Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 752412, 12 pages
http://dx.doi.org/10.1155/2013/752412

Research Article

Secure e-Health System on Passive RFID: Outpatient Clinic and Emergency Care

Kou-Hui Yeh,[1] Nai-Wei Lo,[2] Tzong-Chen Wu,[2] and Chieh Wang[2]

[1] *Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan*
[2] *Department of Information Management, National Taiwan University of Science and Technology, Taipei 106, Taiwan*

Correspondence should be addressed to Kou-Hui Yeh; khyeh@mail.ndhu.edu.tw

Received 11 July 2013; Accepted 8 October 2013

Academic Editor: YingJiu Li

In recent years, many researches have demonstrated several RFID-based solutions to enhance patient medication safety and avoid human errors. Although RFID-based procedure is more efficient than traditional process, patient's information may be attacked (or stolen) during the data transmission period. This will cause inappropriate medication use and medical errors. In this paper, we introduce a robust RFID-based e-Health system which strengthens the system security and protects the patient's privacy as well. In addition, our e-Health system can provide better efficiency of outpatient clinic procedure and emergency care procedure in hospital environment.

1. Introduction

Recently, RFID technology has promptly been adopted to enhance the communication efficiency in hospital environment. As a result, the development of a broad range of new electronic-Health (e-Hhealth) applications has emerged; these are, for example, patient safety and medication management [1–8], ubiquitous healthcare systems [9], inpatient-care systems [10, 11], autotracking clinical interventions [12], and electronic-health records [13]. All of these applications promise patient, nurse, doctor, and administrator to efficiently access relevant health information, enhance the quality of patient care, reduce healthcare errors, increase collaboration, and encourage the adoption of healthy behaviors.

Since new and efficient health information technologies realize the implementations of diverse e-Health services, the system security and patient (or hospital administrator) privacy have been focused by human right organizations, governments, and research community. The essential security elements for e-Health systems are data confidentiality, data integrity, service availability, accountability, and nonrepudiation of information. Meanwhile, personal privacy is the fundamental human right, and basic privacy protection principles are universal. Information privacy concerns exist wherever personally identifiable information is collected, processed, stored, and disclosed. In the following, we present basic information securities and privacy principles [14, 15].

(i) Patient data must be processed fairly and used for specified and lawful purposes.

(ii) Unauthorized or unlawful processing of patient data must be efficiently measured and dealt with.

(iii) Accountability should be guaranteed.

(iv) The consent for data processing should be freely given.

(v) Patient data must not be exploited without adequate level of protection.

(vi) Patient data must be adequate, relevant, and not excessive in relation to the purpose for which it is processed.

(vii) Patient data processed for any purpose must not be kept for longer than is necessary for that purpose.

Based on the previous properties, we argue that data processing should be legal and meet regulatory and contractual obligations. In addition, the patient's health data (or personal examination report) is sensitive and, however, usually identifiable. Therefore, personal health data must be well protected

to fulfill the above mentioned security and privacy principles; for example, the international standard ISO 27799 [16] can be a solution for security management of health information.

In this paper, we focus on RFID technology integrated with the process for medicine error reduction, patient (and inpatient) safety enhancement, and health care management. In particular, the issues of performance efficiency, system security, and patient privacy will be thoroughly investigated. We intend to deliver a patient privacy-aware e-Health system based on passive RFID to simultaneously enhance system efficiency and patient privacy.

2. Related Work

In 2007, Agrawal and Johnson [13] proposed a so-called Hippocratic Database which enables enterprises to comply with privacy and security laws without impeding the management of personal health information. To secure electronic health records, their proposal involves five techniques: (1) active enforcement of fine-grained data disclosure policies, (2) efficient auditing of past database access, (3) privacy-aware data mining, (4) deidentification of personal health data, and (5) robust information sharing. Later, to deal with the difficulty of securely manage the aggregation of health related data from various IT environments, Boyd et al. [10] developed a honest broker mechanism to maintain privacy for patient care and academic medical research. The honest broker can offload the burden of housing identifiable data elements of protected health information as well as manage date transfer between clinical and research systems.

In 2010, two tag coexistence schemes had been proposed by Chien et al. [2] to eliminate medication errors and enhance patient's safety. An online-based administration protocol and an offline version were proposed, respectively. However, the two proposed mechanisms did not consider important security and privacy issues [5]. Moreover, the feasibilities of these two schemes are doubted as only protocol designs are provided. That is, without any demosystem implementations, the practicability of these two protocols still has space for improvement. Later, Peris-Lopez et al. [4] implemented an Inpatient Safety RFID System (IS-RFID) which takes into account the information technology infrastructure of real hospital environment and completely covers the whole drug administration process. The system efficiency can be guaranteed as only lightweight cryptography modules such as random number generator and exclusive-or operations are exploited in IS-RFID. However, the insecurity of IS-RFID has been pointed by Yen et al. [7] in 2012.

Next, Yu et al. [8] developed a mechanism utilizing only simple logic gates, for example, AND, XOR, and ADD bitwise operations, to construct a secure e-Health system. Their scheme is efficient as it does not need any complicated cryptography modules. However, Wu et al. [6] have pointed the security vulnerability, that is, impersonation attacks, of their protocol. A lightweight binding proof protocol is then proposed to overcome the weakness identified in Yu et al.'s scheme. Next, Lin and Zhang [3] introduced an Elliptic Curve Cryptography- (ECC-) based solution to prove the coexistence of multiple RF tags and improve patient's drug security. Yet, as the heavy computation cost of ECC module cannot be afforded on resource-constrained RF tags, there exists a doubt on the feasibility of Lin and Zhang's scheme.

A wireless autotracking system for clinical intervention, such as drug administrations and blood tests at the patient bedside, is proposed by Ohashi et al. [12]. The system can authenticate patients and nurses, confirm medications, and provide relevant information based on the clinical situation and personal location. According to the evaluation, the proposed system can reduce significant medical errors and nurse workload with high efficiency. Najera et al. [11], in their study, first analyzed the case of a medical equipment tracking system for healthcare facilities enabling both real-time location and theft prevention. The authors then provided a solution for care and control of patients in a hospital environment based on passive RFID. Lo et al. [9] proposed a decision support systems, called the Ubiquitous Context-aware Healthcare Service System (UCHS), which uses microsensors integrated with RFID technology to sense user's life vital signal, such as electrocardiogram, heart rate, respiratory rate, blood pressure, blood sugar, and temperature and light. The UCHS is built upon an integrated service platform in which medical experts' knowledge and all position and negative influence of therapy are inferred via semantic network.

In 2013, Köstinger et al. [17] developed a ward round system with mobile smartphones in which Near Field Communication (NFC) technology is utilized to explore new ways of interaction. The system achieves patient identification via NFC tags. In their proposed scenario, when the patient arrives in the hospital, he/she will get a NFC wristband. This wristband carries information about their real identity, and in the following the hospital staff will utilize NFC-enabled mobile device to retrieve the information from the wristband. In 2013, Ajami and Carter [18] analyzed the advantages and disadvantages of adopting RFID in emergency room. In their study, the advantages are as follows: improving patient's safety, eliminating or reducing clinical errors, and decreasing medical errors to improve patient safety and save lives. However, the authors argued that the cost of healthcare system is still high for service providers. In addition, the privacy, legality, and security are the key problems needed to be solved in e-Health environment. Safdari et al. [19] have pointed that the organization needs to concentrate on the following privacy and security issues: (1) only authorized users can access sensitive information, (2) the integrity and accuracy of data should be guaranteed, and (3) the hospital needs to protect the patient information. In order to achieve these three goals, the authors provided a security solution, that is, anonymous transmission at tag side. That is, user can retrieve the unique tag ID without revealing the relationship between the object and the tag ID.

