At the same time, medical-resource is wasted as a result of repeating rounds of exhaustive queries, tests, and diagnoses [1, 6, 7].

EPR's goal is to record patients' medical information and histories by digitizing them into a pile of electronic documents that can be stored, utilized, and modified. Not only do EPRs provide doctors with the usual diagnosis records, nursing records, reports, and other image records, but EPRs also provide patients with their complete and correct medical problems along with other functions such as medical alerts or reminders, clinical decision supports, and links to their medical support groups [1–3, 8].

The ultimate aim of EPRs is to allow the sharing of patients' medical histories scattered among medical institutions through the Internet. With comprehensive information in hand, every doctor in any medical institution can make the proper diagnosis and treatment for a patient in the very first time correctly. It is quite clear that the buildup of EPRs can facilitate real-time diagnosis and correct treatment for each patient without being held up by the need to rerun tests due to lack of information. At present, many organizations have drawn up protocols such as HL7 [5, 9, 10] and DICOM [11–14] for sharing patients' medical information. However, the establishment of medical information systems remains as the core in future development. A highly feasible information system can supply electronic treatment services for medical users. For example, it can provide conversion and integration of EPRs in different formats, extensive medical history exchange services, and even translation services for medical records. These are highly recommended supplement electronic treatment systems in the future.

As to the rapid development of Grid computing and Cloud computing, the Internet has no doubt risen in popularity for facilitating network services, information, and even information management [15–17, 26]. Hence, Integrated EPR Information System through the Internet can provide all institutions, doctors, and patients with sufficient information for further personal decision making, clinical decision making, maintenance and analysis for health purposes, record linkage for researches, and payment auditing. As illustrated in Fig. 1, all the users, who could be from medical academic institutes, from large hospitals or from private clinics and even an individual patient, can be free to request all of the services within the integrated EPR information system. Once they complete the verification process or other security protocols, they can have access to the right information.

Obviously, the security issue for the integrated EPR information system becomes a significant concern. Speaking specifically, the most concerned security issue is of how to ensure information privacy and security during transmission through the insecure Internet. Relevant user authentication schemes or secret-key distribution protocols are generally used to solve this kind of problem because these protocols are regarded as the primary safeguards in network electronic applications [7, 18–21]. Among these protocols, the password-based mechanism is the most widely employed method because of its efficiency [22–25]. Under such mechanism, each user is allowed to select his password and keep in mind without any additional assistant device for the further authentication process. Therefore, we would like to propose an efficient password-based scheme in this paper suitable for Integrated EPR Information System, namely a password-based user authentication scheme.

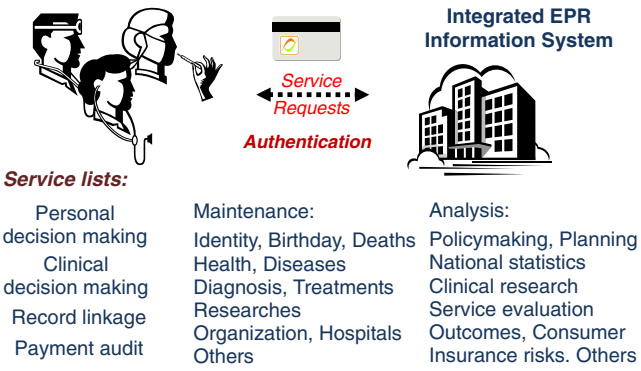


**Fig. 1** Provided services of integrated EPR information system

The rest of this paper is organized as follows. "Preliminary" introduces the corresponding techniques applied in our proposal. "The proposed scheme" illustrates the proposed password-based user authentication scheme. Security analyses are done in "Security analysis", and finally, conclusions are drawn in "Conclusions".

## Preliminary

Our scheme employs three techniques related to computer science. They are smart card, one-way hash function, and bitwise operations. Below is the detailed explanation of them.

### Smart card

Smart card is a plastic card that is similar in size to the credit card or the ATM card. The difference being there is an additional Integrated Circuit (IC) chip on smart card. Besides memory function, this IC chip can compute and process data, in addition to statistical functions. Therefore, this card can store the personal information of the cardholder, such as, in terms of medicine, identity, password, secret values, prescriptions and various related personal diagnostic records; in paired with the system operation, it can even acquire calculating, integrated, and statistical functions [27].

