Mobile Application for Secure Healthcare System

SABINA YESMIN

Master of Science Thesis
Stockholm, Sweden 2013

TRITA-ICT-EX-2013:78
Abstract

Usage of mobile applications and wireless networks is growing rapidly at different sectors in the world. Mobile healthcare application is devotedly accepted by the healthcare organizations and also by patients. The reasons behind accepting mobile healthcare applications are as user friendly, reliable, low cost, time efficient, mobility etc. Though the use of mobile applications is rising day by day in the healthcare sectors still those applications are not completely secure to prevent disclosure and misuse of patient’s sensitive data. However, security issues in healthcare applications get attention by many organizations.

In this thesis we have presented an integrated architecture for secure mobile healthcare system. This application provides management of patient medical records in a regional environment. Our mobile application is developed for Android platform. This solution is secure enough, because it fulfills important security requirements: integrity, confidentiality and availability.

Keywords: Mobile healthcare, wireless network; security; privacy; encryption; authentication and data confidentiality.
Acknowledgments

First of all I would like to show gratitude to my thesis supervisor Prof. Sead Muftic for his valuable supervision and also for giving me an opportunity to work with this interesting topic under his supervision and also support me during the entire period of my thesis.

I would like to thank to all of my friends, the team of SecLab and my teacher in Communication Systems for their help and guide throughout the thesis period and also in my study period in KTH- Royal Institute of Technology.

I am also grateful to my parents for their continuous support, love and for their good wish and also thanks to my lovely two sons Sadin and Sabin for their great support. Very special thanks to my beloved husband for his help and support.

Finally thanks to my almighty for always bless me.
To my parents
### Table of Contents

List of Figures ........................................................................................................................................ vii

Chapter 1: Introduction ........................................................................................................................... 1

1.1 Background ....................................................................................................................................... 1

1.2 Problem Statement ............................................................................................................................ 1

1.3 Goals and Activities ........................................................................................................................ 1

1.4 Deliverables ...................................................................................................................................... 2

1.5 Purpose ............................................................................................................................................. 2

1.6 Methodology .................................................................................................................................. 2

1.7 Audience ....................................................................................................................................... 3

1.8 Thesis Organization ........................................................................................................................ 3

Chapter 2: Existing Projects, Security Issues and Related Standards ..................................................... 4

2.1 Analysis of Existing Projects .......................................................................................................... 4

2.2 Security Considerations against Threats ......................................................................................... 5

2.2.1 Authentication ............................................................................................................................ 5

2.2.2 Authorization ............................................................................................................................. 5

2.2.3 Confidentiality .......................................................................................................................... 6

2.2.4 Data / Message Integrity ......................................................................................................... 6

2.2.5 Privacy .................................................................................................................................... 6

2.2.6 Accountability ......................................................................................................................... 6

2.2.7 Availability .............................................................................................................................. 7

2.2.8 Non-Repudiation .................................................................................................................. 7

2.3 Related Standards .......................................................................................................................... 7

2.3.1 HIPAA ...................................................................................................................................... 7

2.3.2 FIPS 196 ................................................................................................................................. 8

2.3.3 Data Protection Directive ....................................................................................................... 10

2.4 Cryptographic Mechanisms .......................................................................................................... 10
2.4.1 RSA .......................................................................................................................... 13
2.4.2 SSL/TLS .................................................................................................................... 13
2.5 Certification .................................................................................................................. 14
2.6 Wireless Communication Standards ............................................................................. 15

Chapter 3: Concept of an Integrated m-healthcare System .................................................. 17
3.1 Roles .............................................................................................................................. 17
3.2 System Architecture ....................................................................................................... 18
3.2.1 Internal Architecture of m-healthcare System ......................................................... 19
3.3 Message Flow ................................................................................................................ 22
3.3.1 Message Flow for Authentication ............................................................................ 22
3.3.2 Messages to book an Appointment ........................................................................ 23
3.3.3 Insert Prescription .................................................................................................... 25
3.4 Analysis of Security Features ........................................................................................ 26
3.4.1 m-healthcare Threats and Attacks .......................................................................... 26
3.4.2 Security Components ............................................................................................... 27

Chapter 4: Operations/ Use of the System ........................................................................ 29
4.1 Services Provided by the Application ............................................................................ 29
4.2 Modules in the Application .......................................................................................... 30
4.2.1 Registration Window .............................................................................................. 30
4.2.2 Login Window ........................................................................................................ 31
4.2.3 Patient's GUI Tree .................................................................................................. 31
4.2.4 Doctor's GUI Tree ................................................................................................ 32
4.2.5 Nurse's GUI Tree .................................................................................................. 33
4.2.6 Pharmacist's GUI Tree ......................................................................................... 34
4.2.7 Laboratory Technician's GUI Tree ......................................................................... 35