3. The Proposed e-Health System: Novel Outpatient Clinic Process and Emergency Care Procedure

In this section, we introduce an efficient and patient privacy-aware e-Health system based on passive RFID. We assume that the tags are able to perform PRNG function and *XOR*

operation. Note that the output of PRNG function must be at least 96 bits for system security. In addition, 128 bits, 256 bits, and 512 bits are acceptable bit lengths also. Before we present the details of our proposed system, it is important to define the adversary model of our system environment. In 2001, Canetti and Krawczyk [20] demonstrate two adversary models: the unauthenticated-links model and the authenticated-links model. In the unauthenticated-links model, there exists a probabilistic polynomial-time attacker *Eve* who controls the communication links and the schedule of protocol events. *Eve* has the abilities, such as message modification, transmission injection, and the protocol event rescheduling. In general, *Eve* is able to send the following queries.

(i) Session-state reveal: *Eve* submits a party's identity and an incomplete session identifier to learn the state of the session. Note that *Eve* cannot learn any long-term secrets or master keys held by the party.

(ii) Session-key query: *Eve* submits a party's identity and a complete session identifier to learn the session key in the intended session.

(iii) Session expiration: *Eve* submits a party's identity and a complete session identifier for letting the simulator erase the session key and related session states.

(iv) Party-corruption query: *Eve* decides to corrupt a party and learns all secrets or master keys of the party and then completely controls the party.

On the other hand, the authenticated-links model is applicable to the case that the attacker does not have the capability to inject or modify the transmitted messages. Under the previous assumptions, we then define our adversary model into two types: type I model and type II model. In type I model, a probabilistic polynomial-time attacker *Eve* controls the communication links and the schedule of protocol events. In addition, *Eve* is able to perform message modification, transmission injection, and the protocol event rescheduling with oracle queries such as session-state reveal, session-key query, session expiration, and party-corruption query. Mapping to the hospital environment, *Eve* can be the roles of nurse, doctor, examiner, and system administrator who are legitimate and verified in our system and possess the authorization of some system functionalities. In type II model, there exists a probabilistic polynomial-time attacker *Eve*, who is restricted to delivering messages generated from one of the communicating parties to the other one. Mapping to the hospital environment, this kind of attacker can be an outsider who does not have the capability to inject or modify the transmitted messages. Note that an insider without any entity verification or function authorization can be an example also. In addition, all the adversaries can simply obtain an RF reader and smart card reader to help his/her cryptanalysis.

In the following, we will demonstrate the details of our system. The proposed system consists of two newly designed processes on passive RFID that are (1) outpatient clinic process and (2) emergency care procedure, which accelerate and improve hospital administration and patient services.

3.1. New Outpatient Clinic Process on Passive RFID. This subsection presents a novel outpatient clinic process adopting passive RFID technology. The major procedures are illustrated in Figure 1 in which eight processes, that is, parts A to H, are presented. First, the part A's purpose is to bind patient's identity with a temporarily issued RFID tag in which patient's smart card will be utilized to encrypt (or protect) tag's information. Afterward, an anonymous authentication mechanism will be adopted in part B when doctors require confirming patient's legitimacy. Suppose that the patient is diagnosed with needing further examination tracking or condition tracking. Part C will be informed to maintain the record of the doctor's diagnosis. Next, in part D the inspector will reconfirm patient's legitimacy via patient's tag, and generates evidences in part E. Lab processes bind the drug jar and patient's identity, and store the binding information in backend server via part F. Finally, parts G and H are utilized for medication administration. In the following, we illustrate the details of these eight procedures.

3.1.1. Part A: RFID Tag Issuing & Bind It with ID Card. In part A (Figure 2), the main target is to bind RF tag Tag_i and patient's identity, where the patient's smart card is used for data encryption. In this part, the tag and the patient's identity will be bound in backend server.

(A1) Patient's tag $\text{Tag}_i \rightarrow$ Reader: PID_i.

Patient's smart card $\rightarrow$ SCReader: k_i.

In action (A1), the RF reader inquiries the Tag_i and retrieves the unique identity PID_i of Tag_i. Note that PID_i can be the patient's temporary and unique identity. At the same time, the smart card reader (SCReader) scans the user's smart card to retrieve the patient's secret key k_i. Note that the user's smart card can be any type of smart card which possesses the user's secret key such as *Citizen Digital Certificate* [21] or *Mifare Card* [22].

(A2) Reader $\rightarrow$ SCReader: PID_i.

(A3) Data encryption for PID_i.

The RF reader transfers PID_i to SCReader for encryption in action (A2). When SCReader receives the PID_i, it exploits the patient's secret key k_i to encrypt PID_i in action (A3), that is, $x_i = \text{AES}_{k_i}(\text{PID}_i)$, where AES represents *Advanced Encryption Standard* [23].

(A4) SCReader $\rightarrow$ Reader: Pseu_i, x_i.

(A5) SCReader $\rightarrow$ Backend Server: Pseu_i, x_i.

Afterward, SCReader generates a pseudonym Pseu_i connected to value x_i and sends $\{\text{Pseu}_i, x_i\}$ to RF reader which then writes the received value $\{\text{Pseu}_i, x_i\}$ to Tag_i to replace the original value PID_i in action (A4). Meanwhile, SCReader transmits $\{\text{Pseu}_i, x_i\}$ to the backend server. So far, both the tag Tag_i and the backend server maintain the values Pseu_i and x_i.