The center of smart cards is the processor, also called Central Processing Unit (CPU). Smart cards sometimes are called CPU card for the CPU is built into a single chip

which executes instructions. The chip itself is a small piece of silicon with a complicated electrical circuit called an IC. The IC chip can be divided into many domains, each of which performs different function. The IC chip has the following features [8, 27, 30, 31]:

1. Includes a CPU, and a preprogrammed Card Operating System (COS),
2. Capable of hierarchal access security control and information verification,
3. Has larger memory storage space than other cards, where information can be modified or deleted,
4. Has higher security, and cannot be easily replicated,
5. Can operate off-line, thereby cuts down communication costs
6. Has encryption programs such as Data Encryption Standard (DES) and RSA to provide active protection.

In sum, development on the smart card over the past decade has turned it into a widely applied technology in electronics.

### Hash function

A hash function is a mathematical operation that transforms a variable-size message into a fixed-size digest [28]. For example, a hash value $H$ is generated by a hash function $h$; this is denoted by $H = h(M)$, in which $M$ is a message of variable length and the hash value $H$ is limited to a fixed length. The hash value $H$ is appended to a message to allow the receiver to verify its legitimacy and integrity. In addition, the hash function can be used to create the "fingerprint" of a file, a message, or a block of data. The function $h$ contains the following properties:

1. $h$ can be applied to a block of data of any size.
2. $h(x)$ is efficient to derive any given $x$ so that the implementation of both hardware and software can be more practicable.
3. The output of $h$ is limited to a fixed length no matter the length of the input.
4. For any given $H$, it is computationally infeasible to find $x$ so that $H = h(x)$ can be derived. This is defined as the one-way property.
5. For any given block $x$, it is computationally infeasible to find $y \neq x$ but satisfy $h(y) = h(x)$. This is defined as weak collision resistance.
6. It is computationally infeasible to find any pair $(x, y)$ so that $h(x) = h(y)$. This is defined as strong collision resistance.

One normally used cryptographic hash function is the secure hash algorithm SHA-256 whose fixed-size output digest has a length of 256 bits. Besides, SHA-384 or SHA 512 algorithm will be able to replace the recommended SHA-256 algorithm if there are security or efficiency concerns in the future [28].

### Bitwise operation—XOR

A bitwise operation is a computation that operates on binary numerals at the level of their individual bits which is slightly faster than addition and subtraction operations and significantly faster than multiplication and division operations in computer programming or applications. XOR is one type of the bitwise operations. It takes two bit patterns of equal length and performs the logical XOR operation on each pair of corresponding bits. The result in each position is 1 if the two bits are different, and 0 if they are the same, as Fig. 2 shows.

### Symmetric cryptosystem

Cryptosystems are used to transform a plaintext into an unreadable ciphertext to prevent unauthorized disclosure. They can be classified into two main groups: symmetric and asymmetric cryptosystems [28]. Symmetric cryptosystem's approach involves interaction between parties, for example: a requester and a server shares a secret (or session) key, and uses it to encrypt messages sent over the internet. By using the same session key, the receiver of the message can decrypt the message. Advanced Encryption Standard (AES) [28], one of the most famous symmetric cryptosystems nowadays, has vastly superior security and good throughput, so it is recommended in many electronic applications, including e-medicine, for its proper secret (session) key to guarantee confidentiality and efficiency [4, 6, 29].

## The proposed scheme

Our password-based user authentication scheme is composed of four phases. They are registration phase, login phase, verification phase, and password change phase. The main entities include users and the remote server. Users are patients, physicians, doctors, nurses, or researchers. The remote server is a trusted center, the integrated EPR information system, which provides many services related to the electronic patient records such as integration, investiga-

| | | | | | | |
|---|---|---|---|---|---|---|
| String1 | 1 | 0 | 0 | 1 | 0 | 1 |
| XOR | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ | ⊕ |
| String2 | 1 | 1 | 0 | 0 | 1 | 0 |
| Result | 0 | 1 | 0 | 1 | 1 | 1 |

**Fig. 2** XOR operation

tion, recording, modification, and maintenance. The system also restricts rights to access and change according to different levels, such as only doctors can alter relating EPRs.