Chapter 5: System Implementation and Demonstration ...................................................... 36
5.1: Development Environment ......................................................................................... 36
5.1.1 Eclipse SDK .......................................................................................................................... 36
5.1.2 Java Programming Language ................................................................................................... 36
5.1.3 Android Mobile Operating System ........................................................................................ 36
5.1.4 MySQL Database .................................................................................................................... 37
5.1.5 PHP ........................................................................................................................................ 37
5.1.6 JSON Format .......................................................................................................................... 37
5.2 Relational Database Table ........................................................................................................... 37
5.3 Screenshots of the Admin Form for User Registration ................................................................. 38
5.4 Screenshots of User Login and Registration Screen ................................................................. 39
  5.4.1 Password Registration Screen ............................................................................................ 40
5.5 Patient Panel ............................................................................................................................... 40
  5.5.1 Patient Login and Home Screen ......................................................................................... 40
  5.5.2 Patient Appointment Options ............................................................................................. 41
5.6 Doctor Panel ............................................................................................................................... 45
  5.6.1 Doctor’s Home Screen ........................................................................................................ 45
  5.6.2 Doctor’s Appointment Options .......................................................................................... 45
  5.6.3 Check Specific Appointment ............................................................................................ 46
  5.6.4 Doctor’s Activities for a Specific Patient ........................................................................ 46
5.7 Nurse Panel ............................................................................................................................... 48
5.8 Lab Technician Panel ................................................................................................................ 48
5.9 Pharmacist Panel ....................................................................................................................... 49
Chapter 6: Conclusions and Future Work ...................................................................................... 50
6.1 Conclusions ............................................................................................................................... 50
6.2 Future work .............................................................................................................................. 50
References ....................................................................................................................................... 51
List of Figures

Figure 2.1 Mutual Authentication Protocol [20] ........................................................................................ 9
Figure 2.3 Hash Function [27] .................................................................................................................. 12
Figure 2.4 X509 Certificates ..................................................................................................................... 14
Figure 3.1 m-healthcare System Architecture ......................................................................................... 18
Figure 3.2 Internal Architecture of m-healthcare System ........................................................................ 20
Figure 3.3 Message Flow for Authentication ........................................................................................... 23
Figure 3.4 Message Flow for book an Appointment ................................................................................ 24
Figure 3.5 Message Flow for insert Prescription .................................................................................... 25
Figure 3.1 Relational Database of the System ......................................................................................... 38
Figure 5.1 Registration Window for Users ............................................................................................... 31
Figure 5.2 Login Window with the Initial Window of Different Kinds of User ........................................ 31
Figure 5.3 Detail GUI Tree for a Patient ................................................................................................... 32
Figure 5.4 Detail GUI Tree for a Doctor .................................................................................................... 33
Figure 5.5 Detail GUI Tree for a Nurse ..................................................................................................... 34
Figure 5.6 Detail GUI Tree for a Pharmacist ............................................................................................. 34
Figure 5.7 Detail GUI Tree for a Laboratory Technician ........................................................................... 35
Figure 5.8 Patient Home Screen ............................................................................................................... 41
Figure 5.9 Patient Login Screen ................................................................................................................ 41
Figure 5.10 Book a Doctor Screen for Patient .......................................................................................... 42
Figure 5.11 Book a Nurse Screen for Patient ................................................................. 42
Figure 5.12 Laboratory Area Choice for Patient ............................................................ 42
Figure 5.13 Book a Laboratory ...................................................................................... 42
Figure 5.14 Appointment List Sorted by Date of Appointments ...................................... 43
Figure 5.15 Single Appointment Detail .......................................................................... 43
Figure 5.16 List of Appointments for Cancelation ............................................................ 43
Figure 5.17 Appointment Detail for Cancelation .............................................................. 43
Figure 5.18 Personal Medical Records .......................................................................... 44
Figure 5.19 List of Prescription Sorted by Creation Date .................................................. 44
Figure 5.20 Single Prescription Detail ............................................................................ 44
Figure 5.21 View Doctor’s Comment Detail ..................................................................... 44
Figure 5.22 Doctor’s Home Screen .............................................................................. 45
Figure 5.23 Doctor’s Appointment Options ..................................................................... 45
Figure 5.24 Search Specific Patient .............................................................................. 46
Figure 5.25 Specific Patient’s Details ............................................................................ 46
Figure 5.26 Doctors Activities for a Specific Patient ....................................................... 46
Figure 5.27 Prescription Option ..................................................................................... 47
Figure 5.28 Create Prescription .................................................................................... 47
Figure 5.29 Create Comments for a Specific Patient ....................................................... 47
Figure 5.30 Nurse Home Page ..................................................................................... 48
Figure 5.31 Laboratory Home Page .............................................................................. 49
Figure 5.32 Pharmacy Home Page .............................................................................. 49
List of Abbreviations