3.1.2. Part B: Examined and Diagnosed by a Doctor (Anonymous Authentication). In part B (Figure 3), the patient gets

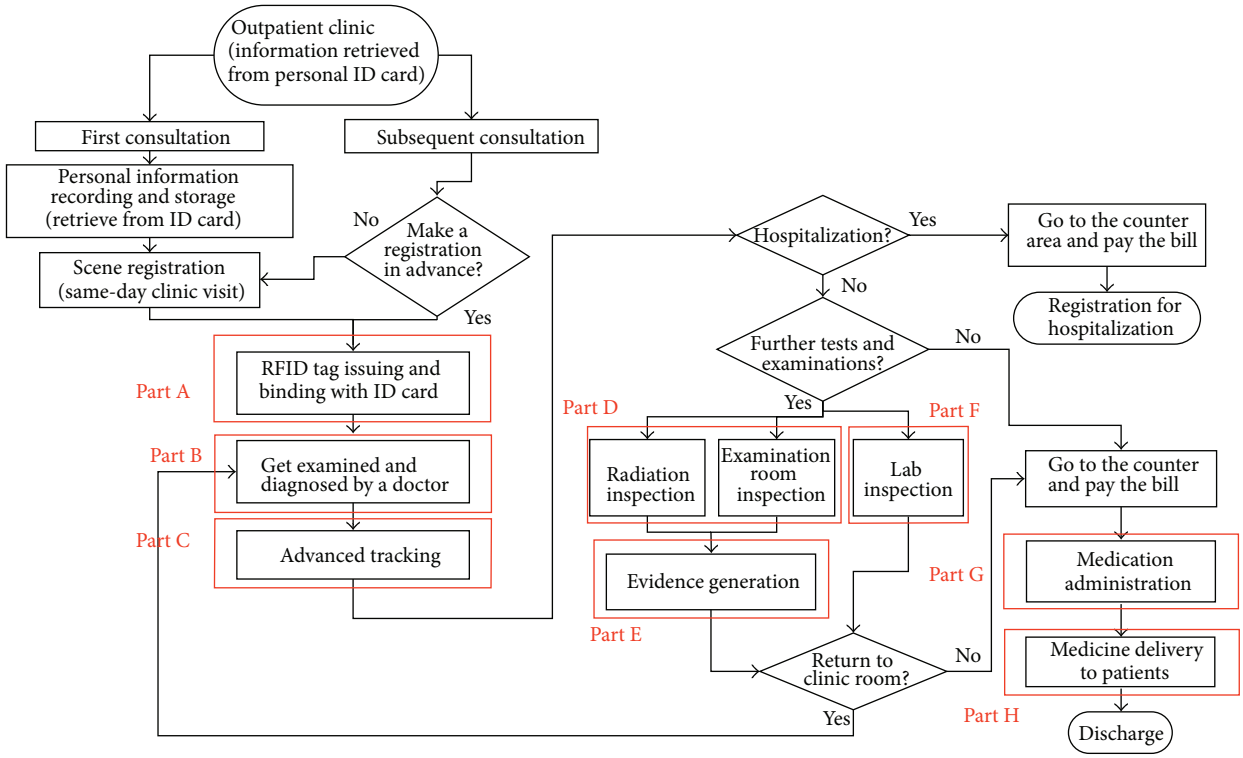

Figure 1: The proposed outpatient clinic process based on passive RFID.

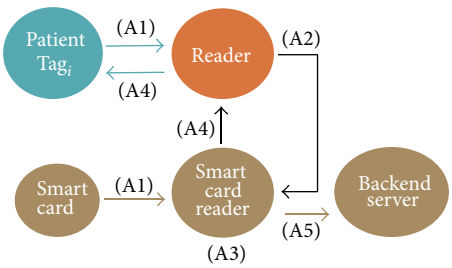

Figure 2: The part A of the new outpatient clinic process.

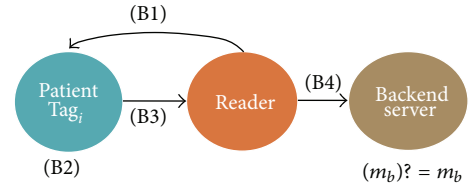

Figure 3: The part B of the new outpatient clinic process.

examination and diagnosis from a doctor. During the procedures, an anonymous authentication is invoked to protect patient's privacy.

(B1) Reader $\rightarrow$ Tag$_i$: n_r^b.

(B2) Tag$_i$: $m_b = x_i \oplus \text{PRNG}(n_r^b \oplus x_i)$.
First, the doctor utilizes the RF reader to send a newly generated random number n_r^b to the patient's tag Tag$_i$ in action (B1). With this random number n_r^b, Tag$_i$ computes $m_b = x_i \oplus \text{PRNG}(n_r^b \oplus x_i)$ in action (B2).

(B3) Tag$_i$ $\rightarrow$ Reader: Pseu$_i$, m_b, n_r^b.

(B4) Reader $\rightarrow$ Backend Server: Pseu$_i$, m_b, n_r^b.

Next, in action (B3) Tag$_i$ responds the message (Pseu$_i$, m_b, n_r^b) to the RF reader which soon forwards (Pseu$_i$, m_b, n_r^b) to the backend server. Finally, the backend server exploits Pseu$_i$ to efficiently retrieve the value x_i and computes $x_i \oplus \text{PRNG}(n_r^b \oplus x_i)$. Then, the backend server verifies the correctness of m_b in action (B4), that is, whether the received value m_b equals to the calculated value $x_i \oplus \text{PRNG}(n_r^b \oplus x_i)$ or not. If this verification is passed, the legitimacy of patient can be confirmed without revealing his/her identity. Note that in this stage, Pseu$_i$ is used to gain system efficiency. Since Pseu$_i$ is a random nonce temporarily representing the patient's primary key during the search in the backend database, Pseu$_i$ will not reveal any information regarding the patient's privacy. For this reason, this design will not influence the system security.

3.1.3. Part C: Further Tracking. Once the patient needs further physical examinations, part C (Figure 4) will be launched. The doctor firstly encrypts and stores the patient's diagnosis (or inspection report) with a unique number P in the backend server. The patient then utilizes the following processes to record the reference number of his/her diagnosis (or inspection report) in his/her own tag Tag$_i$.

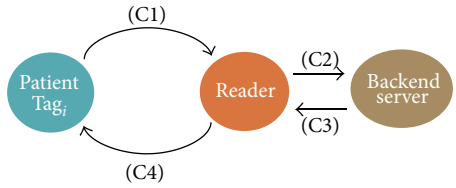

Figure 4: The part C of the new outpatient clinic process.

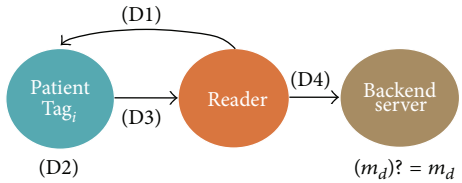

Figure 5: The part D of the new outpatient clinic process.

(C1) $\text{Tag}_i \rightarrow$ Reader: Pseu_i, n_t^c.

(C2) Reader $\rightarrow$ Backend Server: Pseu_i, n_t^c.

First of all, Tag_i generates a random number n_t^c and sends $\{\text{Pseu}_i, n_t^c\}$ to the RF reader in part (C1). Secondly, RF reader forwards $\{\text{Pseu}_i, n_t^c\}$ to the backend server in Part (C2).

(C3) Backend Server $\rightarrow$ Reader: m_c.

(C4) Reader $\rightarrow \text{Tag}_i$: m_c.

Thirdly, the backend server retrieves the value x_i via Pseu_i and computes $m_c = \text{PRNG}(n_t^c \oplus x_i) \oplus P$. Then, the backend server transmits $m_c = \text{PRNG}(n_t^c \oplus x_i) \oplus P$ to the RF reader in part (C3). Finally, the reader sends m_c to Tag_i which then derives the number P with the received value m_c, that is, $P = m_c \oplus \text{PRNG}(n_t^c \oplus x_i)$. After that, Tag_i possesses the values P.

3.1.4. Part D: Examination Room & X-Ray Process (Anonymous Authentication). Once the patient obtains the reference number, that is, P, of the diagnosis (or inspection report), the next stage is performed, that is, examination procedure or *X-ray* process. In part D (Figure 5), the inspector at each substage will reconfirm patient's legitimacy via patient's tag Tag_i.

(D1) Reader $\rightarrow \text{Tag}_i$: n_r^d.

First, the RF reader generates a random number n_r^d and sends it to Tag_i in action (D1).

(D2) Tag_i: $m_d = (x_i \parallel P) \oplus \text{PRNG}(n_r^d \oplus x_i)$.

(D3) $\text{Tag}_i \rightarrow$ Reader: Pseu_i, m_d.

(D4) Reader $\rightarrow$ Backend Server: $\text{Pseu}_i, m_d, n_r^d$.

Second, Tag_i calculates $m_d = (x_i \parallel P) \oplus \text{PRNG}(n_r^d \oplus x_i)$ in action (D2) and transmits $\{\text{Pseu}_i, m_d\}$ to the RF reader in action (D3). Finally, in action (D4) the reader forwards $\{\text{Pseu}_i, m_d, n_r^d\}$ to the backend server which then retrieves x_i and P via Pseu_i and verifies the correctness of m_d. That is, if the received value m_d, equal to the calculated value $(x_i \parallel P) \oplus \text{PRNG}(n_r^d \oplus x_i)$, the legitimacy of this patient can be proved.

