A Non-Repudiated and Intelligent RFID Medication Safety Management System

Chin-Ling Chen, Yeong-Lin Lai, Chih-Cheng Chen, Chun-Yi Zheng & Li-Chih Chang


To link to this article: http://dx.doi.org/10.1080/10798587.2015.1126452

Published online: 08 Feb 2016.

Submit your article to this journal

Article views: 19

View related articles

View Crossmark data
A Non-Repudiated and Intelligent RFID Medication Safety Management System

Chin-Ling Chen, Yeong-Lin Lai, Chih-Cheng Chen, Chun-Yi Zheng, and Li-Chih Chang

ABSTRACT
Radio frequency identification (RFID) technology is a significant solution for homeland and cyber defense. Patient and cyber safety issues have been regarded as the most important quality policy of hospital management. Enhancing patients' safety and reducing medication errors are priority issues of the World Health Organization (WHO). With the increasing number of inpatients, medication safety is a major concern for doctors, pharmacists, and nurses. In this paper, we employ the RFID, digital certificate, and digital signature to enhance inpatient medication safety management. The proposed scheme can promptly present the information on the inpatient medication and improve the management of the inpatient medication safety. It not only enhances the quality of medical treatment but also provides non-repudiated and intelligent medication safety management. In our scheme, the automated medication dispensing machine (AMDM) is equipped with RFID tags and readers to improve the medication safety. The comprehensive analysis of the key performance indicator (KPI) of our scheme shows a significant 50% reduction in total cost and increased satisfaction on the part of hospital nurses.

1. Introduction
Medication safety has always been one of the most important issues in hospitals. In the processes involved in providing medication, medication errors inevitably occur, caused by doctors, pharmacists, and nurses. In hospitals, there are four medication stages including ordering, administration, transcribing, and dispensing. The percentages of the occurrence of medical errors for those stages are 56, 34, 6, and 4%, respectively (Bates et al., 1995). The Institute of Medicine (IOM) issued a report stating that a patient in a hospital is expected to be subjected to more than one medication error each day and that at least 1.5 million preventable medication errors occur in the United States each year (Bootman, Wolcott, Aspden, & Cronenwett, 2007). In order to reduce the medication errors and improve medication safety, a medication safety management system using modern information technology is necessary (Adhikari, Tocher, Smith, Corcoran, & MacArthur, 2014; Koutkias et al., 2010; Slagle et al., 2010).

Koutkias et al. used mobile base unit (MBU) and the sensors to propose a framework for personalized medication treatment management that could be employed to extend existing personalized chronic care systems (Koutkias et al., 2010). Slagle et al. designed a next generation system for child-centered medication management (Slagle et al., 2010). They have completed a working prototype of a scheduling system, a text-message-based alert and reminder system, and a medication administration record based on web-entered patient data. Adhikari et al. examined a medication management system (Adhikari et al., 2014). The existing information systems in hospitals cannot provide automated medication dispensing processes and real-time warning of medication errors. Most medication errors are related to the prescription errors of pharmacists and dispensing errors of nurses (Kamei, Teshima, Fukushima, & Nakamura, 2001; Kamei, Teshima, & Nakamura, 2000; Wang & Lin, 2008). Patient and cyber safety issues have been regarded as the most important quality policy of hospital management. Cyber attacks and warfare to the critical infrastructures, such as hospitals and power stations, are considered important threats to every country in the world (Pieters, Lukioso, Hadziosmanovic, & van den Berg, 2014).