Figure 3 illustrates the flowchart of this proposal. All users need to pass the register phase so as to get the login password and medical smart cards. Then they can login to the remote server through smart cards and acquire the desired services after the server has verified their identities, passwords, and the transmitted parameters. If one would like to change the password, he can execute the password change phase.

Before describing the details of our proposal, the notation defined and used in this scheme is shown in Table 1.

## Registration phase

When the user $U$, which includes researchers of the medical academia, physicians and doctors of large hospitals or small clinics, nursing staffs, and patients want to obtain some services provided by the integrated EPR information system, he must first register to this remote server $S$. He would propose a registration request so as to get his own medical smart card from the server system as follows:

Step 1: $U$ submits his own identity $ID$ and the chosen password $pw$ to $S$.

Step 2: $S$ checks the validity of $ID$, and then computes the related hash value $v = h(K \oplus ID)$, where $K$ is the secret number belonging to $S$.

Step 3: $S$ finds a appropriate value $N$ and makes the sum of $v \cdot pw + N$ being equal to a constant secret value $H$. Then $S$ computes $s = h(pw \| K)$, where $\|$ is a bit concatenation operator. For example, 0 $\|$ 1 would become 01.

Step 4: $S$ personalizes $U$'s medical smart card included with the above parameters $[h(\cdot), N, s, pw]$. The number $s$ is well protected by the device of smart card, and no other user, except the smart card holder, can catch the value of $s$.

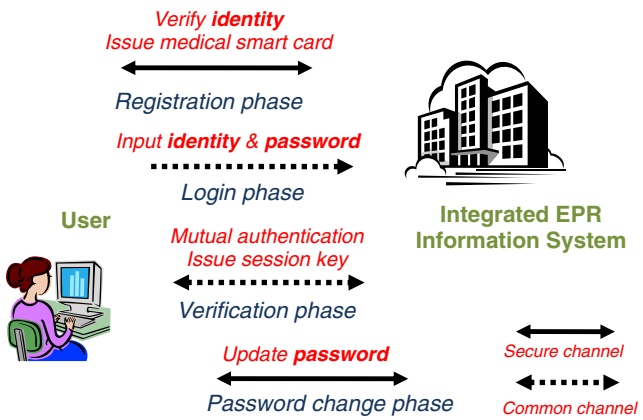


**Fig. 3** Flowchart of proposed scheme

**Table 1** Notation defined and used in our scheme

| | |
|---|---|
| $U$ | the medical service requester (user) |
| $pw$ | the password of user $U$ |
| $ID$ | the identity of user $U$ |
| $S$ | the integrated EPR information system |
| $h(\cdot)$ | a public one-way hash function |
| $\oplus$ | a bit-wise XOR operation |

Step 5: $S$ returns the medical smart card to $U$ through a secure channel.

## Login phase

When user $U$ wants to log into the integrated EPR information system to acquire the needed services, he inserts his medical smart card into a terminal and then keys in his identity $ID$ along with his password $pw$. The smart card will execute the following steps automatically:

Step 1: Choose a random number $r_1$ to compute $C_1$ and $C_2$, where $C_1 = h(s \| r_1)$, $C_2 = r_1 \cdot pw$.

Step 2: Retrieve the smart card's saved value $N$ and user's $ID$, with $C_1$ and $C_2$ and passes them on to the remote integrated EPR information system $S$ through the common network channel.

## Verification phase

When the integrated EPR information system receives the service request with parameters $(N, ID, C_1, C_2)$ from the user, server $S$ does the verification as follows:

Step 1: Check the validity of user's identity $ID$. If the $ID$ is legal, $S$ accepts the service request; otherwise, the service request is rejected.

Step 2: Apply the owned secret values $K$ and $H$, and the obtained $N$ to restore user's password $pw$: Compute $v = h(K \oplus ID)$, and $pw = (H - N) \cdot v^{-1}$.