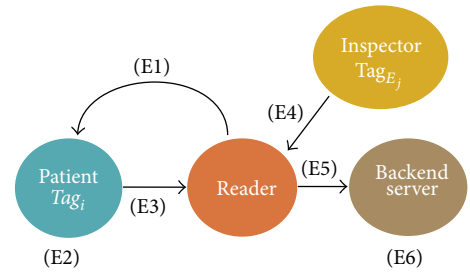

Figure 6: The part E of the new outpatient clinic process.

3.1.5. Part E: Examination Room & X-Ray Process (Evidence Generation). Once the legitimacy of the patient is confirmed, the patient will get the service from examination or *X-ray* rooms. In this stage, we will generate a corresponding evidence (or proof) for further verification if any. That is, part E (Figure 6) will create an evidence for the patient's inspection procedure.

(E1) Reader $\rightarrow \text{Tag}_i$: n_r^e, t_i.

(E2) Tag_i: $m_e = (x_i \parallel P \parallel t_i) \oplus \text{PRNG}(n_r^e \oplus x_i)$.

(E3) $\text{Tag}_i \rightarrow$ Reader: Pseu_i, m_e.

First, the RF reader generates a random number n_r^e and sends (n_r^e, t_i) to Tag_i in action (E1), where t_i is the current timestamp. Second, Tag_i computes $m_e = (x_i \parallel P \parallel t_i) \oplus \text{PRNG}(n_r^e \oplus x_i)$ in action (E2) and then sends $\{\text{Pseu}_i, m_e\}$ to the RF reader in action (E3).

(E4) $\text{Tag}_{E_i} \rightarrow$ Reader: n_r^e, t_i.

(E5) Reader $\rightarrow$ Backend Server: $\text{Pseu}_i, m_e, E_i, n_r^e$.

(E6) Backend server: digital signature of $\{\text{Pseu}_i, m_e, E_i, n_r^e\}$.

Next, the tag Tag_{E_i} sends E_i to the RF reader in action (E4), where E_i is the inspector's identity maintained in the inspector's tag Tag_{E_i}. Then, the reader transfers the message $\{\text{Pseu}_i, m_e, E_i, n_r^e\}$ to the backend server in action (E5). Finally, the backend server will generate a digital signature of $\{\text{Pseu}_i, m_e, E_i, n_r^e\}$ as an evidence for further verification. This proof will be useful once possible medical disputes happen. Note that the technique of digital signature can be RSA [24] or DSA [25].

3.1.6. Part F: Lab Process. The purpose of lab process (Figure 7) is to bind the target blood jar and patient's identity in the backend server. That is, we intend to correctly identify the source, that is, the target patient, of the target blood jar.

(F1) Reader $\rightarrow \text{Tag}_i$: n_r^f.

Reader $\rightarrow \text{Tag}_{C_j}$: n_r^f.

(F2) Tag_i: $m_f = x_i \oplus \text{PRNG}(n_r^f \oplus x_i)$.

(F3) $\text{Tag}_i \rightarrow$ Reader: Pseu_i, m_f.

Firstly, in action (F1) the reader generates a random number n_r^f and sends it to Tag_i and Tag_{C_j} embedded

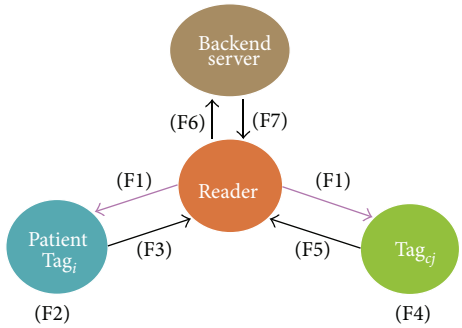

FIGURE 7: The part F of the new outpatient clinic process.

on the target blood jar. Then, Tag_i computes $m_f = x_i \oplus \text{PRNG}(n_r^f \oplus x_i)$ in the subpart (F2) and issues $\{\text{Pseu}_i, m_f\}$ to the RF reader in the subpart (F3).

(F4) Tag_{C_j}: $m'_f = n_r^f \oplus C_j$.

(F5) $\text{Tag}_{C_j} \rightarrow$ Reader: m'_f.

Next, Tag_{C_j} sends a computed value $m'_f = n_r^f \oplus C_j$ to the reader in actions (F4) and (F5), respectively, where C_j is the identity of Tag_{C_j}.

(F6) Reader $\rightarrow$ Backend Server: $\text{Pseu}_i, m_f, n_r^f, C_j$.

(F7) Backend server: verify the legitimacy of the patient.

The RF reader then retrieves C_j from m'_f and transfers the message $\{\text{Pseu}_i, m_f, n_r^f, C_j\}$ to the backend server in the subpart (F6). Finally, in action 7 the backend server retrieves x_i via Pseu_i, and verifies the legitimacy of the patient. That is, the backend server examines whether the computed $x_i \oplus \text{PRNG}(n_r^f \oplus x_i)$ equals to the received m_f or not. If it holds, the server appends the information C_j to the patient's record.

3.1.7. Part G: Medication Administration. Part G (Figure 8) discusses the medication administration which is able to confirm the correctness of each target drug suggested by the doctor. In brief, this process will verify if current medicine jar is in the drug list suggested by the doctor; if yes, the medicine (or drug) in the jar will be taken into the patient's unit dose medication. Note that since the doctor's diagnosis has been completed in parts B and C, the suggested medicine list is maintained in the backend server. This list corresponds with the patient's information x_i.

(G1) Backend Server $\rightarrow$ Reader: n_r^g.

First, the backend server generates a random number n_r^g and transmits n_r^g to the RF reader (e.g., the action (G1)).

For each tag M_m, $m = 1, 2, \ldots, n$.

Reader $\rightarrow$ Tag M_m: n_r^g.

Tag M_m: $m_g = \text{PRNG}(n_r^g \oplus n_t^g) \oplus \text{ID}_{M_m}$.

Tag $M_m \rightarrow$ Reader: n_t^g, m_g.

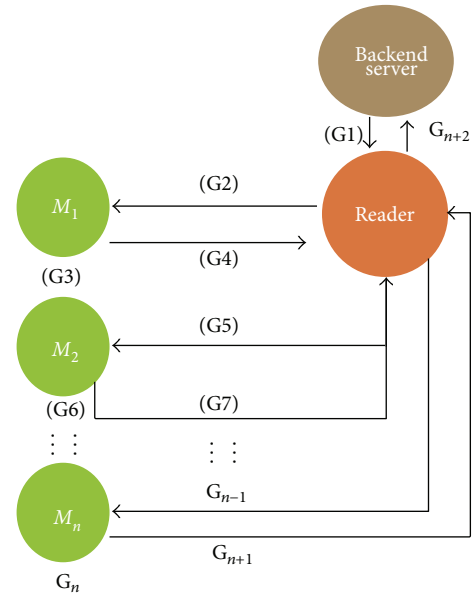

FIGURE 8: The part G of the new outpatient clinic process.

Second, the reader forwards n_r^g to the tag M_m embedded on each medicine jar (e.g., the subpart (G2)), where $m = 1, 2, \ldots, n$. Third, the tag M_m computes $m_g = \text{PRNG}(n_r^g \oplus n_t^g) \oplus \text{ID}_{M_m}$ and sends (n_t^g, m_g) to the reader, where n_t^g is a random number generated by the tag M_m (e.g., the action (G3) and (G4)).

(G_{n+2}) Reader $\rightarrow$ Backend Server: n_r^g, all (n_t^g, m_g)s.

Next, the reader forwards n_r^g with all (n_t^g, m_g)s to the backend server which then verifies all the received values m_gs to check if ID_{M_m} is in the suggested list. If the verification holds, the server will inform the pharmacist to put the drug into unit-dose medication. Finally, the backend server calculates $m_{\text{UD}} = \text{ID}_{M_m} \oplus x_i$, and stores m_{UD} in both the backend server and tag D_i embedded on the patient's medicine bag.