Radio frequency identification (RFID) technology is one of significant solutions for cyber defense (Casoni & Paganelli, 2011; Rieback, Crispo, & Tanenbaum, 2006; Tran, Yousaf, & Wietfeld, 2010). RFID security is an important issue as for as cyber defense is concerned (Kambourakis, Gritzalis, & Park, 2010; Zhou, Xu, & Li, 2011). RFID is a promising technology for supply-chain, inventory management, battery exchange station, privacy protection, location tracking, and medical applications (Chang, Lai, & Chen, 2012; Chen, Lai, Chen, Deng, & Hwang, 2011; Dabrowski, Gromada, Moustafa, & Forestier, 2013; Jara, Zamora, & Skarmeta, 2010; Lai, Chang, Liu, Sun, & Yin, 2014; Lai & Chen, 2011; Lai & Cheng, 2014; Miyaji, Rahman, & Soshi, 2011). Chien et al. proposed a double RFID-based solution to enhance inpatient medication safety. They proposed one extended RFID authentication protocol for the on-line case and one RFID grouping-proof protocol for the off-line case (Chien, Yang, Wu, & Lee, 2011). However, security issues should be considered for inpatient medication safety (Huang & Ku, 2009). Generally speaking, the security issues should involve the following requirements: Confidentiality, authentication, integrity, and non-repudiation.
In this paper, we employ the key performance indicator (KPI), digital signature, digital certificate, and IT technology (such as RFID and mobile reader) to solve the security issues and enhance the medication safety. Our research uses the "Human-Computer Interface Design" to construct an efficient RFID preventive system for pharmacists. We use RFID technology to design a non-repudiated and intelligent medication safety management system with an automated medication dispensing machine (AMDM) to enhance the medication safety of patients.

The remainder of this paper describes and analyzes a non-repudiated and intelligent medication safety management as follows: Section 2 presents our proposed protocol, and the security requirements are analyzed in Section 3. The system demonstration and discussion are offered in Section 4. Our conclusions are presented in the final section.

2. System Scheme

The main processes and functions of our proposed scheme are shown in Figure 1. An introduction to the roles in the system is described as follows:

**Doctor (D):** After diagnosing the patient, the doctor issues the prescription.

**Health Information System (HIS):** It deals with the resources, devices, and methods required to optimize the acquisition, storage, retrieval, and use of information in health and biomedicine.

**Automated medication dispensing machine (AMDM):** Automated medication dispensing devices have been suggested as a technology that can assist in reducing the rates of medication errors when dispensing medication and tracking usage.

**Pharmacist (PM):** Pharmacists dispense prescription drugs to patients. They provide information about those drugs and help patients to understand the instructions their doctors or other health practitioners provided.

**Nurse (N):** The job of a nurse is to provide direct patient care by administering medication, caring for wounds, treating illnesses, and making sure patients get enough nutrients.

**Patient (P):** A patient is any recipient of medical attention, care, or treatment.

**Mobile Reader (MR):** A mobile reader can scan the tag of the drug package and get the medical messages.

**HIS server:** The HIS server issues the digital certificate and stores the related health information.

The process flow of the entire transaction system is described as follows:

1. **Step 1:** After the doctor diagnoses the patient, he/she will prescribe and sign the prescription, and the prescription will be stored in the database. The doctor uses his/her own private key to sign the prescription.

2. **Step 2:** After receiving the prescription, the HIS system sends the prescription to the AMDM. Each unit dose drug package (UDDP) will be attached an RFID tag and the prescription message will be stored in the tag’s memory.

3. **Step 3:** The pharmacist uses the private key to sign the prescription from the AMDM after checking the prescription.

4. **Step 4:** Once receiving the medicine from the pharmacy, the nurse uses the private key to sign the prescription via the mobile reader.

5. **Step 5:** The nurse checks if the doctor has changed the prescriptions via the HIS system.

6. **Step 6:** The nurse dispenses the drugs to the patient.

7. **Step 7:** The doctor patrols the inpatient ward and diagnoses the patient. If the doctor finds that the drugs are ineffective for the patient, he/she may update the prescription.

2.1. Notations

The following are the notations that will be used in our scheme.