PIN – Personal Identification Number
FIPS – Federal Information Processing Standards
PIV – Personal Identity Verification
CA – Certificate Authority
DES – Data Encryption Standard
MAC – Message Authentication Code
RSA - Rivest, Shamir and Adleman
PKI – Public Key Infrastructure
SHA - Secure Hash Algorithm
NSA - National Security Agency
PKC – Public-Key Cryptography
IDMS – Identity management Server
SECLAB – Security Laboratory
IPS – Identity Provider Server
TCP – Transmission Control Protocol
SA – Strong Authentication
SSL – Secure Socket Layer
AOP - Aspect Oriented Programming
HTML – Hyper Text Markup Language
APDU - Application Protocol Data Unit
API – Application Programming Interface
DS – Digital Signature
HCSP– Healthcare Service Provider
DB– Database
Chapter 1: Introduction

1.1 Background
The use of information technology within the healthcare domain is increasing day by day all over the world. Previously, mainly devolved countries were using computers and their devices within the healthcare domain. But nowadays developing countries are also moving towards it. Coverage of mobile networks in most of all areas in a country makes everyone interested to use mobile phones. And within the last few years the uses of smart phones drastically increased. Due to this change, user community is pushing for development of mobile applications. Now user can use most of all desktop applications in their smart phones. Even healthcare service providers and patients are feeling comfortable to use mobile devices for patient records and/or patient diagnostic process. The use of mobile phone within the healthcare domain is called m-healthcare. An m-healthcare application can be used by patients as well as by physicians.

1.2 Problem Statement
The area of healthcare is involved with handling of patient sensitive data. Security and privacy of these data is very important. While doing online transfer of these secret data over the public network, it can be viewed and/or modified by the attackers. It can be also accessed by unauthorized persons who can break privacy of the patient's data. Patient's private data can be viewed by third party from the device if the handheld is lost.

1.3 Goals and Activities
The main goal of this project is to develop an m-healthcare application that will provide secure, trustful and reliable communication for different communities in healthcare area. We have planned to develop an application that will provide interface to both physicians and patients. It will be an application that will be secure from the three important types of threats. As we have discussed above, the three types of major threats are (1) Threats that attack during network communication, (2) Unauthorized access to data and (3) Third persons access to the device storage data, if the device is lost or using some malicious software. In our software we will eliminate the threat during the communication by encrypting and decrypting data transferred between mobile devices and the data server. Using authentication and role based
access control, we shall protect application from unauthorized access. We shall protect our device data from the third party by using device level data encryption.

1.4 Deliverables
We have designed the complete architecture of the m-healthcare application which shows the entities involved in a healthcare application and their access roles. It is an Android application. A laboratory assistant will be able to enter patient diagnosis data to the server. The physicians will have access to patient's data, make necessary comments on it and also be able to create prescriptions for them. A patient will be able to view his diagnosis report, view the physician's comments and the prescriptions for him/her. The Medicine Store workers will be able to access the patient's prescriptions, to sell the proper medicine using his mobile device. Within the architecture a Java server will be used as a gateway for accessing patient's data from all mobile devices.

1.5 Purpose
The purpose is to develop an m-healthcare application that makes our life easier and saves our time. People have a tendency to mistrust security functionality strength of m-healthcare applications and are worried about it. Aim of this project is to provide a secure and trustful m-healthcare application, so that users can use this application for their sensitive data without any doubt of security threat. It is also a user friendly application, so users can easily use the application.

1.6 Methodology
In this research, we have used design science research methodology (DSRM). As per Kan et al.[35] “The DS process includes six steps: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication”. The main reason why we choose this method is because we have followed the same steps in our research. First we have identified the problem area, and then we have defined the objectives for the solution of the problem with studying the related technologies. After that we have designed a secure m-healthcare application. We have also developed a prototype of the design and then we have demonstrated our solution. We have tested the application in lab environment. The last step of the DSRM is the future work of this research.
1.7 Audience

This document is aimed at any potential or succeeding person who has good background in computer science or engineering field. It is also suggested that they have an interest in the area of computer and mobile security.

1.8 Thesis Organization

There are six chapters in this document. In this chapter problem, goal, purpose and methodology are described. Below we describe the main theme of the next chapters.

Chapter 2: Existing Projects, Security Issues and Related Standards: It describes related standard and technology, security consideration, cryptography mechanisms and certification in existing projects and also analyses functionality and security of healthcare related existing projects.

Chapter 3: Concept of Integrated m-healthcare System: This chapter illustrates the role of users of m-healthcare system and also describes the system architecture of this system and describes the working procedure of this system.

Chapter 4: System Implementation: The chapter describes the implementation of this application and also describes the services and modules in the application.

Chapter 5: System Implementation and Demonstration: This chapter demonstrates different developing environments that are used to implement the m-healthcare application and also contains description of screenshots of the mobile client application.

Chapter 6: Conclusions and Future Work: conclusions of the thesis and its future work are discussed in this chapter.
Chapter 2: Existing Projects, Security Issues and Related Standards

There are several relevant standards and solutions in the developing field of m-healthcare services. This chapter presents security issues and standards utilized in existing projects and also describes related standards used in this thesis.

