DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

SECURE MEDICAL ADMINISTRATION IN HOSPITAL

by
Deniz BUKREK

June, 2015
İZMİR

SECURE MEDICAL ADMINISTRATION IN HOSPITAL

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of DokuzEylül University
In Partial Fulfillment of the Requirements for the Degree of Master of Science
in Computer Engineering

by

Deniz BUKREK

June, 2015
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"SECURE MEDICAL ADMINISTRATION IN HOSPITAL"** completed by **DENİZ BUKREK** under supervision of **ASST. PROF. DR. SEMİH UTKU** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

.....
Asst. Prof. Dr. Semih UTKU

Supervisor

.....
Asst. Prof. Dr. Tuğkan TUĞLULAR

Jury Member

.....
Asst.Prof.Dr. Canan Atay

Jury Member

Prof.Dr. Ayşe OKUR

Director

Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

I would like to thank to my advisor Assistant Professor Dr. Semih UTKU for his help, suggestions and guidance to this study.

I would like to thank to my co-workers at Metadata Information Technology Industry and Trade Co. for their support.

This thesis is supported by a project which is called: “Yatışlı Hastaların Mobil Cihazlari İle İlaçTakipSistemi” with the code no: 113s-419 in TÜBİTAK Institution.

Deniz BUKREK

SECURE MEDICAL ADMINISTRATION IN HOSPITAL

ABSTRACT

Patient safety has gained importance after an increase in the number of errors made in healthcare. The number of deaths due to healthcare errors is in the 8th spot, among deaths due to traffic accidents, breast cancer, AIDS etc. The main goal is raising the patient health quality and patient safety. JCAHO (Joint Commission on Accreditation of Healthcare Organizations) recommends the "five right" principles in all hospitals. With this principle the correct patient, the correct medicine, the correct dosage, the correct method at the correct time philosophy is practiced. This principle has to be executed correctly for a good quality healthcare process. After the evaluation of the state of the patient, the needed care and service has to be identified and planned. This is the area where IT is gaining a major role in healthcare. Due to their characteristics RFID and NFC technologies can be used to set up a ubiquitous system to reduce human errors in a hospital.

Our project involves the control and monitoring of the medicine and the medication procedure of an inpatient, after being granted the inpatient status by a doctor. One of the main goals of our project is to monitor the security of the medication procedure and control the overall medication process. The solution is a system which is made up of tags placed on inpatients for identification, tags in identification cards of the doctors and nurses for treatment and medication tracking and mobile devices as tools to relay information to the back end servers. It is planned that the tags are used to keep information about the actors of the procedure. The developed system described in our project will improve the monitoring of inpatient's medication and by doing so, it will boost human healthcare, help to improve the technological infrastructure of our university and form a positive step towards our country's economy and development of the software sector.

Keywords: Mobile application, drug follow, mobile security, near field communication – NFC, XML

HASTANELERDE GÜVENLİ TIBBİ YÖNETİM SİSTEMİ

ÖZ

Günümüzde ortaya çıkan medikal hatalardan dolayı hasta güvenliği önemli bir değer kazanmıştır. Bu tıbbi hatalar nedeniyle meydana gelen yıllık ölüm oranları trafik kazası, meme kanseri, AIDS gibi başlıca ölüm nedenleri arasında sekizinci sırada yer almaktadır. Hasta güvenliği ve sağlık kalitesinin artması temel hedeftir. JCAHO(Joint Commission on Accreditation of Healthcare Organizations) tüm hastanelerde "beş doğru" metodunun geçerli olması gerektiğini öngörmektedir. Bu metot ile doğru hasta, doğru ilaç, doğru doz, doğru yöntem ve doğru zaman felsefesi uygulanmaktadır. Sağlıkta kalite sürecinde bu metodun düzgün şekilde uygulanması gerekmektedir. Bilişim teknolojisi sağlık alanında daha büyük ve temel rol kazanmaktadır. Hastane içerisinde medikal hataların indirgenmesinde RFID veya NFC teknolojilerini özellikleri nedeniyle tıbbi hataları azaltmak için güvenli bir sistem oluşturmada uygulayabilmekteyiz.

Projemiz ile yatışlı bir hastanın, hastane içerisinde geldikten sonra doktor tarafından kontrol edilmesi ve yatış kararı verilmesi ile bu süreçte kullanacağı ilaçların ve uygulanacak sürecin kontrol edileceği bir sistem oluşturulacaktır. Bu sistemin temel amaçlarından bir tanesi ilaç takibinin güvenli bir yapıda takip edilmesi ve sürecin kontrol altında tutulmasıdır. Bu çözüm, yönetimi ve denetimi için arka uç sunuculara, hasta üzerinde takılı ve doktor / hemşire' nin kontrol altında tutulacağı kablosuz etiketler ve mobil tabletlerden oluşan bir sistemdir. Tüm sistem tek merkezden kontrol edilecktir. Projemiz ile, hastane içerisindeki yatışlı hastaların ilaç takip süreçlerine katacağı iyileştirme ile insan sağlığı ve sağlık alanındaki teknolojik çalışmalar konusunda farkındalık yaratılması hedeflenmiştir.

Anahtar kelimeler: Mobil uygulama, ilaç takip, mobil güvenlik, yakın alan iletişimi - NFC, XML

CONTENTS

Pages

LIST OF FIGURES

Pages

LIST OF TABLES

Pages

CHAPTER ONE
INTRODUCTION

Medical care institution planned six main objectives for the 21st century (Wolcott, 2007). The following objectives are aimed:

- Security: protection of patients from medical errors
- Event: helping to reduce overuse of medical resources, and the lack of them and the provision of support to patients
- Patient-Centered Structure : medical decisions' not offering values which mislead patients
- Timeliness: The reduction of patient treatment delays and waiting time
- Productivity: making the equipment efficient and reduction of manpower loss
- Equality: providing similar medical opportunities regardless of gender, race, region and social status.

Hospitals have begun to use various technologies for these purposes. Systems such as Computerized Physician Order Entry (CPOE), Automatic Distribution System (ADS) and barcode solutions aimed to reduce errors. CPOE is a decision support tool to avoid drug-drug interactions of prescriptions. The main purpose of the ADS is deploying drugs automatically and reducing the burden of pharmacists. Finally, barcodes are used to identify patients in ensuring the delivery of the right drug to the right patient. These tools are used to prevent prescription errors, medication errors, dispensing errors and administration errors. ICT (Information and Communication Technologies) and HL7 (Health Level Seven) are preparing a common ground in the creation of a unified monitoring system at this point. The main goal of these technological developments will improve patient safety and the quality of patient care (Kaushal, 2001). HL7 is a standard that has been accepted to exchange data in health information systems, data integration and exchange in access to health data in fifty five countries. Many different standards (CEN / TC 251, the W3C, DICOM, ISO / TC 215, etc.) are using HL7 standards within the implementation of the rules adopted by the orchestration. The security of patient data, processing and sharing information have

been common with accepted standards in the world. In line with this, at CDA (Clinical Document Architecture) structural infrastructure is developed in interpreting and changing the XML-based clinical data within information technology integration. Common standards were formulated by keeping the data to be sent via messaging standards within a certain mold.

1.1 Overview

Information technology is gaining a larger and more central role in the health care field. Increased patient safety and healthcare quality is the main goal. JCAHO (Joint Commission on Accreditation of Healthcare Organizations) in all hospitals requires that a "five rights" method should valid (Eurobarometer, 2006). These methods are right patient, right drug, right dose, right time and right method. This method of quality processes in health should be properly applied. Following the evaluation of the patient, the care he needed should be defined and planned. In order for the patient to pass from a reliable maintenance process in accordance with his needs;

- Determination of treatment to be applied
- Planning of the operations to be applied to a patient (anesthesia, surgery, medicine, nutrition)
- Giving all the information to the related patient and their relatives related to the treatment
- Receipt of approval
- Planning nursing care
- Keeping regular patient records is required

In the quality process of health care, it is necessary to manage the information in the right way in the service process. The organization should determine which data and information will be regularly collected and infrastructure of information management system to collect these data should be formed.

- How to protect the confidentiality
- How to ensure the safety
- How to protect to the integrity of data and information should be planned.

System should be worked as integrated with Hospital Information Management Systems. Records and information should be protected against loss, damage, theft and from access by unauthorized people. In the healthcare system, many different organizations offer development and implementation of hi-tech solutions. Basic key technologies which are RFID, NFC, Data Matrix, EPC global and GS1 global standards have stood out. In the following process of products, recent studies (Peris-Lopez et al., 2011), have discussed different supply tracking technologies (RFID and NFC-based). XML-based messaging standard is also widely used as a standard workflow emerging with this situation.

Barcode technology uses the "line-of-sight" technology. This requires a browser to see the label to read the barcode. Also the possibility of deformation, scratching, tearing of barcode labels is high. In these cases reading problems may occur. Barcode creation also needs to be standardized. This problem can be summarized under five items. First, barcodes are in a printed structure and they might fade and tear over time. Secondly, reading barcodes creates problems in the event of contamination. Third, while reading the barcode, it must be in the line of sight. Fourth, information is very limited in terms of storage. All of these structures that ensure the security of patient information in a hospital environment must be created and supported. At this point, RFID and NFC structures appear as a solution. If compared, the costs of the RFID and security points are considered to have deficiencies in different situations. On the other hand, with NFC technology, these problems are reduced or even eliminated. However, in researches, NFC and RFID technology are evaluated differently both in cost and security.

Figure 1.1 NFC and RFID tags

Medical errors are defined as wrong implementation of a drug to the patient in a way which will harm him, or the giving a drug to him in a wrong dose. Recently, many different solutions are used to prevent human errors in medicine. High-end servers, desktops, personal digital assistants (PDAs), tablet, automatic drug dispensers (AMD), and recently, radio frequency identification (RFID) and technologies such as NFC tags can be given as examples to these. Despite the complex systems and standards, medication errors continue to occur. At this point, actors (patients, doctors, nurses) need to reach a solution.

Today, patient safety has become an important value as a result of medical errors. Institute of Medicine (IOM) (Wu, Kuo, & Liu, 2005), the number of medical errors resulting with death in a year are reported between 44,000 and 98,000. Medical errors are due to faulty blood transfusions, faulty surgical procedures and incorrect patient identification problems. These errors have been reported to be done more in medical wards and emergency services.

Figure 1.2 RFID wristband

In order to prevent medical errors, more than 50% of overall health care costs are spent in the USA. Annual death rates which occur due to these medical errors rank the eighth among the main death causes such as traffic accidents, breast cancer and AIDS.

According to the Institute of Medicine in USA, each year approximately 530,000 preventable adverse drug effects (ADE) are experienced (Aronson, 2009). For each ADE it costs approximately $8.75 to hospital per day per patient. In total, this figure reaches billions of dollars. However, in this subject, there are various negative statistics acquired by the medical communities.