- $SK_X$: the X’s private key
- $PK_X$: the X’s public key
- $Cert_X$: the X’s certificate issued by HIS server
- $ID_X$: the X’s identity
- $S_X(m)$: use X’s private key to sign a message m
V_X(m) use X’s public key to verify a message m
h() the one way hash function
Sig_X the X’s signature
DN drug name
t_1, t_2, t_3 the time stamps generated by doctor, pharmacist and nurse respectively
M the medication message, where M = (ID_p, ID_p, DN, Dose, Route, Time, t_1)
Msg_comp the message of the inpatient finishing taking medicine
A=B determines whether A is equal to B

The proposed scheme of the enhanced medication is divided into 4 phases: Registration phase, prescription phase, medication-dispensed phase, and prescription change phase. The transmitted messages are protected by a secure channel (such as secure socket layer, SSL) in a hospital private network.

2.2. Registration Phase

The tags, mobile readers, and all parties should register with the HIS server via the secure channel (SSL).

Step 1: First, the Doctor (D), Pharmacist (PM), Nurse (N), and Patient (P) should provide their identities to register with the HIS server as legal parties. Only after passing the identity authentication, the corresponding parties can obtain the certificates Cert_D, Cert_P, and Cert_N from the HIS server, respectively.

Step 2: The HIS server issues the key pairs (PK_D, SK_D), (PK_PM, SK_PM), and (PK_N, SK_N) to doctor, pharmacist and nurse respectively.

Step 3: All of the Mobile Readers (MR) and the inpatient tags should register with the HIS server, and the HIS server will store these legal readers and tags’ identity into the database.

2.3. Prescription Phase

In this phase, the doctor prescribes the prescription and sends it to the HIS server. The AMDM packs the medicine. Afterwards, the pharmacist checks the medicine contents, includes a signature for the prescription, and then sends the medication message with the signature to the nursing station. The overview of the prescription phase is shown in Figure 2.

Step 1: The doctor sends his/her Cert_D to the HIS server for verification. If the doctor passes the authentication, and diagnoses the patient, the doctor only uses his/her private key to sign the message M as follows: Sig_D = SD(M), where M = (ID_p, ID_p, DN, Dose, Route, Time, t_1). This signature Sig_D and M are then transmitted to the HIS for verification. And then according to the prescription M, the AMDM packs the medicine and attaches a tag which stores the prescription.

2.4. Medication-dispensed Phase

In this phase, the nurse should verify the pharmacist’s signature and check the “five rights” every time: right patient, right drug, right dose, right route and right time. Finally, the HIS server stores the medicine-taking record. The overview of the medication-dispensed phase is shown in Figure 3.
Step 1: First, the nurse sends his/her CertN to the HIS server for verification. If the nurse passes the authentication, the nurse uses the pharmacist’s public key and the mobile reader to access the drug database, and then checks whether the drug names and the quantity are correct. The nurse then uses the pharmacist’s public key to verify the received signature as follows: $V_{PM}(\text{Sig}_{PM}) = (M, t)$. If the above equation holds, the nurse uses the mobile reader to send the mobile reader’s certificate CertMR to the HIS server for verification. The HIS server verifies the mobile reader’s legality. The nurse then uses the mobile reader to read the information on the patient’s tag to obtain the identity IDN and check whether the IDN is stored in the database, as well as check the “five rights” every time. The nurse only then administers the medicine to the inpatient. After the inpatient finishes taking the medicine, the nurse has to make a signature as follows: $\text{Sig}_N = S_{SKD}(M', ID_N, t)$. Then the nurse sends the signature to the HIS server and proceeds to step 2.

Step 2: After receiving $(\text{Sig}_N, M_{\text{comp}}, M, ID_N, t_3)$, the HIS server will use the nurse’s public key to verify the correctness of the signature as follows: $V_N(\text{Sig}_N) = (M_{\text{comp}}, M, ID_N, t_3)$. Then the HIS server will verify the correctness of the signature as follows: $V_N(\text{Sig}_N) = (M_{\text{comp}}, M, ID_N, t_3)$ and then record the result.

### 2.5. Prescription Change Phase

The nursing staff should check the medication at three checkpoints: Pharmacy, nursing station and sickroom. If the inpatient has any unusual physical reaction after taking the medicine, the nurse will notify the doctor. If the doctor thinks it is necessary to change the prescription after evaluating and diagnosing the patient, the doctor will renew the prescription $M'$ and make a signature as follows: $\text{Sig}_D = S_{SKD}(M')$ and then send $(\text{Sig}_D, M')$ to the pharmacist.