2.1 Analysis of Existing Projects

As per user needs different application developers are developing m-healthcare application. SCHS is one of them [2]. In SCHS (smart card healthcare system), they developed smart card base of healthcare system. In this system smart card is used for patient information, health data transfer and also data communication. The system developed data communication using distributed protocol. They implemented two smart card software modules. One smart card module is used by patients that is used to load personal information and general patient health information and another is used for healthcare professionals. The system applied encryption keys and digital signature to data communication between client and database server. It is developed by Java platform. Here they used RMI channel in the top of TCP/IP for communication between doctor computer and database server. RMI doesn’t ensure all security requirements during network communication. After that, they used DSA and DES algorithm. But DES is potentially vulnerable to a brute-force attack [2].

They have designed and implemented mobile health care system by using mobile and RFID technology. They worked based on the healthcare problems in Korean healthcare system. This system prevents to issue false prescriptions. This system also provides 1 on 1 service, like it does not consider patients location and time. This system provides improved healthcare system in Korea. [3]

HealthGeat is a real time wearable system that provides patients monitoring services, visualizing and analyzing user’s blood oxygen level (SpO2), physiological signals, HR [4]. This system uses a set of physiological sensors. Here they applied Bluetooth wireless connection for sending physiological data to a cell phone. This system can store, transmit and analyze the collected physiological information and present it to the user [4].
MobiCare is a project area that provides remote monitoring patient care both in house as well as in open areas. It makes possible use of programmable and reconfigurable services. It provides remote registration, remote health data services, self-activities, self-repair with new health services. They have used Bluetooth and GPRS/UMTS network infrastructure [5].

The article "End-to-end secure communication in ad-hoc assistive medical environments using secure paths" focuses on a number of medical treatment services, like monitoring medical parameters, help on demand, alarm triggered, location-based monitoring and also security. They use PGP web of trust for trusted users’ community. This system provides security for distribution of medical information in a secure mode [6].

2.2 Security Considerations against Threats

There are several security concerns in the field of m-healthcare. In this system every data is very private and sensitive. So trust should be set up in every step between each participant. Security can be provided by using general cryptograph ideas. Below the cryptographic concepts are described.

2.2.1 Authentication

Authentication is a process that performs identity verification [13]. There are three types of authentication protocols: client authentication (here server verifies client identification), server authentication (here client verifies server identification), and mutual authentication (here client and server both verify each other identity). The three general ways for authentication factors is described below [13] [14]:

a. Something the participant has, example tokens, ID cord

b. Something the participant knows, example password, PIN

c. Something the participant is, example voice, Biometric

2.2.2. Authorization

Authorization is mechanism that checks permissions of a user for performing some actions. Once authentication process has completed, the next step is authorization. It defines access of an authenticated user in a policy or access control list. There are three methods for access handling of control lists. In mandatory method, computer system decides the access of user
for particular resources. In discretionary method, user makes the decision to access by other users for her/his created resources or files. The third method is role based access control. In this method, user’s access and privileges are determined by role [13].

2.2.3 Confidentiality
During communication process, data can be eavesdropped by third party. The eavesdropper can do any illegal action against the data. Confidentiality makes sure that only intended receiver reads data without attacking third party. It gives secure communication between sender and receiver. Encryption and decryption protect data against reading by third party. Encryption and decryption are performed by a key. There are two types of cryptographic systems based on keys: Symmetric key and Asymmetric Key. In Symmetric key cryptography encryption and decryption share the same key, but in Asymmetric key crypto, they use different keys for encryption and decryption.

2.2.4 Data / Message Integrity
Integrity is another important mechanism of data security. It ensures preventing data from modification or unauthorized change when data/ message is transferred between sender and receiver. Recipient can verify integrity by the attached hash value of original message. Prevention and detection mechanism are two classes of integrity. If any integrity of data is changed/ modified by unauthorized person in an illegal way, the prevention mechanism blocks the illegal attempt of modifying data. Detection mechanisms do not prevent unauthorized modification of data, but it only reports that the data integrity is no longer reliable [14].

2.2.5 Privacy
In most cases data is transferred via Internet between sources to destination. It is very common attack that the personal or private data is readable by third party. Privacy gives the assurance that data/ message is not readable by third party.

2.2.6 Accountability
Accountability can determine the attacker or principle of data/message [13].
2.2.7 Availability
Availability is a system that refers to use of resources or information by intended users. Unavailable system is as no system type. So availability is very important side of reliability and also for system design. [14]

2.2.8 Non-Repudiation
Non-reputation is a mechanism that provided undeniable transaction [13].

2.3 Related Standards
There are different types of standards and technologies which are used to make secure m-healthcare environment. These technologies ensure system security and trustworthiness.