In studies, generally a medication error applied in the treatment process has been shown to cause harm to treatment (Lahtela, 2008). These errors occur when prescribing, implementing the formulation or in the distribution process during the implementation and monitoring of the treatment in hospital. Although realization of medication errors is almost impossible because of the priority of human factors, patient safety, can be improved through appropriate Information Technology (IT) systems.

For example, instead of the wrong interpretation of a hand-written recipe, medication errors can easily be preventable with IT tools created under control. These processes can be controlled and automated with secure drug and patient identification systems. Action-based errors that occur in the process (patient slips) and memory-based errors (omissions) can be prevented (Songini, 2009). A nurse's taking from the shelf some medicine with a similar name or implementation of penicillin to a patient with a known allergy are some examples. Peijas Hospital in Finland (Yao et al., 2011) carried out a study whose results support international reports. In this study it was found out that all medication errors were related to documentation with a rate of 33.6%, drug administration with a rate of 31.1% and drug prescription problem with a rate of 19.5%. A correct method must be applied in the therapy of the patient in the right way at the right time with the right drug in the right dose (EPC Global Inc., 2008). However, because of the pressure and insufficiencies, nurses are in an intense pace of work (Inf technology, 2010).

In 2010 National Patient Safety indicated by the JCAHO set its target entitled: "increase the accuracy of patient identification" as the most significant one among its targets (Eurobarometer, 2006). Therefore, RFID and NFC-based technological solutions can be used to help to reduce the workload of nurses and medical errors. There are UHF Gen-2 RFID tags and systems proposed to reduce medication errors experienced by many people. The capacity of the UHF Gen-2 tags is limited and insufficient for cryptographic algorithms.

To use functions which they supported such as PRNG and CRC and cryptographic algorithms are not suitable for safety reasons.

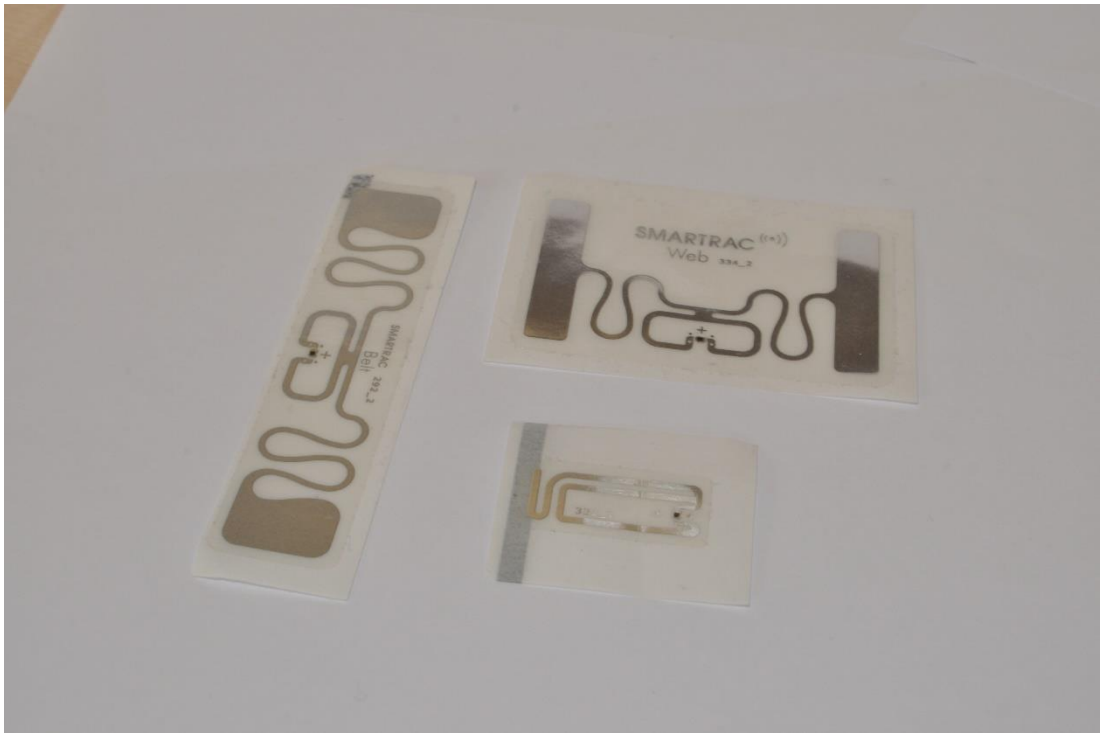

Figure 1.3 Common NFC tags

NFC tags have a higher price than UHF tag. However, it is not the total cost for a complete solution. In a study (Peris-Lopez et al., 2011) the total cost for an average eight-floor hospital, with three nurses for each floor, 5000 inpatient/year and three unit-dose/day have been calculated. An EPC Gen-2 tag cost including per each unit dose packages, is given as plastic 0.5 $ / tag. Each nurse is outfitted with a PDA with a price of $ 300. The total number of tags for inpatients and unit dose was taken as 15,000 / year. A mobile UHF Gen-2 reader is around $ 1,027. When all these values are calculated, the cost which was proposed By Peris et al is $ 70,000 / year. NFC tags, depending on the order size, has a cost between $ 0.421 and $ 0.825. NFC tags are more expensive than EPC Gen-2 tags. But, on the other hand, a popular tablet with NFC (Nexus 7) costs about $ 199.

Therefore, the price is beneficial to NFC reader with 5:1 ratio. With the most expensive NFC tag, our proposal of solution have been calculated with a less cost of $ 21,300 in total when one considers the same health conditions.

In addition to all these information, when the aims of National Patient Safety were examined, the following titles of

- correcting identification of the patient's identity
- ensuring effective communication among caregivers
- ensuring the safe use of drugs
- improving the safety use of key drugs
- giving drugs accurately at the right time

were assessed as important. Therefore, as an answer to the question of what could be done for patient safety asked by the Quality Coordination Office of the Ministry of Health (Quality in Health Services, Bilge Aydin, Ministry of Health, Quality Coordinator), the following must be done:

- Accurate identification of the information about the patient's identity
- Giving a wristband to every patient during the treatment
- Checking the patient's identification prior to any application (before drug application) during the process of the patient's treatment and care,
- Ensuring effective communication between care providers
- Information about the patient's care and his care results must be shared between the doctors, nurses and other health professionals
  - in the shift change
  - between the shifts
  - between the units
  - during the transports.
- Information about the patient's care should be transported together with the patient.
  - Improving the safe use of key drugs
- Determining the drugs with similar spelling and pronunciation and keeping them in a separate location.
- Preventing medication errors

- Right patient, right time, right medication, right dose implementation
- Dual order check
- Packaging of the drugs on behalf of patients
- The detection of drugs used by the patient before hospitalization
- Sticking a label to all drugs and injections

Article No:9 of The Declaration on the Principles and Procedures Regarding the Patient and Staff Safety and its Protection in Health Institutions and Organizations (April 29, 2009, Number: 27214) regulates "the principles and procedures regarding the development and dissemination of patient safety culture to reduce the risks about the safety of patients and employees in health institutions and organizations, the identification of appropriate methods and techniques which will provide that, the dissemination of the best practices developed in patient and staff safety, increasing the awareness and qualifications of staff through in-service training and, formation of reporting systems related to patient and staff safety, improving the safety and quality of patient care and treatment process and protection of patients and employees against possible risks and losses which could be experienced by them during the health care service."

1.2 The Aim of the Thesis

The performance, cost, security and scope of our work are compared with previous proposals. Evaluation shows that the proposed system has stronger security, increased patient safety and equal efficiency, at little extra cost. In contrast to previous unsuitable proposals, IMS-NFC is based on off-the-shelf, modern technologies suitable for healthcare, in every corner of the world. Our project involves the control and monitoring of the medicine and the medication procedure of an inpatient, after being granted the inpatient status by a doctor. Following the safe work of the follow-up medication for inpatients, verifying patient identity, establishing a secure bond between the patient and the health caregivers, prevention of medication errors, ensuring the control of the use of essential drugs have been aimed with this project.

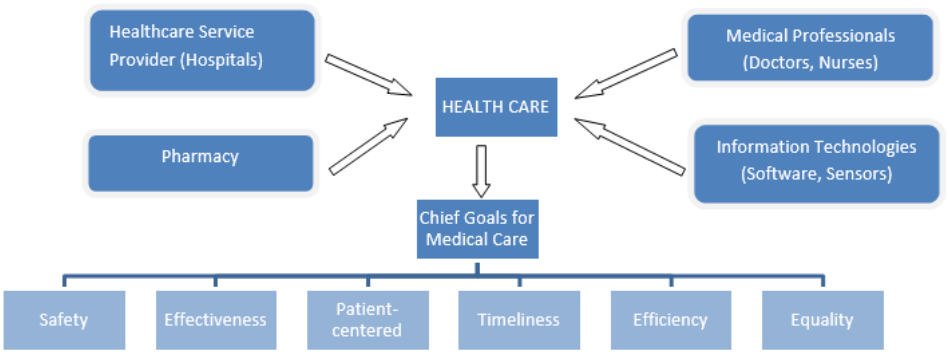

Figure 1.4 Suggested medical administration in hospital

CHAPTER TWO
RELATED WORKS

Day by day, the number of hospital medical errors because of the improper use of drugs in patients is increasing. A system to be applied in general by hospitals must be able to control the use of right medication at the right dosage at the right time. Such a system will help to monitor errors and can react quickly to prevent harm to patients. Two studies have been done using passive UHF radio frequency identification tags. However, because of concerns about privacy and deliberate harm, the proposed system has some problems. In addition, protocols have been examined by using the weak functions such as the PRNG and encryption algorithm.

Institute of Medicine Report (Wu,Kuo, & Liu, 2005) have reported that 98,000 people lost their lives because of the medical errors in the United States. When these data were analyzed, it was documented that 70% of this was due to medical errors, 27% was drug and in 3% it was both. It was determined that medical errors resulted from mostly prescribing practices, drug orders, patients taking wrong medicine and documentation errors; and medical errors and medication errors from lack of communication (41%) and lack of information (22%). In addition, when mistakes that have been done by nurses in the service were examined (Sun, Wang and Wu, 2008), it was reported that the error rate in the dose of 1,000 units was 1.17 in the nurse change during the day while the error rate increased up to 2.12 in the nurse change overnight. In the same survey error rates in the exchange of hospital pharmacists for 1000 dozes were determined statistically during the day as 1:01, 2.24 and 1.88. At the weekend it was stated that the error rates increased from 1.9 to 2.55 according to the drug amount of 1000 dozes during the week.