Step 2: After receiving $(\text{Sig}_D, M')$, the pharmacist will go on the Step 2 of the prescription phase.

### 3. Security Analysis

In order to simplify the medical service process, enhance the conveniences of taking medical treatment, and reduce ordinary people’s burden, and achieve twice the result with half the effort, we designed a medication safety management protocol. In this section, we analyze the proposed scheme to verify if it satisfies the requirements of medical safety as described in Section 1.

#### 3.1. Confidentiality Issue

All the parties should register with the HIS server via the secure channel (SSL). The HIS server issues the key pairs $(PK_{PM}, SK_{PM})$, $(PK_{MR}, SK_{MR})$, and $(PK_{N}, SK_{N})$ to doctor, pharmacist, and nurse respectively. Any party can use the public key $PK_{PM}$ to encrypt the confidential information to protect the information. On the other hand, the receiver can use the private key $SK_{PM}$, $SK_{MR}$ and $SK_{N}$ to decrypt the encrypted information. The intruder cannot read the encrypted message from the ciphertext in our scheme. Since the transmitted messages are protected by secure channel (SSL) in the hospital’s private network; thus, the attackers cannot intercept the prescription contents. Our scheme achieves confidentiality.

#### 3.2. Authentication Issue

It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else. In our scheme, before starting one’s job, the doctors, pharmacist, nurses and mobile reader should login to the HIS server and sends his/her own certificate (CertD, CertPM, CertMR, CertN) to request authentication. Simultaneously, the corresponding nursing staff’s signature (SigD, SigPM, and SigN) should be verified correctly such that the procedure can continue. The authentication mechanism of the identity and message legality are designed in our scheme. Thus, the authentication can be achieved.
3.3. Integrity Issue

It should be possible for the receiver of a message to verify that it has not been modified in transmission and that an intruder cannot substitute a false message for a legitimate one. The receiver can use the sender’s public key to verify the received message. For example, in the prescription phase, the doctor’s signature $\text{Sig}_D = S_D(M)$ can be verified by the doctor’s public key as $V_D(\text{Sig}_D) \land M$. Thus, the pharmacist can ensure the integrity of the prescription. For the same reason, the pharmacist’s signature $\text{Sig}_{PM} = S_{PM}(M, t_2)$ can be verified by the pharmacist’s public key as $V_{PM}(\text{Sig}_{PM}) \land (M, t_2)$. In the medication-dispensed phase, the nurse can ensure the integrity of the prescription. After that, the server can verify the integrity by the following equation $V_s(\text{Sig}_n) \land (M, ID_n, t_3)$. In the same way, if the doctor should change the prescription, he/she should send his/her signature $(\text{Sig}_D, M)$ to the pharmacist for verifying the integrity. Once the transmitted messages are modified, the verification equation will not hold. Thus, our scheme has achieved the integrity.

3.4. Non-repudiation Issue

Non-repudiation means that the request party provides related proof for the other party to verify so that each transaction will not suffer from any false denials. In the implementations, the digital signature is often used to solve the non-repudiation issue. With each party holding related proof issued by the opposite party, as listed in Table I, no one will suffer from repudiation during the transaction. In our scheme, once the related roles completed their task, they should make their signatures and send them to the opposite party for verification.

4. System Demo and Discussion

The AMDM in the market has only the barcode function. There is no RFID AMDM in the market. In this paper, the RFID AMDM is developed, as shown in Figure 4. The advantages of the RFID AMDM with respect to the barcode AMDM include automatic identification, mass processing, and no line-of-sight limitations. The proposed RFID AMDM has been implemented at hospitals to improve the patient medication safety. Figure 5 shows the structure diagram of the RFID AMDM.