2.3.1 HIPAA
The Health Insurance Portability and Accountability Act (HIPAA) is a standard for protecting patient confidential and sensitive health information. Department of Health and Human Services (HHS) of U.S. developed the HIPAA. HHS published HIPAA Privacy rule and HIPPA Security rule. HIPPA Privacy rule gives the privacy of patient individual information. HIPPA Security rule is used to guarantee confidentiality, integrity, and availability of patient electronic protected health information [16]. HIPPA improves effectiveness, protects private information and reduces cost to transfer data between one authorized entity to another [17]. HIPAA covers several standards or regulations as follows:

Standards for Electronic Transactions (EDI) and Code Sets:
HIPAA established specific role for electronic healthcare transactions and the coding standards between healthcare providers. It requires every provider who functions electronically to use the same healthcare transactions, identifiers, and code sets [17].

The Privacy Standard:
This standard is used to store, use and transfer any identification information of any individual patient. HIPAA privacy protects patient private information from any unauthorized person, like names, addresses, cities, phone numbers, fax numbers, e-mail addresses, web addresses, license numbers, zip codes, account numbers, and birth dates [1].
The Security Standard:
In this stage HIPAA requires security at different levels, like administration, technical and physical for protecting patient healthcare information. It guarantees confidentiality and integrity and availability of healthcare information [17].

NPI:
NPI is national provider identifier that has ten digit numbers for assigned provider identification. The provider identification number is provided by central Medicare & Medicaid Services [17].

2.3.2 FIPS 196
FIPS (Federal Information Processing Standards) is an entity authentication protocol based on public key cryptography and digital signature. It is a specification of mutual authentication protocol. The entity authentication depends on two types of verifications, 1. Verify claimant’s binding with its public/private key pair, and 2. Verify claimant’s digital signature of a random number challenge. This protocol prevents several threats, such as masquerade, password compromise, replay attacks, and the signing of pre-defined data [20].

Mutual entity authentication, shown in Figure 2.1, is described as follows [20]:

1) The initiator A sends on authentication request to the responder B.

2) The responder B decides if it will continue or terminate the authentication process. If it wants to continue to authenticate exchange with the initiator, then it generates a random number Rb and sends TokenBA1 to the initiator. Responder B sends a message to the initiator containing TokenBA1 and an optional TokenID.

3) The initiator A receives the message including TokenBA1. It uses TokenID to verify the receiving token. It retains the Ra. The initiator verifies the signature of random numbers Ra and Rb. Then the initiator creates an authentication token, TokenAB that have concatenating data and creates the signature.
After that the initiator A sends a message to responder B which contains TokenAB, a token identifier, the initiator's certificate CertA. The form of the message is:

\[ \text{[TokenID]} \| \text{[CertA]} \| \text{TokenAB} \]

4) After receiving the token ID, responder B verifies the value of Rb. If the value of Rb is the same as the value of step 2 Rb, then the signature verification is complete, or if the Rb value is not present, then the value retained in step 2 and uses the value to verify the signature process of step 4. Then it verifies initiator's certificates and signature. If the verification is OK, that is the initiator A is authenticated to the responder B. Otherwise, the responder B will terminate the authentication.

5) The responder selects an authentication token; TokenBA2 for the initiator A. TokenBA2 includes random number and generates a digital signature. The responder sends a message to Initiator A, which includes TokenBA2, token identifier, and the responder's certificate CertB. The form of the message is:

\[ \text{[TokenID]} \| \text{[CertB]} \| \text{TokenBA2} \]
6) Initiator A receives the message from the responder B including TokenBA2. Initiator verifies the received token that the value of Ra and Rb is present in the token using token ID. Then it verifies responder’s certificates and signature. If the verification is OK, that is, the responder B is authenticated to initiator A. In this way the entities perform mutual authentication.

2.3.3 Data Protection Directive
Protection of personal data is a crucial issue for medical healthcare applications. It is related to privacy of the patient. The European Union Data Protection Directive determines the rules for protection of private data and also for free movement of this data within the EU [22].

2.4 Cryptographic Mechanisms
Cryptography is a mechanism that has the ability to prevent message from being read by others when the message transfers from a sender to a receiver. Cryptography uses the mechanism to encryption and decrypt data. Integrity checking and authentication are also provided by cryptography [23]. Substitution and Transposition are general principles of all encryption algorithms. In the Substitution, every element of plaintext is mapped into other element and transposition reorganizes the elements of plaintext. But, the main requirement is that original information is not lost or changed [24]. There are three types of cryptography functions: asymmetric key or public key cryptography functions, symmetric key or secret key cryptography functions and hash functions.

2.4.1 Symmetric Key Cryptographic Functions
In symmetric cryptography sender and receiver both use same key for encryption and decryption process. This key is known as secret key. This secret key is shared between sender and receiver. Stream ciphers and block cipher are two types of symmetric key algorithms. Stream ciphers produce one output element for several input elements at a time. Block ciphers produce a block of elements at a time. There are several symmetric algorithms, such as Blowfish, DES, AES etc. [25].