In many different studies and applications, there are practices regarding the access to efficient health information for patients, nurses, doctors and health care administrators, improving the quality of patient care, reduction of medical errors and the implementation of increasing the co-operation and healthy lifestyle behavior. Huang and Ku, 2008).

Developments and innovations in Health Information Technologies offers solutions focused on different health services, system safety and patient privacy and these solutions are supported by the human rights organizations, the governments and research institutions. Some medical health systems have begun to use different technologies in the process of the patient's health service (Lahtela, 2008). A secure system to reduce the reduction of medical errors in hospitals could be created with the properties of RFID and NFC tag. In Eurobarometer survey about the perception of medical errors, 78% of respondents stated that misuse of drugs was as a major problem in their country. 23% of respondents in the survey indicated that they were directly or indirectly affected by a medical error. 18% reported that they experienced a serious medical error in a hospital (Van Deursen and Radomirović, 2009). Medical errors were examined based on 15,000 patient records. 83.8% of these errors occurred in the hospital environment. As a result of an investigation conducted by the Taiwanese Ministry of Health in 2001 the 9% of 406 cases was caused by improper medication use.

In a study conducted by Chien, RFID-based solutions enhancing patient safety and reducing medical errors were carried out (Chien et al., 2009). In this study, manager protocol functioning as both online and offline was presented.

In 2011, the study of real hospital infrastructure was presented; it was proposed by Peris-Lopez by using RFID technology about functioning of inpatients' whole medicine system structure (Peris-Lopez et al., 2011). The security deficiencies in this study was demonstrated by Yen, too. In 2010, a study developed by Yu with simple logic operations was presented in the e-medical field. It did not have a completed security infrastructure. Besides, Ohashi (Chien et al., 2009) presented a clinical solution proposal which functions by using wireless infrastructure and offers RFID-based medication management and blood test management to inpatients. This system was also stated to have problems that have been created by the use of wireless infrastructure.

In recent studies, in the follow-up of products, different supply tracking technologies (RFID and NFC-based) are discussed. During medical care, the need for patient safety in order to avoid harm has become so significant. In line with this, this XML-based messaging standard is a standard widely used in the workflow.

2.1 Motivation

Gen-2 RFID grouping proof suggestions facilitate medical management, but as demonstrated, it endangers the patient safety in some cases. The main objective should be to establish a system that does not give away any secrets, disrupt medication or generate false evidence. The main motivation of this work is to eliminate the above by "Inpatient Medication system using NFC technology" (IMS-NFC). For the safety of patients, the medical community must choose true cryptographic functions, instead of those meant for supply chains. In a nutshell, with IMS NFC, it is possible to gain the benefits listed below:

- An optimal working distance for a high level of security.
- Individual authentication of doctors, nurses, inpatients and med packs.
- Pairing of hospital equipment with authorized physicians and nurses.
- Secured Server mobile device to exchange data with asymmetric encryption.
- Three-way authentication in all day communications.
- AES algorithm to encrypt messages exchanged with the day.
- Saving partial evidence for inpatient and med packs next to the server.
- Two alternative systems: An online and offline scheme.

In addition to UHF proposals, High Frequency (HF) system proposals have been appearing in real life healthcare applications. The areas include drug administration, patient care, healthcare monitoring, medical device tracking and others (Najera, Lopez and Roman, 2011). Töölö Hospital in Helsinki is just one example; having seen the weaknesses of UHF solutions, the search for better technologies is very natural. In this

paper, a strong security algorithm based solution is proposed that works in on interference-free UHF environment, the pointed out precautions in the Related Work. The Choice of HF is well placed since its power levels are within the limits of the human safety ANSI / IEEE standards 95-1.

CHAPTER THREE
METHODS

The project aims to be checked by a doctor after a patient came to the hospital, inpatient treatment decision of giving the drugs to be used in the process and the process which will be implemented aims to establish a system to be controlled. One of the main aims is to follow a safe system of work and the process of follow-up medication is kept under control. This solution which is for the management and control of back-end servers is installing wireless tags on the patient and the doctor/ nurse and a system of mobile tablets will be kept under control. Keeping the identification information tags with actors is planned. On the other hand, nurses and doctors are equipped with wireless capabilities; including a tag reader which can do operations on the tablet.

3.1 Recommended Technologies

The system can be designed with open-source resources. System data will be stored in MySQL database. MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation. The transmission of data from the system will be provided to the tablets with java web services. The messages are transmitted in XML format via SOAP with Java web services. SOAP transmission paths, encryption methods, such as method call of rules are determined. Open source Apache Tomcat server will be established for the operation of the service.

Apache Tomcat is one of the Apache Software Foundation (ASF) developed open-source Web server and servlet container. Tomcat implements several Java EE specifications, including Java Servlet, Java Server Pages (JSP), Java and EL Web Socket and provides a "pure Java" HTTP web server environment to run Java code in.

Tomcat is developed by an open community of developers under the auspices of the Apache Software Foundation and maintained, released under the Apache License

2.0 license and is open source software. Server will communicate with nexus 7 tablets which have NFC read and write support. NFC tags are based on MifareDesfire EV1 standard.

3.2 Actors and Elements

HIS (Hospital Information System): A key decision back-end database servers with access to all departments and clinics of the hospital via a wired and wireless local area network. It saves all stationary, doctor, nurse and medical information (ID numbers, timestamps and Pre-Shared Secret Keys), manages and checks the patient, doctor, nurse and medication-related processes (identity card/bracelet sales, registration, medical dispatching, medical management and patients' allergies to certain drugs). It also uses a TLS and Certificate Server that increase the security between the tablets and the server.

Tablets: Tablets will be used for the patient's management and supervisory process. In this tablet programs about the doctor, nurse, pharmacist and registration will be available. Tablets must be NFC-supported. Therefore, Nexus tablets with NFC support were recommended as they are one of the cheapest solutions. In the tablet the application to perform the encrypt-decrypt-hash functions have been developed.

Tag: The cards in the ISO 14443 standard and AES encryption-decryption technology are used. In these cards unique card number, shared secret keys and data are stored and kept in secure areas.

Doctor: He is the actor who will determine the admission status of patients. They are responsible for the drugs which will be given to the patient and their supervision. The system was developed according to the ability of a physician to use different tablets.

Pharmacy: The drugs which will be given to inpatients will be prepared in pharmacies according to the doctor's prescription and then it will be associated with the patient by

putting the information about the patient on the drug label. In this way giving the wrong drug to the wrong patient was prevented.

Nurse: The process of visits and medication of inpatients will be carried out with the tablets given by the hospital. The timing of the drug to be administered to the patient will be controlled by the timing tool created on the HIS server and with the necessary guidance, giving the right medication at the right time will be provided. Nurse, will control the medpacks prepared by the pharmacy by swiping them through NFC tags and prevent errors between medication and patients. By logging the time information in the system giving the patient the wrong medicine will be prevented.

Inpatient Room (Room): With the labeling developed specially for the room where the patient stays, an additional controlling feature which will prevent the nurse from going to the wrong patient was introduced.

Medicine Cart: Patient clinic card.

Medicine Drawer: Drug transporter which keeps patient drugs.

Medicine Pack: Unit-dose med packs packages in drug transport and formed by pharmacies.

3.3 Notation

All the transmissions between the tablet and the server are done using TLS in proposed protocol. It is assumed that all the active actors (tablets, server, and nurse PC) of the Hospital Information system are using TLS. Our system is created over the TLS. Therefore, a certification server is installed and public keys are distributed to our active actors. At first, physician verification is confirmed before starting the control of the patient. The doctor inputs the identity and password to initialize the the tablet. The tablet precedes the mutual authentication with the server. After authentication process, a verification code is generated and transferred to the tablet. Next, the system proceeds with doctor card authentication. The reader processes a mutual authentication with the server to obtain the doctor's information. In proposed scheme, we use the RSA and SHA512 to create a signature of the data and use AES for encryption.

Table 3.1 Definition of terms

id_X	:	the unique identity of X
usr_X	:	the unique user name of X
K_d	:	Doctor's password known by the doctor and the server
$pass_X$	:	the passcode of X
$card\_id_X$	:	the card id of X (7 bytes)
cpu_id_X	:	CPU ID of Tablet X
$P\_ id_X$	:	patient id of X
sign(m, K_{SR}):		uses the server's private key, K_{SR}, to sign message m
usign(m, K_{SU})	:	uses the server's public key, K_{SU}, to unsign message m
E(m,k)	:	uses the key k, to encrypt message m, based on the AES
D(m,k)	:	uses the key k, to decrypt message m, based on the AES
h()	:	SHA512 hash algorithm
K_{SR}	:	server's private key, known only by the server, based on the RSA assumption
K_{SU}	:	server's public key, known by tablets, based on the RSA assumption
K_{SC}	:	secret key known by the server and the Doctor's smart card, based on AES assumption
K_{DC}	:	secret key shared by the smartcard and the doctor
K_P	:	Secret key of the Patient smartcard
t_{start}	:	timestamp when the doctor enters username and password at the beginning
t_0	:	timestamp when the smartcard of the doctor is read by the Tablet
t_1	:	timestamp beginning time of the consultation of patient
t_2	:	timestamp ending time of the consultation
n_0	:	the server uses PRNG function to generate a nonce value (16 bytes),
X? = Y	:	Determines whether or not X is equal to Y
transfer(m)	:	Transfers the given message m, by using TLS channel
f()	:	A simple function.
smessage	:	secure message – Message secured by encryption using AES

3.4 System Workflow

This system is connected to hospital information system database server. (HIS). For doctors and nurses, a general infrastructure which they will operate on tablets were prepared. With HIS central server, an infrastructure connecting different departments, clinics over a local network will be prepared. All information about transactions on the server, for example, the patient's personal information, identity information (ID), such as encryption keys will be made. A label will be attached to inpatient with a wristband and a label for the medication package will be given. Pre-shared secret into the label (encrypted data) will be used for patient authentication. The use of NFC tags in the system is planned. In this way, creating awareness in terms of both security and cost is planned. Thanks to the system, a patient in hospital will be kept under control in the process which passes after the patient is taken into hospital until he is discharged. The systematic preparation of drugs to be used and their reach at the clinical service, and administering them to the patient after their reach can be monitored. An NFC wristband is planned for each patient. These wristbands will have encryption keys stored in order to access the patient's general information and created during the administration to patients. During the process the doctor will swipe his NFC card and sign on the tablet before he moves on to control process.