Step 3: Apply restored $pw$ to calculate the user chosen random number $r_1'$ through the equation $r_1' = pw^{-1} \cdot C_2 = pw^{-1} \cdot pw \cdot r_1$. Simultaneously, the secret value of user $s'$ by $h(pw \| K)$ is computed.

Step 4: Check whether the value of $h(s' \| r_1')$ is equal to $C_1$. If the two values are the same, go to Step 5; otherwise, stop and reply the error message to $U$.

Step 5: Generate the message pair $(a, b)$ for a mutual authentication between $S$ and $U$. $a$ is equal to $r_2 \oplus h(s')$, where $r_2$ is a random number chosen by $S$, and $b$ is equal to $h(pw \| r_2 \| r_1')$.

Step 6: Send $(a, b)$ to $U$ through the common network channel.

When user $U$ receives the reply message ($a$, $b$) from the integrated EPR information system, $U$ does the verification as follows:

Step 1: Restore the server chosen random number $r_2'$ through the equation $r_2' = a \oplus h(s)$.
Step 2: Verify whether $b$ is equivalent to $h(pw \| r_2' \| r_1)$. If they are equivalent, user $U$ confirms that $S$ is valid.
Step 3: Send back $c = h(pw \| r_1 \| r_2')$ to server $S$ for another side authentication.

After the integrated EPR information system $S$ receives $c$:

Step 1: Compare $c$ with the value $h(pw \| r_1' \| r_2)$ calculated to check whether both of them are equivalent or not. If equivalent, $U$ is authenticated and granted access to obtain the services and resources of $S$. A session key $sk = h(r_1' \| r_2) = h(r_1 \| r_2')$ will be generated and used for secure transmission at the following operations after the mutual authentication process is done.

Password change phase

During the effective life cycle of the password, user $U$ can change his password as he likes by the following steps:

Step 1: $U$ sends his identity $ID$, the old password $pw$ and the new chosen password $pw_{new}$ to the integrated EPR information system $S$ through a secure channel.
Step 2: $S$ finds another appropriate $N^*$ to make the value $v \cdot pw_{new} + N^*$ being equal to the secret value $H$. Then $S$ creates the new $s = h(pw_{new} \| K)$, and sends it with the $N^*$ to $U$ through the secure channel.

## Security analysis

A password-based user authentication scheme for an integrated EPR information system is said to be effective when it can assure the system's security in terms of password protection, data transmission, user masquerading and system spoofing. In other words, the scheme can resist various malicious attacks, including stolen-verifier attacks, on-line and off-line password guessing attacks, replay attacks, and server spoofing attacks. In this section, we will analyze each in details and show how the proposed scheme satisfying with the above-mentioned security criteria.

Password protection

Here the passwords play a very important role for each user, such as a doctor, a nurse, a patient, or a scholar, for logging into the integrated EPR information system. Assuring the security of a password is the most crucial key-point in our security analysis. Thus, we would like to prove that our password authentication scheme can withstand two kinds of attacks aimed at passwords. They are the stolen-verifier attack, and the password guessing attack. The password guessing attack can further be classified into on-line and off-line attacks.

Stolen-verifier attacks mean that some machinated insiders of a remote server are able to steal or modify the users' legitimate passwords or update the password-verification tables stored in the server's database. This attack would not succeed in our scheme because the password of a user is instantaneously generated and verified by the server, who uses its secret value $K$ upon the login phase. No passwords or verification tables have to be kept in the server's database; therefore, the insiders would not be able to steal or modify the passwords.

On-line password guessing attacks mean that an attacker continuously guesses the possible passwords and tries each of them to log into the server till he is successful. In our scheme, such attack will be perceived immediately. Suppose an eavesdropper attempts to identify the password of a legal user. He would guess a possible password to go through Step 1 in the login phase to obtain corresponding parameters, such as $C_1$ and $C_2$. However, the probability of knowing the correct password is only $2^{-k}$, where $k$ is the length of the password. On the other hand, the server can rapidly detect this kind of attack by confirming whether $h(s \| r_1)$ is equal to $C_1$ or not. Generally, when the third guess goes wrong, the attacker would be kicked out. Therefore, on-line password guessing attacks cannot work in our scheme.