An example of symmetric cryptographic mechanisms is the following [25]:

Encrypting message: \( E_k (M) = C \)

Decrypting message: \( D_k (C) = M \)
Here plaintext message (unencrypted) is defined as M. The plaintext message M is encrypted by Ek (E is the symmetric encryption and k is the secret key of the encrypted message) and C is defined as encrypted message (ciphertext). Then the ciphertext message C is decrypted by the receiver using the same secret key k and the receiver receives the original message C.

A serious problem of symmetric key cryptography system is key management over insecure communication channels. In symmetric systems it is necessary to send the key through secure channel or key must be encrypted. The key management problem is fully solved by public key cryptographic systems.

2.4.2 Asymmetric Key Cryptographic Functions

Message sender and receiver use different keys for message encryption and decryption process in asymmetric key cryptography system. Here one key is used as private key and it is kept private which is only known to the owner of the key. Another key is used as public key and it is stored in a register or other accessible file. Public key cryptography is also applied for key management and signature applications: keys exchange for symmetric cryptography and digital signature [25].

Mailbox analogy is an example of public key cryptography. Mail box is used as a public key where anyone can throw letter in to mail box. Only mailbox owner is the only person who has the mailbox key (private key) and only he/she can open the mailbox and get the letter with this key.

The brief description of asymmetric cryptographic mechanisms is the following [25]:

Encrypting message: \( E_{PuK}(M) = C \)

Decrypting message: \( D_{PrK}(C) = D_{PrK}(E_{PuK}(M)) = M \)

Sender uses receiver public key(\( PuK \)) to encrypt the message as \( E_{PuK}(M) \) and then sends the encrypted message to the receiver. When receiver receives the message, she/he uses her private key(\( PrK \)) to decrypt it as \( D_{PrK}(E_{PuK}(M)) \). Since only receiver knows her private key, no other receiver can decrypt the message.

2.4.3 Hash Function

Cryptographic hash function is a transformation that takes a variable size of message as input and product an output of fixed length message digest. It is very important for message
authentication and also for digital signature. Cryptographic hash function is one way function. Hash functions can be used for checking modifications of a message or code. Hash functions make signature schema more effective [24][26].

![Figure 2.2 Hash Function [27]](image)

For digital signature message \( m \) is first hashed as \( h(m) \) and then \( h(m) \) is signed in place of message \( m \). The output message \( h(m) \) is smaller than the input message. So the sender can sign \( h(m) \) more quickly than entire message. Therefore it is faster to create signature and requires fewer resources for transmission or storage.

Hash functions used for ensuring data integrity. Sender sends \((m, h(m))\) to the recipient through the communication channel. The recipient receives it as \((M, H)\). Than the recipient checks message whether it is altered or not. For that, the recipient calculates \( h(M) \) and compares it to \( H \). If \( h(M) \) is equal \( H \), than the message is not altered, otherwise the message is altered.

Hash function must have some properties, as follows [24][27]:

- Hash function can take any size of a block of data as its input.
- It gives a fixed size of output
- Message digest \( h(m) \) can be calculated very easily for any given \( m \).
Mobile Application for Secure Healthcare System, KTH

- Hash function is one way function: for a message digest \( x \), it is computationally infeasible to find a message \( m \) that satisfies \( h(m) = x \).

- It is computationally infeasible to find \( m_1 \neq m_2 \) with \( h(m_1) = h(m_2) \) for any given block of \( m \).

- It is computationally infeasible to find messages \( m_1, m_2 \) with \( h(m_1) = h(m_2) \). That is, two different messages should not result in the same hash value.

If any hash function fulfills the above first five properties, then it is referred as weak hash function. If it also fulfills the six the property, then the hash function is referred as a strong hash function.

### 2.4.1 RSA

RSA is a cryptographic algorithm based on elementary number theory. In the RSA cryptographic system, we need two large prime numbers. \( N \) is the part of public key which is the result of multiplication of two large prime numbers. The factors of \( n \) are used as a secret key. Every user has his/her public and secret key in RSA cryptosystem. RSA key generation algorithm follows three steps:

1. Choose large individual primes \( p \) and \( q \), and compute \( n = pq \).
2. Choose \( e \) that is prime to \( \phi(n) \). The pair \( (n; e) \) is published as the public key.
3. Compute \( d \) with \( ed \equiv 1 \mod \phi(n) \). \( (n; d) \) is used as the secret key.” [26]

The number \( n \), \( e \) and \( d \) are used as modulus, encryption and decryption exponent respectively. The respected user only need decryption exponent \( d \) to decrypt or generate digital signature. He/she doesn’t need to know large prime numbers \( p \) or \( q \). The number \( p \), \( q \) and \( n \) are the factors to give the security of RSA cryptography system. \( p \) and \( q \) are two large prime numbers. Factor \( n \) is an effective algorithm which is known as factoring assumption. Large prime number makes the system slower. Brute force attack is possible for RSA cryptosystem. The system can be more secure if the number of bits in \( e \) and \( d \) are large.