At the start of the examination procedure, the doctor starts the process by scanning a patient wristband to control. The doctor will confirm the person's information both within the framework of information coming from NFC tag and from person's biometric data which will be sent through the server. After the inspection process, with the decision of admitting the patient, necessary treatment method will be determined on the application on the tablet. The treatment to be implemented, medication doses and similar treatment process for the relevant patient will be entered into the system by the doctor. With this information, the amount of drug entered by the doctor will be determined by the hospital pharmacy, packed with NFC tags specific to the relevant patient and sent to the service. After the patient comes to the clinic, the nurse will start checking process of the patient. At this stage, the authentication applied for the doctor will also be applied for the nurse, and the nurse will do the necessary safety checks on

the tablet and sign in. Then information about the medication and general information about the inpatients that are on the same floor with the nurse will be transferred on the nurse's tablet. While the nurse is delivering the drug to the patients on the floor, she will reach the information by swiping the medpacks on NFC tags on the relevant patient's the wrist and she will have given the right patient the right drug at the right time. With this project, it is planned that every stage of the inpatient is kept under control and monitored with a secure system after he came to hospital. The adoption of technological solutions and supported information systems in hospitals will be used to improve patient safety and provide a safe environment in order to increase the quality of health services. In figure 3.1, process orders have been described.

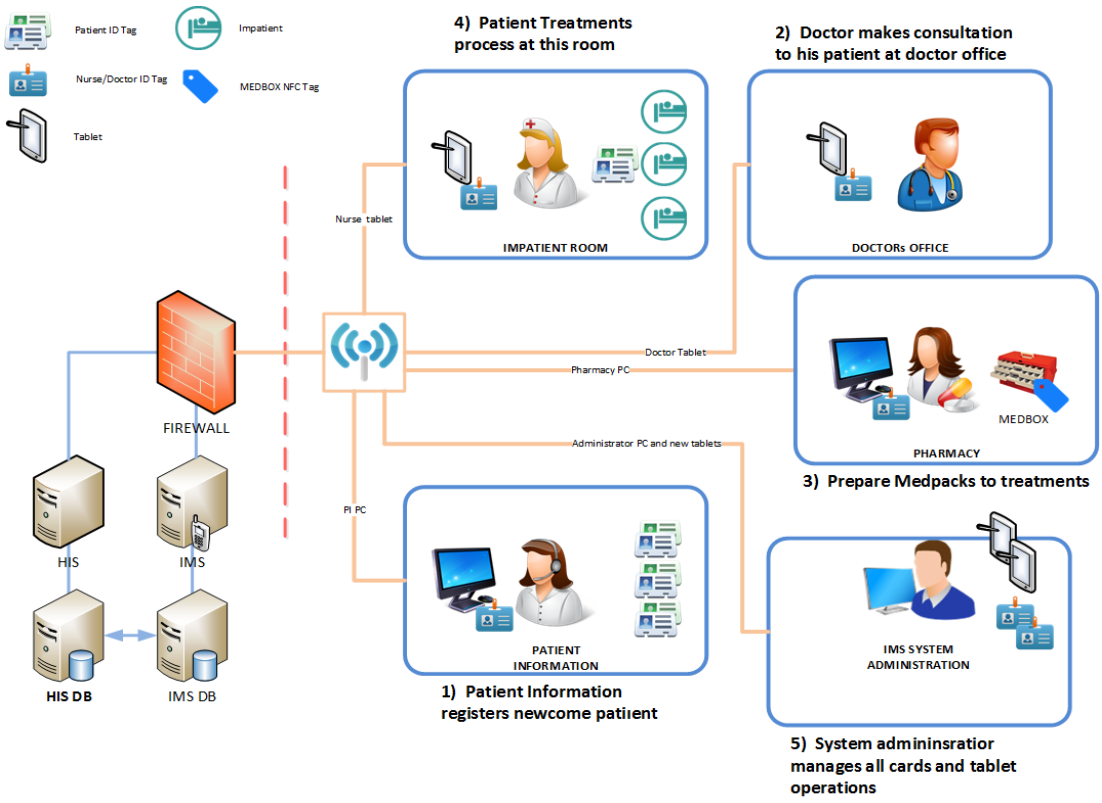

Figure 3.1 IMS main system

The sectional scheme has three phases. The phases follow a chronological order, report to the HIS and can't be skipped. The inclusion of a patient into the database starts with registration. When the patient is checked out, the personal and biometric data are preserved. In the first phase, the person is dispatched to a doctor, who grants

the inpatient status. In the second phase, the pharmacy prepares the unit-dose medications and sends them to the clinic of the inpatient. The inpatient checks into a room at the clinic. The third phase starts after the nurse makes preparations and visits the inpatients in a medication round. After the medication, the nurse gathers proof that drug administration has been carried out and sends them to the HIS. In the final stage, drug administration evidence is monitored for errors; if found, an alarm is generated. The used wristbands and med packs are re-initialized for the next user.

3.4.1 Phase 1: Registration and Dispatch

Patient Registration:

- The id_{Inpi} is linked to the $card\_id_{Inpi}$
- A photo is taken
- Additional personel info is stored in HIS (name, surname, sex, bdate, registration_date, email)
- The inpatient tag is loaded with pre-shared keys and files are initialized.
- Medication time is updated for the patient.

Doctor Registration:

- The idInpi is linked to the card_idInpi
- A photo is taken
- Additional personel info is stored in HIS (name, surname, sex, bdate, registration_date, email)
- The inpatient tag is loaded with pre-shared keys and files are initialized.
- Password is taken
- AES key K_{Dri} of the doctor is generated and stored.
- cpu_id_{Dr} value is gathered and stored

Nurse Registration:

- The idInpi is linked to the card_idInpi
- A photo is taken
- Additional personel info is stored in HIS (name, surname, sex, bdate, registration_date, email)
- The inpatient tag is loaded with pre-shared keys and files are initialized.
- Password is taken
- AES key of the nurse is generated and stored
- cpu_id_{Nurse} value is gathered and stored

All the transmissions between the tablet and the server are done using TLS in proposed protocol. We assumed that all the active actors (tablets, server, and nurse pc) of the Hospital Information system are using TLS. Our system is created over the TLS. Therefore, a certification server is installed and public keys are distributed to our active actors. At first, physician verification is confirmed before starting the control of the patient. The doctor inputs the identity and password to initialize the tablet. The tablet precedes the mutual authentication with the server.

- The doctor and the nurse determine their passwords as the first step. The doctor's and the nurse's cards are initialized. (Keys are loaded to the smart cards).
- Each member (server, pharmacist, doctor and nurse) has its corresponding public/private key based on the SSL mechanism.
- All the transmissions between the tablet and the server are done via TLS channel.
- Smart cards are based on MifareDesfire EV1 standard.

The person, who asks to see a doctor with aid_{Inpi} receives a new identity card in the form of a bracelet, with a unique $card\_id_{Inpi}$.If unconscious, even a bracelet for the impatient is provided. The id_{Inpi} is the $card\_id_{Inpi}$ connected. A photo is taken for visual detection. All the data with the other personal data is stored on HIS. Inpatient day is loaded with pre-shared keys and the files are initialized to be updated with the time of the last visit to the doctor or recent medication.Then the person is sent to see a doctor.

3.4.1.1 Doctor and Nurse Authentication

The authentication and the pairing of the doctor with the hospital tablet are shown in Fig 3.2. In the office of the doctor on duty starts the application, the time t_{R_1}.The application prompts for username usr_{Dri} and password.

1) Certification server is installed. Public keys are distributed to our active actors (tablets, and nurse pc). TLS security layer is installed between the active actors because it is assumed that HIS system uses TLS for all the actions.

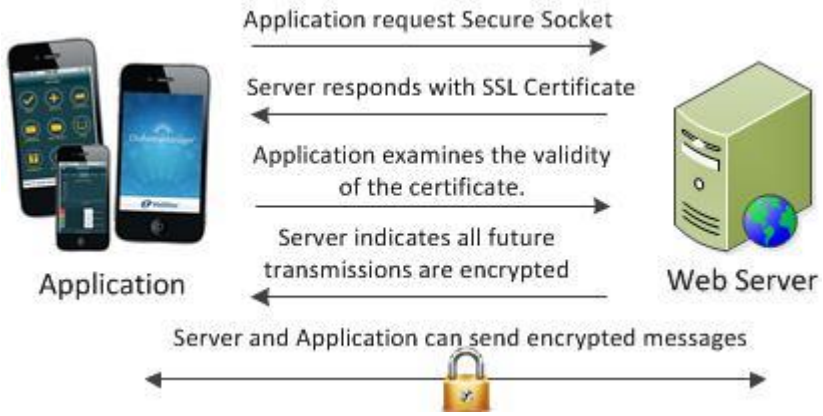

Figure 3.2 Secure communication between application and server

2) The doctor and the nurse determine their passcodes, and passwords as the first step. The doctor's and the nurse's cards are initialized. (Keys are loaded to the smart cards).
3) The doctor's and the nurse's password are not transferred in the transmission channel to prevent replay attack.
4) Each member (server, pharmacist, doctor and nurse) has its corresponding public/private key based on the SSL mechanism.
5) All the transmissions between the tablet and the server are done via TLS channel.
6) Smart cards are based on "MifareDesfire EV1" standard.
7) The server uses PRNG function to generate nonce values with 16 bytes size.
8) Preparing and processing a 30-minute ticket is controlled accordingly.

Process Step (tablet) 1: The doctor inputs the user name (usr_{dr}) and password (K_d) to authenticate the application. The tablet and the server create a TLS channel. The doctor's password (K_d), the tablet's CPU identification number (cpu_id_{dr}) and time (t_{start}) are encrypted using AES.

$$smessage1 = E((cpu\_id_{dr}, t_{start}),K_d) \quad (3.1)$$

Transfer Step (tablet – server) 1: By using TLS, the tablet sends processed message and the doctor's username to the server.

$$transfer(usr_{dr}, smessage1) \quad (3.2)$$

Process Step (server) 2: When receiving the initialization information from the tablet, server checks the doctor username, finds K_d from the database and decrypts the message $E((cpu\_id_{dr}, t_{start}),K_d)$ and extracts cpu_id_{dr}, t_{start}. Then, by using the doctor's username, it finds the doctor's identity number (id_{dr}) and produces hash value by using SHA 512 functions, and signs it with its private key, which means the tablet is bound to that doctor at t_{start}. Then the server uses PRNG function to generate a nonce value $\{n_0\}$ (16 bytes), encrypts this value with a Key only known by the server and the Doctor's smart card (K_{sc}) and produces $E(n_0,K_{sc})$.

$$\begin{gathered} D((cpu\_id_{dr}, t_{start}),K_d), \text{ extracts } cpu\_id_{dr}, t_{start} \\ Ver1\_DrTablet = sign((h(cpu\_id_{dr}, t_{start}, id_{dr})), K_{SR}) \\ \text{generate } \{n_0\}, \text{ and } smessage2 = E\ (n_0, K_{sc}) \end{gathered} \quad (3.3)$$