3.1.8. Part H: Pick Up the Medicine (Matching Verification). In part H (Figure 9), we present the matching verification in Outpatient Department (OPD) dispensary when collecting medicine.

(H1) Reader $\rightarrow$ Tag_i: n_r^h.

Reader $\rightarrow$ Tag D_i: n_r^h.

(H2) $\text{Tag}_i \rightarrow$ Reader: Pseu_i, $m_t = (x_i) \oplus \text{PRNG}(n_r^h \oplus x_i)$.

Tag $D_i \rightarrow$ Reader: $m_h = (m_{\text{UD}}) \oplus \text{PRNG}(n_r^h \oplus m_{\text{UD}})$.

First, in the subpart (H1) the reader generates a random number n_r^h and sends n_r^h to both Tag_i and the tag D_i embedded on the patient's medicine bag. Second, Tag_i sends Pseu_i and $m_t = (x_i) \oplus \text{PRNG}(n_r^h \oplus x_i)$ to the RF reader, and D_i transmits $m_h = (m_{\text{UD}}) \oplus \text{PRNG}(n_r^h \oplus m_{\text{UD}})$ to the reader in the subpart (H2).

(H3) Reader $\rightarrow$ Backend Server: $\text{Pseu}_i, m_t, m_h, n_r^h$.

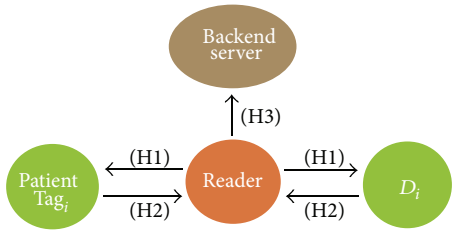

Figure 9: The part H of the new outpatient clinic process.

When the reader receives these two incoming values, the reader forwards $\{\text{Pseu}_i, m_t, m_h, n_r^h\}$ to the backend server for the matching verification, that is, whether the received value m_t is equal to the computed value $(x_i) \oplus \text{PRNG}(n_r^h \oplus x_i)$ or not, and whether the received value m_h is equal to the computed value $(m_{\text{UD}}) \oplus \text{PRNG}(n_r^h \oplus m_{\text{UD}})$ or not. If it is verified successfully, this medicine bag correctly and actually belongs to the patient with x_i. Note that Pseu_i will be used to efficiently retrieve corresponding information of the patient.

3.2. Novel Emergency Care Process on Passive RFID. In Section 3.2, we present a novel emergency care process based on passive RFID (Figure 10). The major difference between outpatient clinic procedure and emergency care process is whether the patient is a roadside patient or not. In general, the roadside patients may not possess their ID card. This causes the inconvenience on identifying these patients. In such case, our process will issue a RFID tag as the roadside patient's temporary ID card. Please refer to part A of Figure 10. In the following, we present part A in a more detailed way. Note that the other parts in emergency care process are the same with that ones in outpatient clinic process. For clarity, we hence ignore the details of these procedures.

In part A of Figure 10, there are two conditions in this action. If the patient is roadside patient without ID card, the hospital will issue an RFID card with a temporary identity number to this patient. Next, in action (A1) of Figure 11 the RF reader inquiries the Tag_i and retrieves the unique identity PID_i in action (A1). After that, RF reader transmits PID_i to the backend server. Since in this stage the roadside patient does not have any history of medical information, the consideration of this patient's privacy can be ignored. Therefore, PID_i can be substituted for x_i in emergency care process until the patient's has been identified. In other conditions, if this roadside patient has the ID card, the process will perform the same steps of part A of the new outpatient clinic process.

4. Security and Efficiency Analyses

In this section, we present the security and efficiency analyses of our proposed e-Health system, such as data confidentiality and patient anonymity, data integrity and nonrepudiation, resistance to the replay attack, and system efficiency.

4.1. Security Analysis. In our proposed e-Health system, we consider the adversary who does not have the capability to inject or modify the transmitted messages. Thus, such type of attacker can be an outsider (and an insider) without any entity verification or system authorization.

Claim 1. The proposed e-Health system can provide patient anonymity and data confidentiality

In the outpatient clinic process, we use the key k_i in the user's smart card to encrypt the patient's PID_i number. This prevents the attacker from cracking PID_i number as the attacker cannot know the key. In addition, since $x_i = \text{AES}_{k_i}(\text{PID}_i)$ is connected with the patient's secret key k_i, this value x_i can correctly be connected to this patient via k_i even though this patient had left the hospital and this card had been assigned to another new patient. Moreover, at each session we utilize the secret value x_i to protect all the transmitted messages. Without knowing the value x_i, the adversary cannot obtain the sensitive information regarding the patient. Hence, our proposed system can ensure the data confidentiality.

Furthermore, as we implement an anonymous authentication technique in the proposed e-Health system, the doctor only needs to know if the patient is legal (or illegal) without revealing the real identity of this patient. In a more detailed way, in our proposed system all the messages are transmitted in cipher format instead of plain text. The secret x_i is utilized to protect transmitted messages during each action. In that case, all sensitive information such as reference number P and the patient's identity are well protected. In addition, at each action we exploit random numbers, that is, n_r^b, n_t^c, n_r^d, n_r^e, n_r^f, n_r^g, and n_r^h, to randomize transmitted messages. On the other hand, in the emergency care process we cannot learn the patient's identity (or privacy) because the roadside patient will not provide any information of his/her medical history. As a result, our proposed system can guarantee the property of patient anonymity.

Claim 2. The proposed e-Health system can provide data integrity and nonrepudiation

In part E of our proposed system, we generate a random number n_r^e and retrieve the identity E_i of the inspector's tag Tag_{E_i}. Next, to make an evidence for further verification, the signature of message $\{\text{Pseu}_i, m_e, E_i, n_r^e\}$ is produced [24, 25]. If adversary intends to modify $\{\text{Pseu}_i, m_e, E_i, n_r^e\}$, the verification of this signature will fall. Therefore, the generated evidence can achieve the data integrity and non-repudiation at the same time.

Claim 3. The proposed e-Health system can resist to the replay attack

In each session of our proposed system, we exploit random numbers, that is, n_r^b, n_t^c, n_r^d, n_r^e, n_r^f, n_r^g, and n_r^h, in randomizing transmitted messages. In addition, in part E a timestamp t_i is involved with the signature creation. These random numbers and timestamp cannot only randomize the transmitted messages but also ensure the resistance the replay attack.