There are three parts in the RFID AMDM: (1) RFID Reader, (2) RFID tag, and (3) UDDP. Figure 6 is the integration system of the RFID AMDM. The prescription information of the tags in the AMDM is read out by the reader and sent to the integration system by the 2.45-GHz RFID.

In this paper, the security protocol for the RFID AMDM is designed. The RFID tags are put into the UDDPs. The kernel program of AMDM is modified and the prescriptions of the drugs are written into the tags of the UDDPs.

The comprehensive analysis of the KPI of the proposed system is indicated in Table II. The results show that the manpower growth rate is reduced by 50%, the medication errors by 70%, and the total cost by 50%. Satisfaction on the part of the nurses of hospitals and the tracking of the clinical path are greatly increased.

The medication dispensing machine needs plenty of manpower to do the correction work, which wastes time and manpower. Before using the RFID system, the average manpower requirement is up to four people. After the introduction of the RFID system, the manpower requirement will reduce to two people, meaning that the cost is accordingly reduced by 50%. The hand-packed medication system needs proof-reading, and the error rate is about 70%, which is provided by the hospital.

In Table III, we make a comparison of the related medication safety management systems. Basically, these researches (Adhikari et al., 2014; Koukias et al., 2010; Slagle et al., 2010) do not focus on the comprehensive analysis of KPI, security analysis, and non-repudiation proof issues. But these issues are important for medication safety management system. In this paper, we propose a novel solution.
Disclosed statement
The authors declared that there is no conflict of interest regarding the publication of this paper.

Notes on contributors
Chin-Ling Chen was born in Taiwan in 1961. He received a B.Sc. degree in Computer Science and Engineering from Feng Cha University in 1991 and an M.Sc. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005, respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at Chunghwa Telecom Co., Ltd. He is currently a professor in the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security, and electronic commerce.
commerce. Dr. Chen has published over 60 articles on the above research fields in SCI/SSCI international journals.

Yeong-Lin Lai received the Ph.D. degree from the Institute of Electronics, National Chiao Tung University, Taiwan, in 1997. He is currently a Professor and the Chairman of the Department of Mechatronics Engineering, National Changhua University of Education, Taiwan. He is also the Director of the Mechatronic Integration and System Control Research Center, National Changhua University of Education. He was the Guest Editor of VLSI Design. His research interests include IoT, RFID, intelligent systems, and optoelectronic technologies. Dr. Lai received the Excellent Ph.D. Dissertation Award for Industries and the Outstanding Educator Award from Ministry of Education, Taiwan. He received the Creation and Invention Awards and the Academic Research Award from the Foundation of National Changhua University of Education. Dr. Lai received the National Academic Award of IIP. He received the Superior Mentor Award, Outstanding Faculty Teaching Award, and Outstanding Faculty Research Award of National Changhua University of Education. Dr. Lai is a Fellow of the ElectroMagnetics Academy and an International Fellow of Chinese Innovation and Invention Society.

Chih-Cheng Chen is an Assistant Professor in Department of Health Policy and Management, Chung Shan Medical University. He earned a Master and Ph.D. Degrees in Department of Mechatronics Engineering from National Chunghua University of Education in 2005 and 2011 respectively. He has been practicing the RFID application system in many fields such as the patrol system and the long-term care of elders. His research interests include mobile technology and RFID applications.

Chun-Yi Zheng received the B.S. and M.S. degrees from Department of Electronics Engineering, Feng Chia University, Taichung, Taiwan, in 2001 and 2003, respectively. He received the Ph.D degree from Department of Mechatronics Engineering, National Chunghua University of Education, Changhua, Taiwan, in 2012. His research interests include high frequency integrated devices, RF circuits, and MMICs design.

Li-Chih Chang is currently working toward the Ph.D. degree at the Department of Mechatronics Engineering, National Chunghua University of Education, Taiwan. He had industrial experience in the fields of RFID system design, software-hardware co-design, antenna design and system engineering. His research interests include RFID systems, microwave engineering, and system integration.


References


Downloaded by [Chaoyang University of Technology] at 17:58 06 June 2016