Transfer Step (server – tablet) 2: Ver1_DrTablet, message_E2 and id_{dr} are transferred to the tablet via TLS.

$$transfer\ (Ver1\_DrTablet, smessage2, id_{dr}) \quad (3.4)$$

Process Step (tablet) 3: By using the Server's Public Key (K_{su}) Ver1_DrTablet is verified, which also means that the server is verified by the tablet. Verification step:

$$h(cpu\_id_{dr}, t_{start}, id_{dr}) \text{ ?= usign(} h(cpu\_id_{dr}, t_{start}, id_{dr}), K_{SU}) \quad (3.5)$$

The doctor enters his passcode and lets the tablet read his smartcard and gets the doctor's card id from the smartcard. By using the passcode ($pass_{dr}$) and the doctor's card id ($card\_id_{dr}$), the secret key of the doctor (K_{DC}) is generated.

$$K_{DC} = E(card\_id_{dr}, pass_{dr}) \quad (3.6)$$

Transfer Step (tablet – smartcard) 3: Transmission between the doctor and the smartcard goes on; the doctor lets the tablet read his smartcard by using K_{DC}. The authentication of the card is done according to the ""MifareDesfire EV1"" standard. After authenticating to the card, encrypted data is sent to the smartcard of the doctor.

$$transfer(smessage2) \quad (3.7)$$

Process Step (smartcard) 4: The Smartcard gets the $E(n_0,K_{sc})$ value, then

$$D(n_0,K_{sc}) \text{ and gets the } n_0 \text{ value, and generates } E(f(n_0),K_{sc}) \quad (3.8)$$

Transfer Step (smartcard – tablet) 4: Generated data with function f is transferred to the Tablet.

$$Transfer(E(f(n_0),K_{sc}))) \quad (3.9)$$

Process Step (tablet) 5: The tablet creates a package of data and sends to the server where t_0 is used to indicate the reading time of the Doctor's smartcard.

$$smessage3 = (t_0, id_{dr}, cpu\_id_{dr}, E(f(n_0),K_{sc}), Ver1\_DrTablet) \quad (3.10)$$

Transfer Step (tablet – server) 5:

$$\text{transfer (smessage3)} \tag{3.11}$$

Process Step (server) 6: The doctor's identity number is used to check whether the doctor has the correct smartcard. id_{dr} and cpu_id_{dr} are used to check that connection is unique and the doctor isn't logged in anywhere else. Ver1_drTablet_ID verifies that this is the right session, not a replay attack. Then it creates Ver1_DrTablet_ID' and checks it with the Ver1_DrTablet (value that was sent from Tablet).

$$Ver1\_drTablet \text{ ?= } sign((h(cpu\_id_{dr}, t_{start}, id_{dr})), K_{SR}) \tag{3.12}$$

The Server applies to the same function to $\{n_0\}$ and generates $E(f(n_0),K_{sc})$ on the server side and checks it with the transferred value $E(f(n_0),K_{sc})$ that the tablet sent. If it matches, the smartcard is the correct one.

$$E(f(n_0),K_{sc}) \text{ ? = } E(f(n_0),K_{sc}) \tag{3.13}$$

The next step is to create Ver2_DrTablet,

$$Ver2\_DrTablet = sign(h(t_0, Ver1\_DrTablet),K_{SR}) \tag{3.14}$$

Transfer Step (server – tablet) 6: Ver2_DrTablet_ID, biometric information of the doctor (picture of him) are sent to the Tablet.

$$\text{transfer(Ver2\_DrTablet, doctor\_biometricdata)} \tag{3.15}$$

Process Step (tablet) 7: By using the Server's Public Key (K_{SU}) Ver2_DrTablet is verified. Verification step:

$$h(t_0, Ver1\_DrTablet) \text{ ?= } unsign(h(t_0, Ver1\_DrTablet),K_{Su}) \tag{3.16}$$

Then the bracelet (having MifareDesFireEV1 chip) of the patient is read by the tablet. Patient_ID is read from the bracelet.

Transfer Step (tablet – server) 7: Patient Identity number (P_ id_1), Consultancy time (t_1), and Ver2_DrTablet are sent to the server.

$$\text{transfer}(P\_\ id_1,\ t_1,\ \text{Ver2\_DrTablet}) \tag{3.17}$$

Process Step (server) 8: Ver2_DrTablet_ID is verified by the server

$$\text{Ver2\_DrTablet} \mathrel{?}= \text{sign}(h(t_0,\ \text{Ver1\_DrTablet}), K_{SR}) \tag{3.18}$$

and Ver3_DrTabletP is generated by the server

$$\text{Ver3\_DrPDA} = \text{sign}(h(t_1,\ \text{Ver2\_DrTablet},\ P\_\ id_1),\ K_{SR}) \tag{3.19}$$

alsoKp is encrypted by using the doctor's password K_d.

$$\text{smessage4} = E(K_p, K_d) \tag{3.20}$$

Transfer Step (server – tablet) 8: Ver3_DrPDA, $E(K_p,K_d)$ and the biometric and personal information of the patient (picture of him) are sent to the Tablet.

$$\text{transfer}(\text{Ver3\_DrPDA},\ \text{smessage4},\ \text{patient\_biometricdata}) \tag{3.21}$$

Process Step (tablet) 9: The Doctor's password (K_d) is used to decrypt $E(K_p,K_d)$.

$$K_p = D(K_p, K_d) \tag{3.22}$$

The doctor can check the personal information and picture of the patient from his Tablet screen and examines the patient.

Transfer Step (tablet – server) 9: In inpatient status**;** Ver3_DrPDA, inpatient medicine units, ending time of the consultation, patient identity number and tablet's CPU identification number (cpu_id_{dr}) are sent to the server.

$$transfer(t_2, P\_ id_1, Med1, doz1, Med2, doz2, cpu\_id_{dr}, Ver3\_DrPDA) \quad (3.22)$$

3.4.2 Phase 2: The Preparation of The Medpacks

After receiving the order from the server, the pharmacy stationary the medpack with a tag with an AMD. The time t_2 within the tag is checked if it is the initialization value. Then, time of packaging t'_2 is written in the card. The $card\_id_{MPInpi}$ of the tags is connected to the stationary $card\_id_{Inpi}$. The med pack is placed into the corresponding drawer of the clinic's med cart, which also has an identification tag. The med packs of the inpatients in the same room are in the same drawer. HIS is informed, and the med cart is sent to the hospital.

3.4.3 Phase 3: Nurse Station and Medicine Administration

Nurse application (NA) helps nurses to make treatments of their patients by following doctors' consultation. Nurse should be authenticating NA with her/his NFC card after logging in with their user name and password. Firstly, nurse interacts with an NFC patient wristband for displaying information about pending tasks of this patient**.** The system clinical record is automatically updated on the tablet in offline mode; if the tablet is online, the patient record is updated on the IMS – Server. To start a treatment, nurse has to be authenticated NA with patient's wristband to access to patient consultation information. At this step, nurse can see patient information, current treatments and treatment history of patient with all the details in Figure 3.4.and 3.5. After authenticating the patient wristband and listing treatments, nurse selects current treatment to implement.

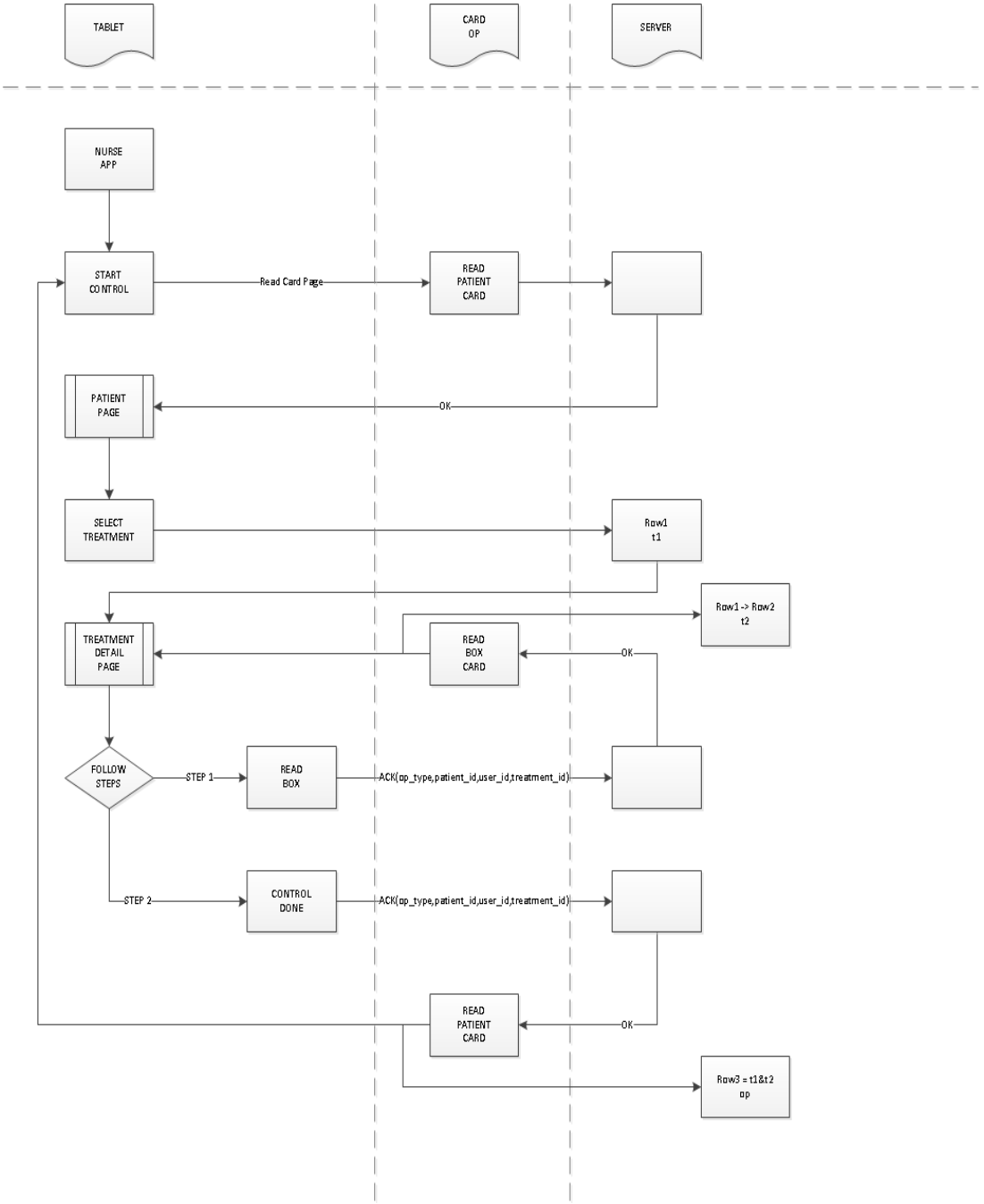

Figure 3.3 Communication at nurse treatment between application and server

After getting details of treatment from NA screen, nurse finds the related medpack and implements drugs to patient. After drug implementation operation, nurse authenticates medpack with swiping medpack NFC card with tablet. After successful authentication, operation nurse presses DONE button to finish treatment.