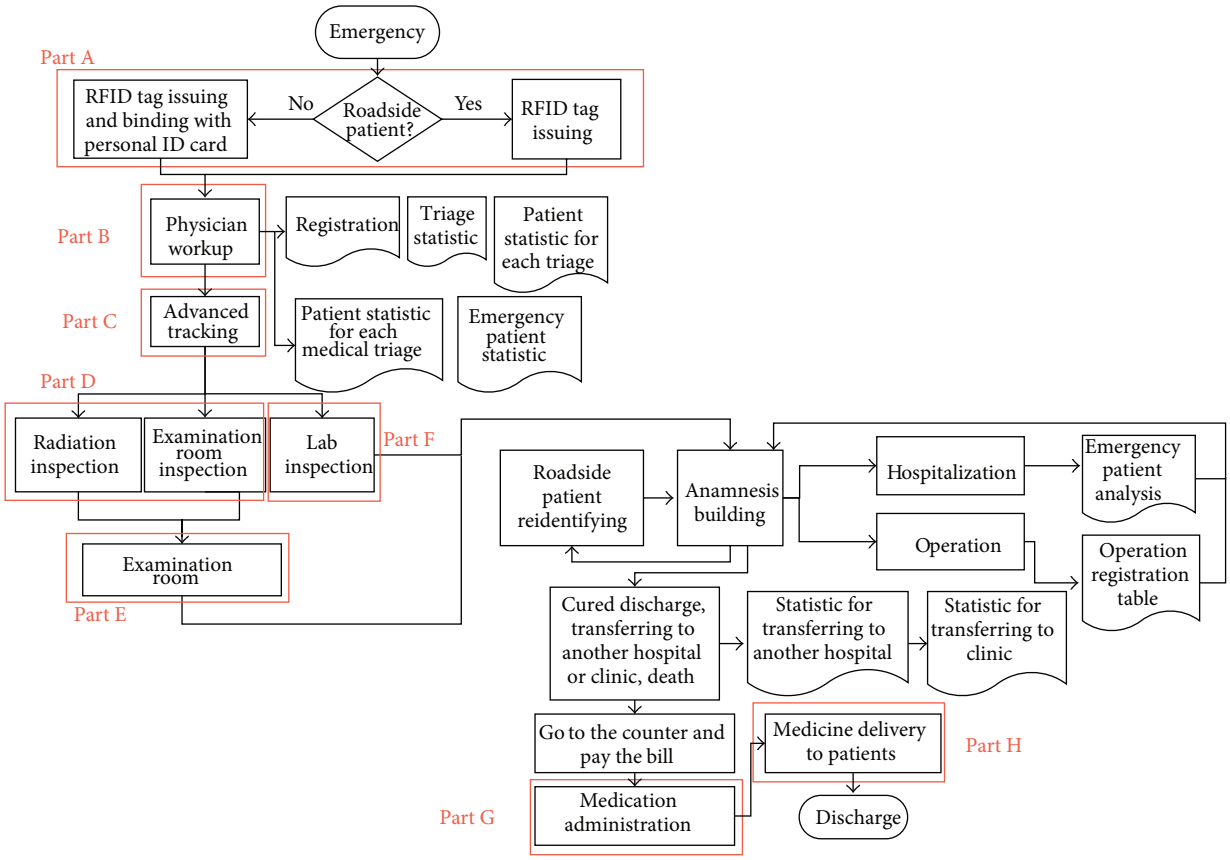

Figure 10: The proposed emergency care process based on passive RFID.

Figure 11: The part A of the novel emergency care process.

4.2. Discussion on Efficiency and Security. In this paper, we adopt the concept of passive RFID to construct our proposed system, where RF tag only needs to support lightweight cryptography modules, that is, random number generator PRNG and exclusive-or operations *XOR*. This design is one of the future trends of RFID technology development in hospital environments [4, 8, 18]. The cost of RFID tag reflects the capability of tag; that is, heavy cryptography modules always need higher computation cost while lightweight ones require fewer. In the hospital environment, the computation efficiency is highly critical as the processing time for each medical procedure is one of the major considerations during the design of an e-Health system. Thus, without any heavy cryptography modules, we believe that our proposed system achieves a good system efficiency.

In addition, from Figures 1 and 10, we can easily conduct the traditional outpatient clinic process and emergency care procedure without any RFID related procedures. Compared to the original non-RFID hospital administration system, we believe that the efficiency can be gained during parts D and F. In general, the process of examination room and LAB is time consuming. With our design, the process time of these two processes can be reduced, and the patient security is guaranteed as well. Note that although the other parts mainly focus on security enhancement and privacy protection, we still think that our proposed e-Health procedures are efficient. In brief, our system introduces a new way to implement a solution for not only achieving hospital administration efficiency but also delivering the security enhancement and privacy protection at the same time.

5. Prototype Implementation

In this section, we demonstrate the prototype implementation of our proposed e-Health system.

5.1. System Environment. In the prototype implementation, the environment is shown as that in the Table 1. First of all, we adopt android with version 4.1.1 as the base operating system to construct our e-Health system. In addition, we use the Eclipse Java EE IDE to develop our system. NEXUS 7 tablets are used to support the computations at the tag side and at the reader side. For instance, once the authentication process begins, the NEXUS 7 tablet at the doctor (or nurse) side will act as a RF reader to send a random number to the Mifare card at the patient side. Note that we also utilize Mifare cards as

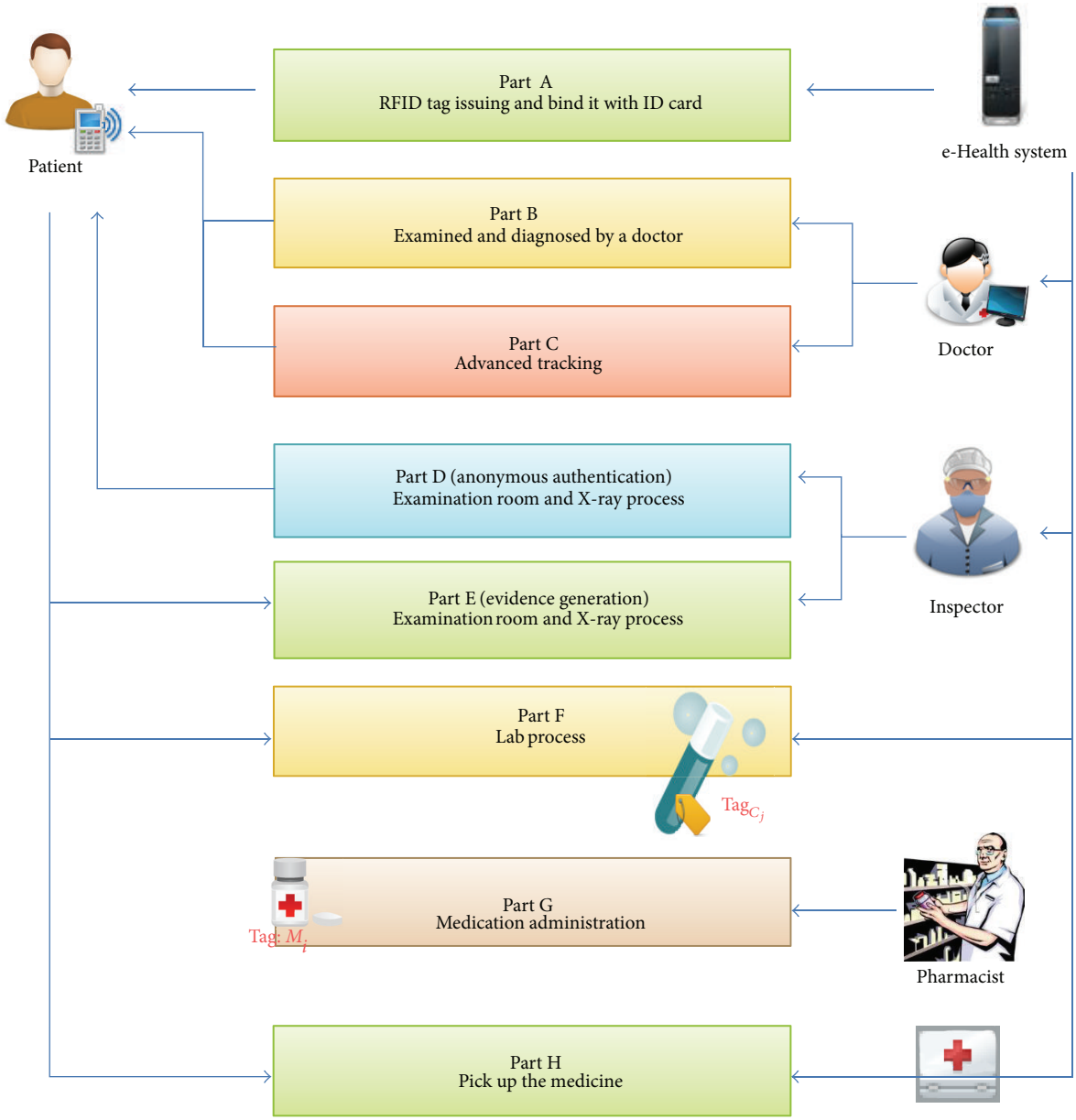

Figure 12: The architecture of the outpatient clinic process.

the target RF tags embedded on the drug bag. In our system, NEXUS 7 tablets are used to transfer and receive information via Near Field Communication (NFC) technology. Moreover, NFC has three communication modes that are peer-to-peer mode, read/write mode, and card emulation mode. In our prototype implementation, we use read and write mode as the basic communication mode.