### 2.4.2 SSL/TLS

Secure Sockets Layer / Transport Layer Security (SSL/TLS) is designed to protect user-level process. It provides secure communication over the Internet. SSL/TLS allows mutual authentication between two parties and establishes session key for getting protection cryptographically in this current session. Transport Layer Security (TLS) is a protocol based
2.5 Certification

Certification is a process that provides electronic document of an entity to use all potential verifications in the communication field. Certification handles all functions of certificates. Certification also helps to create new certificate request, submit certificate request to the CA server, and receive back new certificate.

2.5.1 X509 Certificates

X.509 is a certificate format defined in a directory service. The directory has a set of servers. This server maintains a database that contains user’s information. X.509 is the heart of all standardized formats of certificates. It includes several values in the certificate field, as shown in Figure 2.3. The meaning of the certificate field is described below [24]:

![Figure 2.3 X509 Certificates](image)
**Version:** There are three versions of X.509 certificate format. So it is necessary to state version number for different code.

**Serial number:** It is integer number. It is unique within the issuing CA.

**Signature algorithm identifier:** It is used to sign the certificate with any associated parameter.

**Issuer name:** It is the X.500 name of the CA that created and signed the certificate.

**Period of validity:** It indicates valid period of a certificate.

**Subject name:** “The name of the user to whom this certificate refers”[24].

**Subject’s public-key information:** It includes public key of the subject and identifier of the algorithm.

**Issuer unique identifier:** A string field used to identify uniquely the CA that issued the certificate.

**Subject unique identifier:** A string field used to uniquely identify the subject.

**Signature:** It contains the hash value of all other fields of the certificate, encrypted with the CA’s private key. The CA uses its private key to sign the certificate. The user can verify the certificate’s validity by using CA’s public key.

### 2.6 Wireless Communication Standards

There are different wireless communication standards that need to be defined in this thesis, because they are very much related to the m-healthcare technology.

**Internet**

In this m-healthcare system, user can use mobile internet in his/her mobile device or user can use provider Internet to their mobile.

**Bluetooth**

Bluetooth is a wireless short range communication system. It is a simple system and it maintains high level of security. Bluetooth has the ability to simultaneously handle data and voice transmissions. A master device can connect with several devices to make a network. There are two devices: master and slave. According to their connection agreement, one device
acts as a master device and others are slaves. Data transfer can be made from the master device to other. The range of Bluetooth technology is application specific [28].

**HTTP**

HTTP (Hypertext Transfer Protocol) is used as a request-response or server-client protocol in hyper media information systems. HTTP is stateless protocol [25]. The server doesn’t uphold any information between two connections. “In general, an HTTP server may act as an origin server, proxy, gateway, or tunnel.”[25, p-259]. In layering, HTTP uses SSL and TSL as a sub-layer. HTTP handles two attacks, eavesdropping and man-in-middle attack.
Chapter 3: Concept of an Integrated m-Healthcare System

A healthcare application can be used by different types of end users like the doctors, the nurses, the laboratory technicians, the pharmacist and obviously the patients. All of this kind of users need to access patients data which may be entered by one type of user and accessed by some other type of user. As a result of this situation we need an integrated m-healthcare application which will make the healthcare application users’ life easier. This chapter illustrates the roles of different types of healthcare application users. We have also described system architecture of an integrated m-healthcare system and the working procedure of this architecture.

3.1 Roles

In a healthcare organization there are different types of users/staffs (doctor, nurse, lab tech, pharmacist, administrator and patient). Different users have different roles in this system.

Doctor: Doctor performs different functions, such as create appointment with a patient, check appointment, create prescription (for medication and for laboratory), create comment about patient health, and check previous health record of a patient.

Nurse: Nurses create appointment with patient, check appointment, remark any important health situation of a patient in the comment line and also check patient’s health record.

Lab Technician: Lab technician can check the prescription or can input the tested data in the field of test result.

Pharmacist: Pharmacist can check the specific prescription of a specific patient and also can input sold medicines in the specific field.

Patient: Patient has different kinds of jobs, like create appointment with a doctor or nurse, check appointment, cancel appointment, book a time with a diagnosis center), check his/ her health records, etc.
3.2 System Architecture

The designed architecture ensures a secure and complete m-healthcare system. Secure m-healthcare system involves several components which assist secure environment. Different types of users use this system, like patient, doctor, nurse, lab technician, pharmacist and administrator. The first requirement of this system is that every user must have mobile application and Internet connection. To use this system every user connects through the communication server via Internet. The users are authorized through the communication server. Then the valid user can use the system by their assigned role.

![Image](image_url)

**Figure 3.1 m-healthcare System Architecture**

There are different components in this mobile healthcare system with different functionality.

**Client Unit**

Every user requires a mobile unit with Internet connection. User need to have this m-healthcare application in order to communicate with the healthcare server. Every user can get/serve the healthcare services by using this unit.
Internet
Here the user can use Internet service from provider of Internet or mobile operator (which provides GPRS/UMTS access for Mobile Unit) Internet.