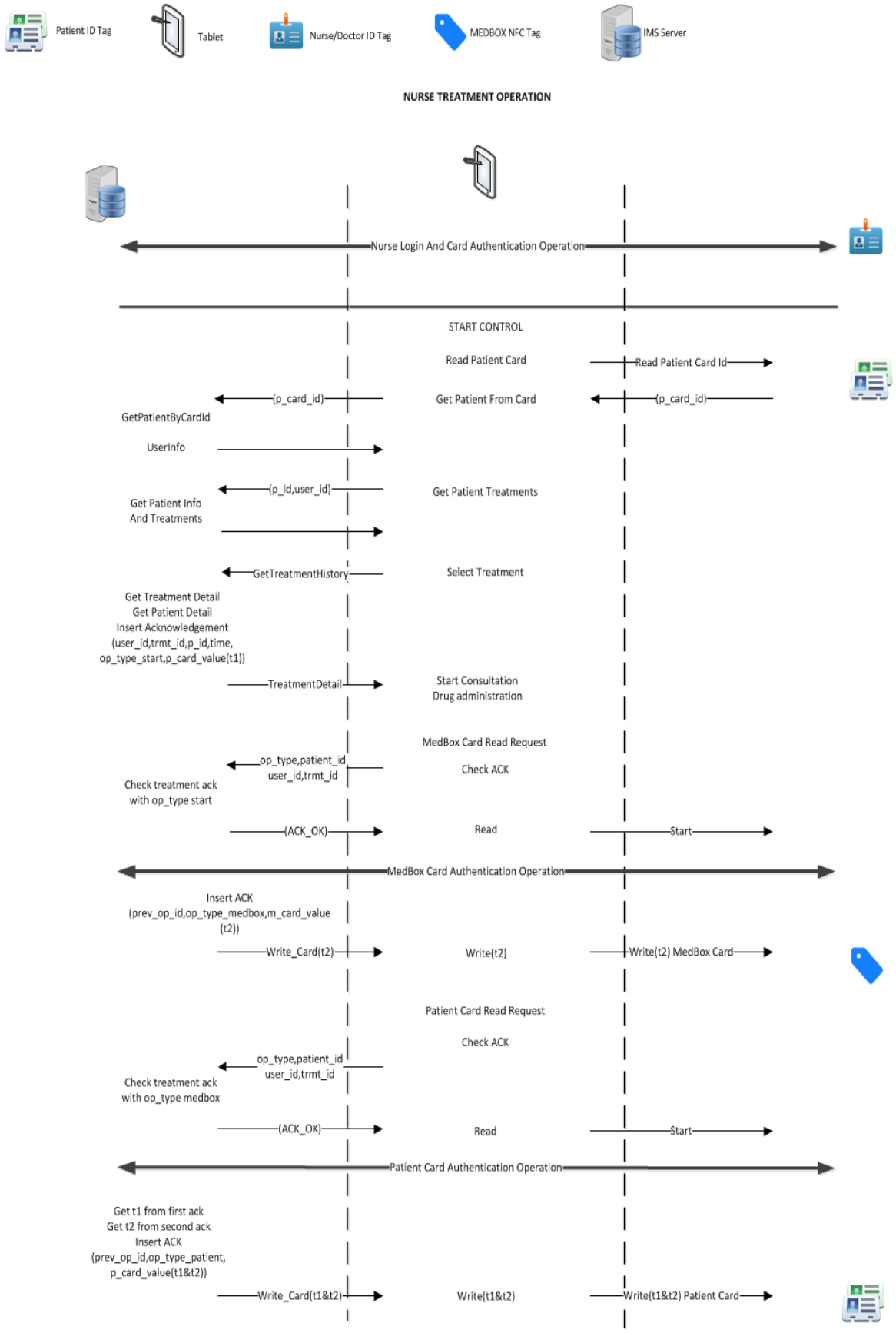

Figure 3.5 Detailed communications at nurse treatment applications and server

After nurse logged in to application and authenticated successfully, to start a new treatment he/she must authenticate patient with her card. If authentication is successful, nurse can list patient's information, treatment history and ongoing treatments. If nurse wants to apply a new treatment to patient, he/she selects an ongoing treatment from list. At this time nurse app shows details about treatment and server creates an acknowledgement record on the database for selected treatment.

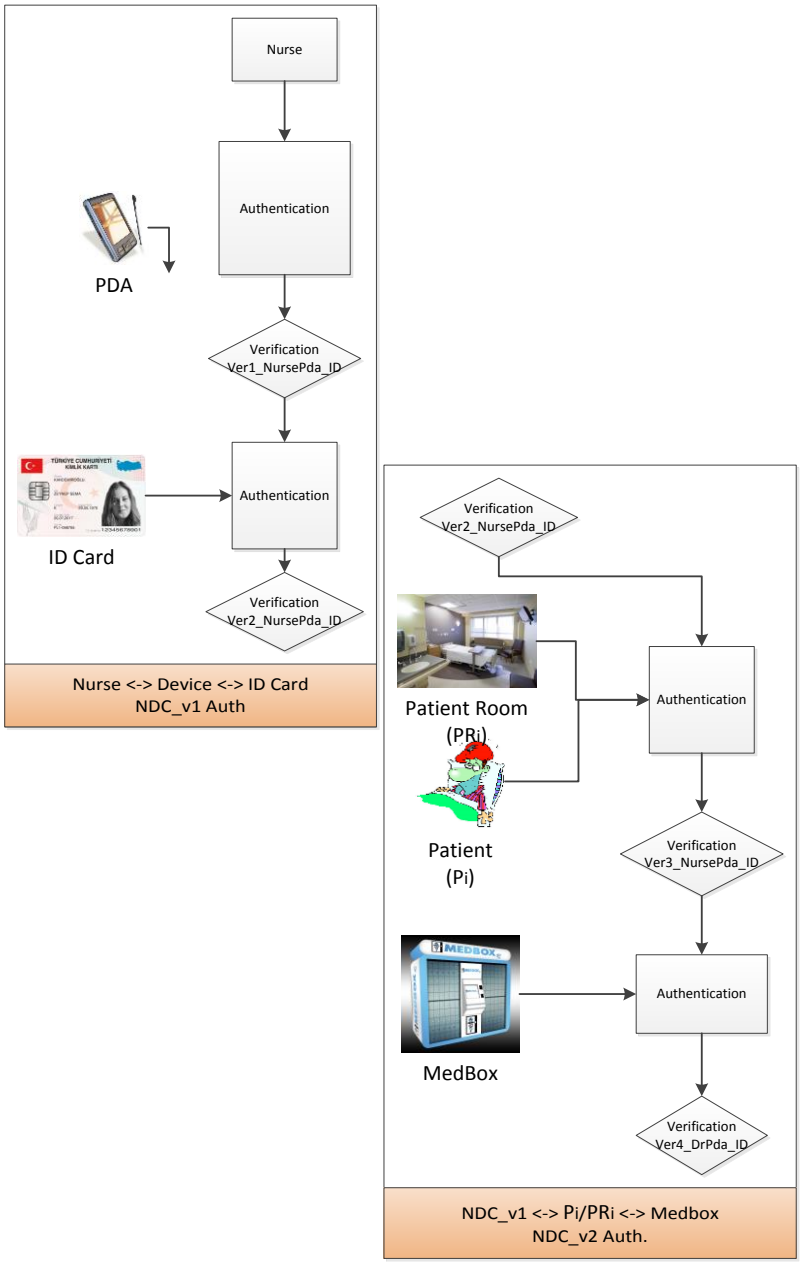

Figure 3.6 Summary of nurse treatment operation

This record includes user id, treatment id, patient id, acknowledgement create date and time, operation type (SELECTTREATMENT) and patient NFC tag time value. After getting details about treatment, nurse tries to authenticate medpack with swiping medpack NFC card. At this step, nurse application sends a request to server to check "SELECTTREATMENT" acknowledgement. If server finds acknowledgement, it lets the app authenticate with medpack card and add a new record.

This record keeps user id, treatment id, patient id, operation type (MEDBOXREAD), previous ACK operation id and medpack NFC tag time value. This time, nurse gives patient his/her drugs and finishes the treatment with authenticating patient's card. After successful implementation, nurse finishes treatment by pressing DONE button. At this step, nurse application sends a request to server to check "MEDBOXREAD" acknowledgement. If server finds acknowledgement, it lets the app authenticate with patient card and adds a new record.

IMS-Server gets first acknowledgement value with id of patient card. Then server gets second acknowledgement by first acknowledgements id and checks values. If values match, a new time value (t1&t2) will be generated which is a logic operation of first (t1) and second (t2) acknowledgements' time value. At this logic operation, server processes half of the byte "AND" operation and the other half of byte "XOR" operation. New time value will be written to patient NFC tag at authentication step and server records third acknowledgement (PATIENTREAD). Next, inpatient identification and medicine administration (at the right time) can take place online or offline.

The nurse uses the wireless infrastructure to stay online with the HIS, during drug administration round. In this mode all card authentications take place. Medication starts with authenticating the inpatient first. The time t'_1 of the doctor's visit or previous medication is read, checked and then the new time t''_1 is written to the wristband, using session key K_{sInpi}. The nurse verifies the inpatient photo on the screen and opens the drawer belonging to the room; touches the medpack tags to locate the

correct color-coded (morning/noon/night) drug for the inpatient. After server authentication of the pack, preparation time t'_2 is read and checked. Then the time of medication t''_2 is written on the card. Additional cross-evidence is provided by writing t''_1 into the med pack tag. An indication is given on the screen and the nurse administers the medicine. Finally, the nurse touches the wristband of the inpatient for the final cross-evidence generation. After authentication, time t''_2 of med pack is written into the inpatient tag. Hence, both the inpatient and the med pack contain cross evidence. The application collects the data ($card\_id_{Inpi}$, $card\_id_{MPInpi}$, t_1, t'_1, t''_1, t'_2, t''_2) into a tuple. The tuple is signed using RSA algorithm to form the evidence $e_{Inpi} = S_{NRK}$ ($card\_id_{Inpi}$, $card\_id_{MPInpi}$, t_1, t'_1, t''_1, t'_2, t''_2) and sent to HIS immediately.