Off-line password guessing attacks mean that an attacker employs some intercepted information or some self-generating parameters to guess the password of a specific user. To render this kind of attack ineffectual, our scheme protects the password-related parameters, i.e. the random numbers $r_1$, $r_2$ and secret number $s$, with the cryptographic hash function. Now, assume that an eavesdropper can obtain the following parameters $C_1$, $C_2$, or $a$, $b$, $c$ in the login and verification phase. However, without $s$, he cannot know the right $r_1$ by $C_1 = h(s \| r_1)$. Similarly, it is also unable for him to guess the correct password $pw$ by $a = r_2 \oplus h(s)$, $b = h(pw \| r_2 \| r_1)$, $c = h(pw \| r_1 \| r_2)$ without $r_1$ and $r_2$. Therefore, off-line password guessing attacks can be withstood.

Data transmission security

After a user logs into the remote integrated EPR information system successfully, another crucial security issue upon authentication arises, which is assuring data integrity and security during transmission. Safeguarding confidential

data from revelation, modification, or deletion during its transmission is the major concern in this stage.

A session key is used in our scheme to protect the confidential data from being revealed, modified, or deleted during its transmission. The session key is generated via hashing two random numbers $r_1$ and $r_2$ after the verification process. All of the confidential data are encrypted by the session key, which means that without the session key, no attacker can eavesdrop, modify, or delete the transmitting data.

Furthermore, the session key in our scheme will be invalid whenever the communication between the user and the integrated system server goes to the end. This means the key will have expired its period of usage and cannot be used any more so that it is revoked. When the user enters the system again, a new session key will be generated for him to encrypt his information during the current communication process. Therefore, there will be much difficulty for anyone to calculate any of the probable previous session keys despite using all his known information.

Therefore, unless the user shares his session key on purpose with the third party, our scheme shows the ability to achieve the requirement of data transmission security with the help of the session key.

## User masquerading detection

While the password authentication is being processed, conspiring attackers may impersonate the identities of the medical staff, patients, or researchers in order to pass the authentication phase and gain the right to access the data in the remote integrated EPR information system. To prevent the disclosure of users' privacy, protocols are necessary to fend off replay attacks. A replay attack is a kind of network attack where a valid data transmission is maliciously repeated by some machinated eavesdropper. Generally, the eavesdropper intercepts the data from a certain user and transmits it repeatedly to log into the integrated EPR information system by masquerading. To prevent such attack, we make use of two fresh and random variables $r_1$ and $r_2$ in our scheme during the login and verification phases. Suppose that an eavesdropper intentionally intercepts ($ID$, $N$, $C_1$, $C_2$) from the login phase, and impersonates the legal user to log into the server by replaying this message. However, without knowing the random number $r_1$, he cannot restore the correct $r_2$ to compute $c$ for server $S$ and furthermore, he is unable to confirm his identity, even though he may have received the replied message ($a$, $b$) in the verification phase. Therefore, the replay attacks will fail.

Actually, the password in our scheme is protected by the cryptographic hash function, and thus an attacker is unable to generate and interpret authentication messages correctly without the knowledge of a user's password. It is obviously impossible for a person in our scheme to masquerade as a legitimate user to log into an integrated system server and acquire system services.

## Server spoofing detection

Similar to "User masquerading detection", the attack by someone masquerading as the server to cheat other users is another security concern. An attacker may masquerade the identity of the remote integrated EPR information system to carry out illegal, imperceptible authentication behavior, and consequently obtain the private information of some user through the transmitted data. This is known as server spoofing attacks: someone masquerades as the server to cheat other users.

There are two possible ways to let a conspiring attacker successfully spoof the other users in our scheme. One is when the attacker obtains the secret values $K$ and $H$ of a remote system, he can impersonate the server; the other is when the attacker guesses correctly the password of a certain user, he can directly perform partial phases at the server part without secret values. However, the secret values $K$ and $H$ are never transmitted via a common network channel and are stored on the server computer's hard drive which only the administrator has the right to control and access; so it is impossible for anyone to acquire them. In addition to that, the user's password is protected by the cryptographic hash function. Therefore, the server spoofing attacks will be detected and prevented.