Table 1: Environment description.

Smartphone	NEXUS 7
Operating system	Android 4.1.1
RFID tag	Mifare Card
Development environment	Eclipse Java EE IDE

5.2. System Architecture and Implementation. As mentioned in Section 3, the outpatient clinic process and emergency care process are almost the same. We thus implement only the outpatient clinic process as the system prototype. Figure 12 is the architecture of implementation of our proposed outpatient clinic process. In the following, we will illustrate the implementation of each process (i.e., part A to part H). Before that, we present the system snapshot at the doctor side (i.e., the reader side or the server side) in Figure 13, while Figure 14 shows the patient information on the NEXUS 7 tablet at the doctor side. Similarly, Figures 15 and 16 demonstrate the system snapshot at the patient side (i.e., the tag side) and the patient information on the NEXUS 7 tablet at the patient side, respectively. Note that in our implementation, the patient

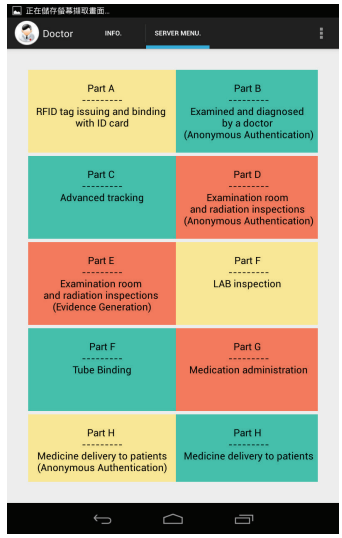

Figure 13: The system snapshot of the NEXUS 7 tablet at the doctor side.

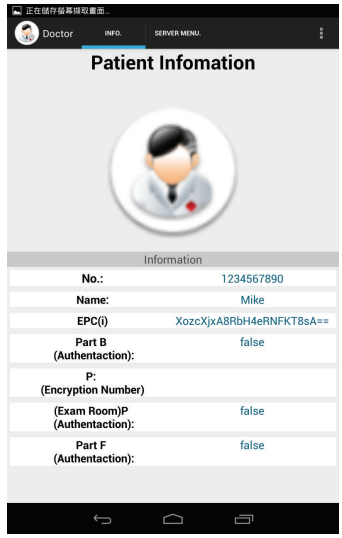

Figure 14: The patient information on the NEXUS 7 tablet at the doctor side.

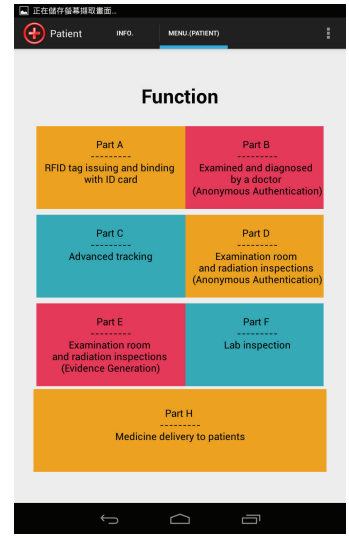

Figure 15: The system snapshot of the NEXUS 7 tablet at the patient side.

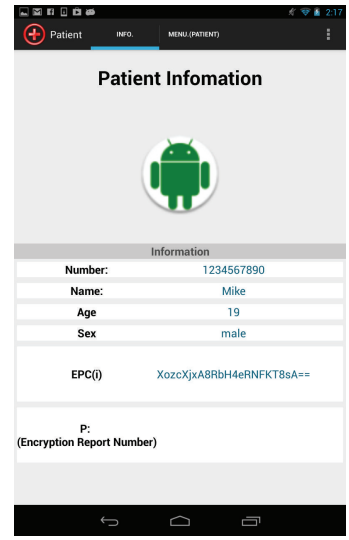

Figure 16: The patient information on the NEXUS 7 tablet at the patient side.

also possesses a NEXUS 7 tablet to clearly demonstrate all processes including the message transmission, entity authentication, match verification, and others. Two NEXUS 7 tablets at the doctor side and the patient side will not exploit the peer-to-peer mode to ensure that the prototype implementation actually reflects the practicality of our proposed RFID-based e-Health system.

(i) RFID Tag Issuing & Bind with ID Card. In our simulation of part A, we use Mifare card to substitute personal smart card with a unique secret key. First, the NEXUS 7 tablet at the server side scans the card and explores the secret key k_i to encrypt the unique identity PID_i, that is $x_i = \mathrm{AES}_{k_i}(\mathrm{PID}_i)$. Second, the NEXUS 7 tablet at the server side stores the information x_i and a temporary pseudonym Pseu_i in backend server for future verification process. Figure 17 presents the message for the success of transmitting the secret information x_i and Pseu_i to the backend server.

(ii) Authenticating the Patient Identity in Part B, Part D, Part E, Part F, and Part H. In parts B, D–F, and H, we implement an anonymous authentication. First, the NEXUS 7 tablet at the server side sends a random number to the NEXUS 7 tablet at the patient side (please refer to Figures 13 and 15). This random number can randomize all transmitted messages. Then, the application (shown in Figure 15) at the patient side will perform the corresponding procedures as that mentioned in Section 3.

(iii) Information Storing at the Patient Side in Part C. Part C presents the patient needs for further physical examinations.

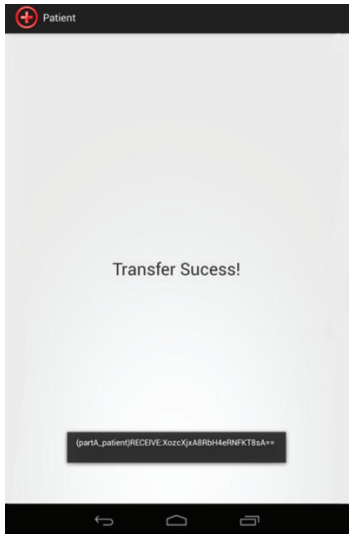

Figure 17: Success image of part A.

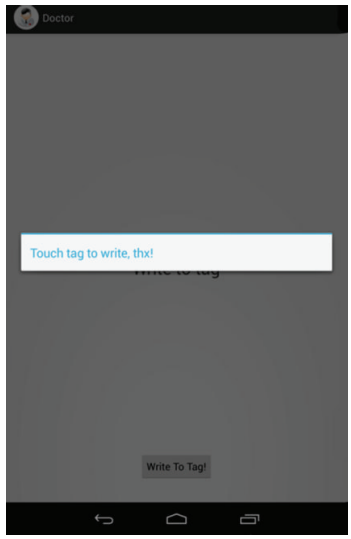

Figure 18: The write mode in part F.

Figure 19: Matching success image of part G.