CHAPTER FOUR
PERFORMANCE AND COST ANALYSIS

By comparing the general characteristics with the effect of EPC Gen-2 and EV1 label on the medical management process, Table 1 has been obtained. UHF and HF tags can be categorized under different standards but in all these labels a memory is integrated as embedded and the energy is supplied by the reader. HF cards are classified as proximity card. Also, UHF tags are widely known as EPC stickers. EPC stickers are generally used in supply chain operations, and proximity cards in the payment systems and library applications.

The most significant difference is the difference between the distances of the applications. Operation distances of HF labels are a few centimeters. On the other hand, operation distances of UHF tags are expressed in meters. This feature is considered as a disadvantage when it is considered for medical applications. Besides all, the reading distances of devices can be reduced by decreasing the antenna power of the readers. Another feature of the UHF tags is that they can be read by the fake readers from distance of a few meters. This feature will cause the message changes to be read by different readers when there is a change in messages (Lahtela, 2008). The same risk is not valid for HF labels. The most important reason for this is that the reading distance is only a few centimeters. When similar properties are considered, UHF tags which can read hundreds of labels at a short time. Although this property seems to be an advantage, it emerges as a disadvantage in medical applications. With this feature, it can read a lot of wristband tags and medpacks at the same time. The main feature desired in medical applications is checking and controlling one single patient and can be carried out the audit process. UHF tags may not exactly provide this feature at this point. Because of these, HF tags seem to be more suitable for medical applications.

Table 4.1 Comparison of Gen-2 and EV-1 label

Property	UHF EPC Gen-2 Tag	HF DesFire EV1 tag
Standard	ISO 18000-6	ISO/IEC 14443A
Scope	Contactless integrated circuit	Contactless integrated circuit
Supply Energy	No battery (passive)	No battery (passive)
Usage areas	EPC stickers	Proximity card
Area used	Supply chains	Payment, library
Operating Distance	Up to 7m	20-100 mm
Tags read	1000 tags/s	1 tag/s
Operating frequency	860-960 MHz	13.56 Mhz
Memory Capacity	512 bit on chip	2, 4, 8 kB NV-memory
Authentication	⊕	AES
Data Integrity	16 bit CRC, framing	16/32 bit CRC, parity, bit coding, bit counting, MAC, CMAC
Mobile device support	Limited	Widely available

Because all these standards are not based on a license infrastructure, operation frequencies of UHF and HF labels of industrial scientific medical (ISM) bands vary. There are many disadvantages of UHF frequencies at this point (Najera, Lopez and Roman, 2011). First, in UHF tags, human body completely blocks reading structure. Secondly, UHF tags have the problem of inability to read correctly when they touch each other. This feature causes UHF tags not to read correctly, particularly medical drug labels (med pack). Finally, the frequency bandwidths and transmission forces of UHF tags can't draw conclusions homogeneously around the world. Our study results showed that HF tags do not have these disadvantages. Moreover, the fact that HF tags are in the standards of ANSI / IEEE 95-1 can be presented as a plus. EV1 integrated circuits have a larger memory than the UHF tags. EV1 which has a large memory structure makes it possible for the critical data to be stored or evidence about safety to

be kept or managed. Being able to keep this evidence about safety is seen as a huge advantage in the EV1. In addition, future protocols or extended user applications show that development of the EV1 is advantageous and more _____ when it is considered it has a larger memory.

The most important difference between these two tags types used today is that they have different safety priorities and features. In the literature review conducted on UHF tags, it was proven that encryption functions such as XOR, PRNG or CRC were effective in the capture of data on the UHF tags in a very efficient way. On the other hand, proposed EV1 label structure and cards were designed on AES engine in the structure of 3-way-mutual-authentication and with mobile application that design has been brought to life.

Another security requirement is to support the realization of exchanging messages between other tags in a safe way. EV1 tags allow many different messages to be transferred safely with their integrated algorithms. Safety comparison considering this feature is presented in Table 4.2.

Table 4.2 - IS-RFID and NFC IMS-Cost analysis

	Equipment Required		Price/Unit ($)		Initial ($) Investment	Yearly Cost ($)
	Tags	Readers	Tags	Readers	Total	Total
EKATE	303,303	24	0.50	1027	176,300	17,630
IMS-NFC	304,975	8	0.623	199	191,591	19,159

The cost analysis we formed by taking into account the study made with UHF tags named EKATE are presented in Table 2 (Peris-Lopez et al., 2011). As it is seen in the cost analysis table, cost analysis which could be created in the hospital information systems (HIS) are shown. When creating the cost table, an eight-floor hospital, about 5000 inpatients per year was considered; and that each floor had three nurses and 3 unit-dose would be used for each inpatient. When these features are considered, it was calculated that there were annually 8x5000 = 40,000 and monthly ((5000 × 8)/12) 3,333 inpatients. Besides all these, there were labels for 3,333 inpatients in hospital

and moreover, there were 90 tags/inpatient for each med-pack. According to all these values, totally (3,333×90) 303,303 labels are needed. IMS system we proposed must be found in medical packs, each room's entrance and in carriers which carry the medical packs. In a situation where each floor has a med-cart and there is a total of 100 rooms (8+ (8 × 100) + (8 × 100)) 1608 extra labels are needed. On a floor where there are three nurses and five doctors, IS-RFID/EKATE system requires 303,303 labels. The needed number of IMS-NFC tags is 304,975.

Gen-2 tag costs are $ 0.5 / price tag. It includes the cost of plastic packaging price for each unit-dose. The prices of tags in other standards which are equal to EV1 packs have $ 0,421-0,825 price range. In our calculations, an average price of a tag is $ 0,623. According to this cost structure, it was calculated that the cost of IS-RFID / EKATE system with UHF in the publication presented in the recent study was $ 151,652 and the general cost of IMS-NFC system we proposed was $ 189,999.

Integration of UHF tag readers to mobile devices are not used very widely. Besides, it is known that in the recently developed mobile devices, there is NFC support (Lahtela, 2008). The price of the tablet with NFC support is around $ 199. In addition, the price of the UHF tag reading device is determined to be about $ 1000. According to all these values, when the two systems are compared again, it was calculated that IS-RFID / EKATE have the additional cost of around $ 24,648 and that IMS-NFC have an additional cost of around $ 1,592.

As a result, all the institutional costs of IS-RFID/ EKATE system are $ 176,300. The entire cost of IMS-NFC was calculated as $ 191,591. If equipment failures in the rate of around 10% and problems in the labels are taken into account, on an annual basis, the IS-RFID / EKATE has an additional cost of (15,165 + 2,465) $ 17,630 / year. The annual additional cost of IMS-NFC is (19,000 +159) $ 19,159 / year. At the end of three years, IMS-NFC we proposed will reach a cost of $249,068 in an installed system and IS-RFID / EKATE's cost will reach $ 229,190. On an annual basis, it will be $ 6,626 cheaper. When viewed on an annual basis, an additional cost of $ 6,626 is not seen as a very large figure for a hospital when security and prevalence are

considered. When the fall in the price of NFC tags over the years is taken into account, these figures will not cause much trouble. The security features of EV1 tags which do not exist in the UHF tags will offer great advantages if they are calculated as cost/safety ratio. If human life is considered, this measurement cannot be calculated numerically. The protocol analysis values of IMS-NFC system are presented in Table 4.3.

Table 4.3 - IMS vs. NFC protocol analysis

	IS-RFID	EKATE	Wu et al.	IMS-NFC
Technology	UHF	UHF	UHF	NFC
ANSI/IEEE 95-1 Compliance	No	No	No	Yes
Interference	Yes	Yes	Yes	No
Proposed Scope	Full	Protocol	Protocol	Full
Full Actor Authentication	No	No	No	Yes
Sym. &Asym. Encryption	No	Yes	No	Yes
Evidence on Actors	No	No	No	Yes
Hash	No	No	No	Yes
Full Disclosure Resistant	No	Yes	No	Yes
Cost Range, Trend	Medium, Stable	Medium, Stable	Medium, Stable	Medium, Dropping

CHAPTER FIVE
SECURITY ANALYSIS

For the safety of the health system, as in other systems, there may be attacks in various areas. Different attacks can lead to different losses. Nevertheless, our aim in the health field is zero errors or zero loss of life. In the safety analysis, proposals of EKATE system suggested that the patient was not given harm. However, as a result of security attacks we made, it was shown that there could be different problems.

In the proposed IMS-NFC authentication and pairings of tablets with the doctors and nurses are unique. In addition, secret information of inpatients are protected by ISO standard. Tags in NFC type are protected with AES-based mutual authentication scheme. Special names, passwords, labels, private keys and secrets complete all the system's security. NFC tag reading distances we chose for the study seems to be an appropriate choice that prevents many ill-intentioned situations.

5.1 General Security Services of IMS-NFC

Data Integrity: All channels are controlled mainly for the integrity of the data. EV1 labels include many algorithms we have stated in Table 1. Data exchanges between tags and tablets are protected by MAC additions. Similarly, messages created by the nurse/signed proof goes to a TLS tunnel. Any changes are determined by public-private keys held on HIS side. Therefore, data integrity is met with IMS-NFC.

False Proof: IMS-NFC resists false evidence in three ways. First, the evidence generated by nurse is signed, using her password created by the private key. The tablet of the nurse was confirmed and mapped at HIS side before a proof was found. Second, the evidence as recommended, is created within a time window defined by the HIS. Thirdly, the time stamps of the labels on the inpatient and the time stamps of the med pack labels are copied and stored in the system. All the time data are saved on the server.

Data Confidentiality: Exchange of confidential data or confidentiality of the information stored is of paramount importance. No message or key is transmitted as plain text in the proposed protocol structure. In the process of exchanging data between tags and tablets, AES algorithm is used. The exchange of data between the tablets and the server passes through the TLS tunnel and some evidence about drugs and some of the messages are signed using the RSA algorithm. Therefore, with a remote difference, IMS-NFC carries out data processing with a better privacy than its predecessor.

Advanced Security: IMS-NFC system guarantees the security of data in the data communication infrastructure. This is obtained with natural production of the session key in EV1. The generated session key always occurs independently according to the earlier new session key. This key secretly formed at the end of a three-way authentication and it certainly does not exchange data as a plain text. Communication in the past is indecipherable without this key.

5.2 Evaluation of Possible Security Attacks On IMS-NFC

Impersonation Attack: It occurs when there is an attacker in the system without being noticed. The attack is possible in the case of his attaining the secret message content in advance. Otherwise, message reception cannot be realized without a person proving the secrets. Because the receiving the secrets of IMS-NFC is not possible, impersonation of this identity is not possible. In the case of impersonation of that identity, attacks could be occurred. Sometimes, the evidence of both sides was shown successful with third-party evidence generation evidence which are independent from others. Therefore, it is recommended that recent evidence be connected to the values calculated according to other tags (Peris-Lopez et al., 2011). In cases where time confirmatory is stored for a label, it is possible to control the attack. This case applies to the IMS NFC. Therefore, it is not possible within the protocol proposed for the impersonation attack.