**Table 2** Comparison with other related schemes

| | Lin-Lai (2004) | Lee-Chiu (2005) | Lu et al. (2008) | Wang et al. (2009) | Our Proposal |
|---|---|---|---|---|---|
| Computational operations in registration phase | 1H+1E | 2H+1E | 1H | 2H | 2H |
| Computational operations in login phase | 2H+2E | 2H+1E | 1EC | 2H | 1H+1M |
| Computational operations in verification phase | 1H+2E | 2H | 3H+2EC | 6H | 10H+1M |
| Suffer insecure attacks | No | No | Yes | Yes | No |

H: one way hash function operations; M: multiplication operations; E: exponential operations; EC: elliptic curve exponential operations

Performance comparisons

To display how our proposed password-based user authentication scheme is suitable and efficient to be implemented under the e-medicine environments, following is the comparison of our scheme with other related schemes as summarized in Table 2. Clearly, Lin-Lai's scheme [22] and Lee-Chiu's scheme [23] require some exponential operations leading to the need for more calculation time resulting into inefficiency. Wang et al.'s scheme [24] and Lu et al.'s scheme [15] suffer from insecure attacks, such as off-line password guessing attacks, server spoofing attacks and are not practical for implementation. Ours on the contrary, has not only very low computation costs, but requires only few hashing functions and multiplication computations. With the analysis of the four security concerns mentioned above, security on using the mechanism is assured.

## Conclusions

In this paper, we aim to propose a password-based user authentication scheme appropriate for the integrated EPR medical information system. Not only did we explain what security requirements EPR medical information systems need, but we have also showed how this proposed scheme can satisfy those requirements. Namely, the security requirements are password protection, data transmission security, user masquerading detection, and system spoofing detection. Besides, this proposed scheme can also resist several malicious attacks, including stolen-verifier attacks, on-line and off-line password guessing attacks, replay attacks, and server spoofing attacks. Analyses show that the scheme is secure and efficient to be implemented under the medical application environments.

**Acknowledgement** This work was supported partially by National Science Council, Taiwan under Grants NSC 98-2221-E-029-025.