At first, patient's encrypted diagnosis with its number P is stored in the backend server. Next, the NEXUS 7 tablet at the patient side sends a random number n_t^c to the server which then computes $m_c = \text{PRNG}(n_t^c \oplus x_i) \oplus P$. The server then sends m_c to the NEXUS 7 tablet at the patient side. Finally, the patient possesses the values P and x_i.

(iv) Lab Process in Part F. In part F, an anonymous authentication for the patient is firstly performed. Next, the server will request the information C_j. Then, server generates a random number n_r^f and sends it to tag C_j which computes value $m'_f = n_r^f \oplus C_j$. Tag C_j send m'_f back to the server. Finally, the server retrieves the number C_j. Figure 18 shows the write mode in part F.

(v) Medication Administration in Part G. In part G, we use RFID card binding with the medicine jar, and our application at the server side can confirm the correctness of drugs suggested by the doctor. The system verifies whether the medicine jar is in the suggested list. If the verification holds, the verified medicines will be put into patient's medicine bag. First, the application at the doctor side generates a random number n_t^g to the tag. Tag computes $m_g = \text{PRNG}(n_r^g \oplus n_t^g) \oplus M_i$ and then sends (n_t^g, m_g) to the server. Next, the server verifies the received value m_g to check if M_i is in the doctor suggested list. After that, the server computes $m_{\text{UD}} = M_i \oplus x_i$ and stores the m_{UD} in the patient's medicine tag D_i for part H. Figure 19 presents the matching success result of part G.

(vi) Pick Up the Medicine in Part H. In part H, the server will first check the validity of the patient. Next, the server needs to make sure the correctness of the patient's medicine tag D_i. As the previous authentication process, the server first generates a random number and sends it to tag D_i. Then, tag D_i computes $m_h = (m_{\text{UD}}) \oplus \text{PRNG}(n_r^h \oplus m_{\text{UD}})$ and sends m_h to the server side for matching verification.

6. Conclusion

In this paper, we have introduced an e-Health system consisting of two processes, that is, outpatient clinic process and emergency care process. Eight RFID-based procedures are proposed for enhancing the system efficiency of these two processes. Several techniques such as data encryption, digital signature, anonymous authentication, and tag coexistence proof are adopted as core designs in the proposed system to simultaneously achieve system security and protect patient privacy. Based on our prototype implementation, we believe that our e-Health system can easily be implemented in hospital environment. In brief, our e-Health system demonstrates the system robustness, user/patient privacy protection, and the process efficiency on the medical administration. In the future, more complex hospital scenarios will be discussed. For example, once patient transferring happens, doctor may need

to access information from different hospitals. As a result, the cross-hospital authentication (and authorization) of the doctor will be considered as a major design issue.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors gratefully acknowledge the support from the Taiwan Information Security Center (TWISC) and the National Science Council, Taiwan, under the Grants nos. NSC 102-2218-E-259-004, NSC 102-2218-E-011-012, and NSC 102-2218-E-011-013. The authors also gratefully acknowledge anonymous referees for their valuable comments which have improved the presentation of this paper.

References

[1] C.-L. Chen and C.-Y. Wu, "Using RFID yoking proof protocol to enhance inpatient medication safety," *Journal of Medical System*, vol. 36, no. 5, pp. 2849–2864, 2012.

[2] H.-Y. Chien, C.-C. Yang, T.-C. Wu, and C.-F. Lee, "Two RFID-based solutions to enhance inpatient medication safety," *Journal of Medical Systems*, vol. 35, no. 3, pp. 369–375, 2011.

[3] Q. Lin and F. Zhang, "ECC-based grouping-proof RFID for inpatient medication safety," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3527–3531, 2011.

[4] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, and J. C. A. van der Lubbe, "A comprehensive RFID solution to enhance inpatient medication safety," *International Journal of Medical Informatics*, vol. 80, no. 1, pp. 13–24, 2011.

[5] A.-K. Wickboldt and S. Piramuthu, "Patient safety through RFID: vulnerabilities in recently proposed grouping protocols," *Journal of Medical Systems*, vol. 36, no. 2, pp. 431–435, 2012.

[6] S. H. Wu, K. F. Chen, and Y. F. Zhu, "A secure lightweight RFID binding proof protocol for medication errors and patient safety," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2743–2749, 2012.

[7] Y.-C. Yen, N. W. Lo, and T.-C. Wu, "Two RFID-based solutions for secure inpatient medication administration," *Journal of Medical System*, vol. 36, no. 5, pp. 2769–2778, 2012.

[8] Y.-C. Yu, T.-W. Hou, and T.-C. Chiang, "Low cost RFID real lightweight binding proof protocol for medication errors and patient safety," *Journal of Medical Systems*, vol. 36, no. 2, pp. 823–828, 2012.

[9] C.-C. Lo, C.-H. Chen, D.-Y. Cheng, and H.-Y. Kung, "Ubiquitous healthcare service system with context-awareness capability: design and implementation," *Expert Systems with Applications*, vol. 38, no. 4, pp. 4416–4436, 2011.

[10] A. D. Boyd, C. Hosner, D. A. Hunscher, B. D. Athey, D. J. Clauw, and L. A. Green, "An "Honest Broker" mechanism to maintain privacy for patient care and academic medical research," *International Journal of Medical Informatics*, vol. 76, no. 5-6, pp. 407–411, 2007.

[11] P. Najera, J. Lopez, and R. Roman, "Real-time location and inpatient care systems based on passive RFID," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 980–989, 2011.

[12] K. Ohashi, S. Ota, L. Ohno-Machado, and H. Tanaka, "Smart medical environment at the point of care: auto-tracking clinical interventions at the bed side using RFID technology," *Computers in Biology and Medicine*, vol. 40, no. 6, pp. 545–554, 2010.

[13] R. Agrawal and C. Johnson, "Securing electronic health records without impeding the flow of information," *International Journal of Medical Informatics*, vol. 76, no. 5-6, pp. 471–479, 2007.

[14] P. Ruotsalainen, "Privacy and security in teleradiology," *European Journal of Radiology*, vol. 73, no. 1, pp. 31–35, 2010.

[15] G. L. Kreps and L. Neuhauser, "New directions in eHealth communication: opportunities and challenges," *Patient Education and Counseling*, vol. 78, no. 3, pp. 329–336, 2010.

[16] ISO 27799, Health Informatics—Security Management in Health Using ISO/IEC 17799.

[17] H. Köstinger, M. Gobber, T. Grechenig, B. Tappeiner, and W. Schramm, "Developing a NFC based patient identification and ward round system for mobile devices using the android platform," in *Proceedings of the IEEE Point-of-Care Healthcare Technologies (PHT '13)*, pp. 176–179, 2013.

[18] S. Ajami and M. W. Carter, "The advantages and disadvantages of Radio Frequency Identification (RFID) in Health-care Centers, approach in Emergency Room (ER)," *Pakistan Journal of Medical Sciences*, vol. 29, no. 1, supplement, pp. 443–448, 2013.

[19] R. Safdari, E. Maserat, and E. Maserat, "RFID technology in health environment opportunities and challenges for modern cancer care," *Asian Pacific Journal of Cancer Prevention*, vol. 13, no. 12, pp. 6533–6537, 2012.

[20] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology—EUROCRYPT 2001*, vol. 2045 of *Lecture Notes in Computer Science*, pp. 453–474, 2001.

[21] Citizen Digital Certificate, http://moica.nat.gov.tw/html/en.

[22] Mifare Card, http://www.mifare.net/en/home.

[23] Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST), November 2001.

[24] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[25] "Proposed federal information processing standard for digital signature standard (DSS)," *Federal Register*, vol. 56, no. 169, pp. 42980–42982, 1991.