Full-Disclosure Attack: This attack reveals all the secrets of a party that participated in the communication. In communication the ways to use these secrets are opened. In

the protocol we propose AES, a new session key, a shared three-way authentication phase is used. Up to now, AES keys are the best way for us because it passwords cannot be broken. In short, the communication of IMS-NFC message have been made secure.

Identity Tracking - Privacy Attack: This attack involves monitoring a person who violates privacy. It is not necessary to catch the identity of a person. Simply, a message can be monitored by monitoring the hard tag identity. $Card\_id_x$ of a patient is fixed, and can be monitored in the proposed scheme. But in contrast to a UHF tag, an NFC tag can't be read from a distance. Therefore, physical attacker must touch the patient to keep track of him. It is obvious that a hospital environment is outside the model of an attacker as he cannot touch the wristband of patients freely. Moreover, EV1 card also has the ability to respond with random numbers; this method cannot be used in our proposal.

Man-in-the-middle attack: This attack involves an active attacker of a communication who mediates between the parties. NFC technology has denied the physical conditions-existence of multi-participants because it is not possible that there is such an active attacker and he intervenes. Even if they exist, cryptographic secrets indicating that messages are safe are needed for the attacker. In addition, all actors in the protocol can be open/trustable to only people working in the hospital.

De-synchronization attack: Because of the NFC, IMS-NFC is resistant to de-synchronization attacks. Messages and a different value tags cannot be blocked by the parties to update the stored time data. In addition, logging methods such as the

improved data integrity control mechanisms and storing the old values on the server, are used (Peris-Lopez et al., 2011). At this point, there must be a person having an ID card, a user name, a password and all the features of the card holder. This is regarded as a case that is not possible to happen in the system. Progress with a system which could be imitated is not possible in these restrictions.

DOS Attack: This attack is not likely to happen IMS-NFC because the physical attacker cannot come near the permanent label. In fact, the label cannot give a proper answer because of the mutual three-way authentication and communication falls if transactions fail.

Replay Attack: The attack works by repeating the whole of a pre-recorded message to fool the system in order to set up a new communication session. After the attacker sets up the illegal session, he tries to get the secrets of the system. To prevent this attack, there should be no constantly repeated, fixed or predictable answer. Therefore, fresh random numbers to use in similar inputs and algorithms producing random values are required. In our proposal it was shown that the only reproducible message was fixed $card\_id_x$. However, secret key information is required in the system after playing the $card\_id_x$. There cannot be any transactions without a password in order to obtain the messages because without the key, authentication will stop.

CHAPTER SIX
CONCLUSIONS

In this project, a solution with medical care in committee active in the field of patient care and hospital planning process set by controlling the structure of drug distressing followed in practice was suggested. The need for patient safety in order to avoid damage caused to patients in the care process should be a priority. JCAHO (Joint Commission on Accreditation of Healthcare Organizations) in all hospitals require that "five rights" methods should be valid. These methods are right patient, right drug, right dose, right time and right method. This method of quality processes in health should be properly applied. The different supply tracking technology commonly used today in the treatment processes (RFID and NFC-based) are discussed. In terms of standards HL7 data in 55 countries to exchange health information systems, data integration, definition of rules to be applied as a standard accepted in access to data and health data exchange is made. Also commonly used as standards in XML-based messaging standard workflow emerges.

In the project, a safe patient follow-up operation with NFC technology monitoring, verifying patient identity, establishing a secure bond between the patient and the people who care, prevention of medication errors were conducted to ensure the control of the use of essential drugs with no hospital that are not in.

This project is realized with the follow-up of inpatients within our country and that cause different problems in hospitals has contributed in order to troubleshoot. The operation of the system with the proposed security infrastructure has been scientifically proven. In addition, overall implementation of the system by pouring into practice the theory presented solutions will be done by evaluating the results of the planned mobile application development. The project with the most significant improvements of the patients in hospital medicine will add to the follow-up process which will be beneficial to human health. It will also create the concept and feasibility

of the development of technological infrastructure at university, with awareness and will provide a positive value for the sector development in the country's economy.

With the help of scientific studies and application solutions, in the first process of making way for hospitals to track equipment in different systems can be implemented at a later stage in the management of patients with the drug will be opened. Use of these methods is also provided in the university accumulation. Also fitting pace with developments in Android-based mobile systems are working on a solution software.

REFERENCES

Wolcott, J., Bootman, J. L., &Cronenwett, L. R. (2007). *Preventing medication errors* (367-408). Washington: National Academies Press.

Kaushal, R., Bates, D. W., Landrigan, C., McKenna, K. J., Clapp, M. D., Federico, F., et al. (2001).Medication errors and adverse drug events in pediatric inpatients. *Jama*, *285*(16), 2114-2120.

Eurobarometer (2006).*Survey on medical errors*.Retrived April 23, 2013 from http://ec.europa.eu/public_opinion/ archives/ebs/ebs_241_en.pdf.

Shojania, K. G., Duncan, B. W., McDonald, K. M., &Wachter, R. M. (2002).Safe but sound: patient safety meets evidence-based medicine. *Jama*, *288*(4), 508-513

Aronson, J. (2009). Medication errors: what they are, how they happen, and how to avoid them.*QJM*, 102(8), 513-521.

Benner, P., Sheets, V., Uris, P., Malloch, K., Schwed, K., & Jamison, D. (2002). Individual, practice, and system causes of errors in nursing: a taxonomy. *Journal of Nursing Administration*, *32*(10), 509-523

Lahtela, A., Hassinen, M., &Jylha, V. (2008).RFID and NFC in healthcare: Safety of hospitals medication care.*In Pervasive Computing Technologies for Healthcare, 2008.PervasiveHealth 2008. Second International Conference on* (241-244). IEEE.

Yao, W., Chu, C. H., & Li, Z. (2012).The adoption and implementation of RFID technologies in healthcare: a literature review. *Journal of medical systems*, *36*(6), 3507-3525.

EPC Global Inc. (2008).*EPC Global Class1 Gen2 RFID Specifications*.Retrieved May 21, 2013 from http://www. alientechnology.com/docs/AT_wp_EPCGlobal_WEB.pdf.

Inf technology (2010). Radio frequency identification for item management -Part 6: *Parameters for air interface communications at 860 MHz to 960 MHz*, http://www.iso.org/iso /iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46149. Accessed 21 May 2013.

Juels, A. (2004). "Yoking-proofs" for RFID tags. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on* (138-143).

Wu, F., Kuo, F., & Liu, L. W. (2005).The application of RFID on drug safety of inpatient nursing healthcare.In *Proceedings of the 7th international conference on electronic commerce* (85-92)

Sun, P., Wang, B. and Wu, F. (2008).A New Method to Guard Inpatient Medication Safety by the Implementation of RFID. *Journal of Medical Systems*, 32(4), 327-332.

Chen, C. L., & Wu, C. Y. (2012).Using RFID yoking proof protocol to enhance inpatient medication safety. *Journal of Medical Systems*, *36*(5), 2849-2864.

Huang, H. H., & Ku, C. Y. (2009).A RFID grouping proof protocol for medication safety of inpatient. *Journal of Medical Systems*, *33*(6), 467-474.

Chien, H. Y., Yang, C. C., Wu, T. C., & Lee, C. F. (2011).Two RFID-based solutions to enhance inpatient medication safety. *Journal of Medical Systems*, *35*(3), 369-375.

Yen, Y. C., Lo, N. W., & Wu, T. C. (2012).Two RFID-based solutions for secure inpatient medication administration. *Journal of Medical Systems*, *36*(5), 2769-2778

Van Deursen, T., & Radomirović, S. (2009).Algebraic attacks on RFID protocols.In *Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks* (38-51). Springer Berlin Heidelberg

Khovratovich, D., & Nikolić, I. (2010, January).Rotational cryptanalysis of ARX.In *Fast Software Encryption* (333-346).Springer Berlin Heidelberg.

Özcanhan, M. H., & Dalkılıç, G. (2013).Mersenne twister based RFID authentication protocol. *Turkish Journal of Electirical Engineering and Computer Science, in published*

Peris-Lopez, P., Orfila, A., Hernandez-Castro, J. & van der Lubbe, J. (2011).Flaws on RFID grouping-proofs. Guidelines for future sound protocols. *Journal of Network and Computer Applications*, 34(3), 833-845.

Chien, H., Yang, C., Wu, T. and Lee, C. (2009).Two RFID-based Solutions to Enhance Inpatient Medication Safety.*Journal of Medical Systems*, 35(3), 369-375.

Peris-Lopez, P., Orfila, A., Mitrokotsa, A., & Van der Lubbe, J. C. (2011).A comprehensive RFID solution to enhance inpatient medication safety.*International Journal of Medical Informatics*, *80*(1), 13-24.

Wickboldt, A. K., & Piramuthu, S. (2012). Patient safety through RFID: Vulnerabilities in recently proposed grouping protocols. *Journal of Medical Systems*, *36*(2), 431-435

Ozcanhan, M. H., Dalkiliç, G., & Utku, S. (2013). Analysis of two protocols using EPC Gen-2 tags for safe inpatient medication. In *Innovations in Intelligent Systems and Applications (INISTA), 2013 IEEE International Symposium on* (1-6).

Özcanhan, M. H., Dalkılıç, G., & Utku, S. (2013). Is NFC a better option instead of EPC Gen-2 in safe medication of inpatients.In *Radio Frequency Identification* (19-33).Springer Berlin Heidelberg.

Kasper, T., von Maurich, I., Oswald, D., &Paar, C. (2011). Chameleon: A versatile emulator for contactless smartcards. In *Information Security and Cryptology-ICISC 2010* (189-206). Springer Berlin Heidelberg

Peris-Lopez, P., Safkhanim, M., Bagheri, N., &Naderi, M. (2013). RFID in eHealth: How combat medications errors and strengthen patient safety. *Journal of Medical Biological Engineering, 33*(4), 363-372

Wu, S., Chen, K., & Zhu, Y. (2012). A secure lightweight RFID binding proof protocol for medication errors and patient safety. *Journal of Medical Systems,36*(5), 2743-2749.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., et al. (2007). *PRESENT: An ultra-lightweight block cipher* (450-466). Springer Berlin Heidelberg.

Najera, P., Lopez, J. and Roman, R. (2011). Real-time location and inpatient care systems based on passive RFID. *Journal of Network and Computer Applications*, 34(3), 980-989.

King, A. (2001). *The primary health care strategy*. Wellington: Ministry of Health.