## References

1. Takeda, H., Matsumura, Y., and Kuwata, S., Architecture for networked electronic patient record systems. *Int. J. Med. Inform.* 60(2):161–167, 2000.
2. Chan, A. T. S., Cao, J., Chan, H., and Young, G., A web-enabled framework for smart card application in health services. *Commun. ACM* 44(9):77–82, 2001.
3. Wang, D. W., Liu, D. R., and Chen, Y. C., A mechanism to verify the integrity of computer-based patient records. *J. China Assoc. Med. Inform.* 10:71–84, 1999.
4. Gritzalis, S., Lambrinoudakis, C., Lekkas, D., and Deftereos, S., Technicl guidelines for enhancing privacy and data protection in modern electronic medical environments. *IEEE Trans. Inf. Technol. Biomed.* 9(3):413–423, 2005.
5. Dolin, R. H., Alschuler, L., Beebe, C., Biron, P. V., Boyer, S. L., Essin, D., Kimber, E., Lincoln, T., and Mattison, J. E., The HL7 clinical document architecture. *J. Am. Med. Inform. Assoc.* 8(6), 2001.
6. Huston, T., Security issues for implementation of E-Medical records. *Commun ACM* 44(9), 2001.
7. Ball, E., Chadwick, D. W., and Mundy, D., Patient privacy in electronic prescription transfer. *IEEE Secur. & Privacy Mag.* 1 (2):77–80, 2003.
8. Yang, Y., Han, X., Bao, F., and Deng, R. H., A smart-card-enabled privacy preserving E-Prescription system. *IEEE Trans. Inf. Technol. Biomed.* 8(1):47–58, 2004.
9. Um, K. S., Kwak, Y. S., Cho, H., and Kim, I. K., Development of an HL7 interface engine, based on tree structure and streaming algorithm, for large-size messages which include image data. *Comput. Meth. Programs Biomed.* 80:126–140, 2005.
10. Ping, X.-O., Ko, L.-F., Shang, R.-J., and Lai, F., Dynamic Messages Creation Method for HL7 Based Healthcare Information System. *HEALTHCOM 2007*, 2007.
11. Hsieh, J.-C., A novel DICOM-based 12-lead electrocardiogram documentary system. *J. Electrocardiol.* 40:S81–S87, 2007.
12. Dolin, R. H., Rishel, W., Biron, P. V., Spinosa, J., and Mattison, J. E., SGML and XML as Interchange Formats for HL7 Messages. *J. Am. Med. Inform. Assoc.* 1998.
13. McAuliffe, M. J., Lalonde, F. M., McGarry, D., Gandler, W., Csaky, K., and Trus, B. L., Medical image processing, Analysis and visualization in clinical research. *CBMS 2001. Proceedings. 14th IEEE Symposium*.:381–386, 2001.
14. Pereira, J., Lamelo, A., and Vazquez-Naya, I. M., Design and implementation of a DICOM PACS with secure access via Internet. *Proceedings of the 23 rd Annual EMBS International Conference*.:3724–3727, 2001.
15. Lu, R., Cao, Z., Chai, Z., and Liang, X., A simple user authentication scheme for grid computing. *Int. J. Netw. Secur.* 7 (2):202–206, 2008.
16. Chen, C.-L., Chen, Y.-Y., and Chen, Y.-H., Group-based authentication to protect digital content for business applications. *Int. J. Innovative Comput. Inf. Control* 5(5):1243–1251, 2009.
17. Zhang, L.-J., and Zhou, Q., CCOA: Cloud computing open architecture. *ICWS* 2009:607–616, 2009.
18. Lamport, L., Password authentication with insecure communication. *Commun. ACM*. 24, 1981.
19. Ateniese, G., Cutmola, R., de Meideiros, B., and Davis, D., Medical information privacy assurance: Cryptographic and system aspects. *Third Conference on Security in Communication Networks*, 2002.
20. Rash, M. C., Privacy concerns hinder electronic medical records. *The Business Journal of the Greater Triad Area*, April 4, 2005.
21. Yee, G., Korba, L., and Song, R., Ensuring privacy for E-health services, *In Proceedings of the First International Conference on Availability, Reliability and Security*, 2006.
22. Lin, C. H., and Lai, Y. Y., A flexible biometrics remote user authentication scheme. *Comput. Stand. Interfaces* 27(1):19–23, 2004.
23. Lee, N. Y., and Chiu, Y. C., Improved remote authentication scheme with smart card. *Comput. Stand. Interfaces* 27(2):177–180, 2005.
24. Wang, Y. Y., Liu, J. Y., Xiao, F. X., and Dan, J., A more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 32:583–585, 2009.

25. Yoon, E., and Yoo, K., An efficient password authentication schemes without using the server public key for grid computing. *GCC 2005, LNCS 3795*, 149–154, 2005.
26. Foster, I., and Kesselman, C., The grid: Blueprint for a new computing infrastructure. *2nd revised edition, Morgan Kaufmann Publishers In*, 2003.
27. Schneier, B., and Shostack, A., Breaking up is hard to do: Modeling security threats for smart cards. *Proceedings of USENIX Workshop on Smart Card Technology.* 175–185, 1999.
28. Stallings, W., Cryptography and network security, principles and practice. *3 rd Edition. Prentice Hall*, 2003.
29. Snyder, A. M., and Weaver, A. C., The e-logistics of securing distributed medical data. *INDIN 2003*. 207–216, 2003.
30. Rankl, W., and Effing, W., Smart card handbook. *John Wiley & Sons, ISBN 0-471-96720-3*, 1997.
31. Guthery, S. B., and Jurgensen, T. M., SmartCard Developer's Kit, Macmillan Technical Publishing. *ISBN 1-57870-027-2*, http://www.scdk.com, 1998.