Healthcare Server System
Secure healthcare server has four components in this architecture. The four components are: healthcare database, communication server, secure policy server, and IDMS server. These healthcare servers provide secure healthcare services to every healthcare user.

Hospital Database Server
In this project we use one database server. The database server is a storage device. All users’ (patient, doctor, nurse, lab technician, etc.) detail information is store here in this database. Patient’s activities and medical records are also stored in the database.

Certificate Authority (CA Server)
Certificate authority is a trust entity that issues certificates. Certificates contain owner’s public key and owner’s identity. At first CA verifies applicant’s credentials, than issues applicant’s certificate. So other users can trust applicant information included in CA certificate. Certificate contains owner's public key, owner's name, expiration date of the certificate, and other information of the owner.

3.2.1 Internal Architecture of m-healthcare System
The internal architecture of m-healthcare system consists of different components which comprise secure m-healthcare server. It has six different types of GUIs, which enable different kinds of user access to the healthcare database. In Figure 3.2 we see internal architecture of m-healthcare system.
Components of the System Architecture

Secure healthcare server comprises all the main components. Different types of users use healthcare data by login in to this server. The secure healthcare server has ten components. Six of these components are used for services to six different types of users. The rest of the four components are communication server, security policy server, IDMS server, and the main healthcare database server.

Components of the secure m-healthcare server are as follows:

1. Communication server: The communication server works as a bridge between users and the healthcare database. All the APIs that provide services to the mobile GUIs are connected to this server management component. Whenever a user tries to use the healthcare database, communication server works as a bridge to checks security constrains for the user with the help of security policy server and IDMS server.

2. Security policy server: Healthcare security components hold different security constrains for different type of users. Security constrains are assigned in the security
policy server. Users are authorized to the data in the healthcare database server through this security policy server.

3. Healthcare database server: Healthcare database server holds patients’ sensitive healthcare data. Different kinds of users use these data through the communication server component.

4. IDMS: Identity Provider Server (IPS) is responsible to manage identities.

5. Administration service API: Administration service API provides services to the admin application GUI. The administrative users of this application insert the detail information of the users.

6. Lab technician service API: Lab technician services APIs are responsible to provide services to the lab technician mobile GUI.

7. Nurse Service API: The nurse service APIs provide services to the nurse's mobile GUI. The users of nurse type access the healthcare database through this module.

8. Doctor Service API: The doctor service APIs provide services to the doctor's mobile GUI. The users of doctor type access the healthcare database through this module.

9. Patient service API: The patient service APIs provide services to the patient's mobile GUI. The users of patient type access the healthcare database through this module.

10. Pharmacist service API: The pharmacist services APIs provide services to the pharmacist's mobile GUI. The users of nurse type access the healthcare database through this module.

Depending on the role of a healthcare database user, there are six different kinds of user GUIs connected with the secure m-healthcare server through their respective service APIs. GUIs are as follows:

1. Patient's Mobile GUIs
2. Doctor's Mobile GUIs
3. Nurse's Mobile GUIs
4. Pharmacist's Mobile GUIs
5. Laboratory Technician's Mobile GUIs

6. Administrator's Windows Application GUIs

The details of these GUIs trees are described in the section 4.1 Services provided by the Application.

3.3 Message Flow

3.3.1 Message Flow for Authentication

1. User sends an authentication request with his/her e-mail address and password to HCSP-DB.
2. HCSP-DB forwards user information to the IDMS server for verification.
3. IDMS verifies it. If user information is invalid, IDMS informs HCSP-DB that the user is invalid.
4. User will get an error message from the HCSP-DB.
5. Otherwise, IDMS informs HCSP-DB that the user is valid.
6. HCSP-DB sends the response to the user that authentication is successful.
3.3.2 Messages to book an Appointment

1. Patient sends a request to HCSP-DB for appointment booking.
2. HCSD-DB sends a query password request to the patient. HCSP-DB verifies the password, because someone else way illegally books an appointment.
3. Patient sends password response to HCSP-DB.
4. HCSP-DB forwards patient password to the IDMS for verification.
5. IDMS verifies it. If patient password is invalid, IDMS informs HCSP-DB that the patient password is invalid.
6. Patient will get an error message from the HCSP-DB.

7. Otherwise, IDMS informs HCSP-DB that the user password is valid.

8. After that HCSP-DB verifies the time slot which is applied for booking by the patient. If the time slot is free, then HCSP-BD sends a positive response to the Patient. Otherwise, it sends a negative response.
3.3.3 Insert Prescription

1. Doctor sends a request to HCSP-DB to insert prescription.
2. HCSD-DB sends a query request for patient ID to the doctor. HCSP-DB verifies the patient ID, because the prescription will be inserted only for authentic patient.

3. Doctor sends a response with patient’s ID to HCSP-DB.
4. HCSP-DB forwards patient’s ID to the IDMS for verification.
5. IDMS verifies it. If patient ID is invalid, IDMS informs HCSP-DB that the patient ID is invalid.
6. Doctor will get an error message from the HCSP-DB.
7. Otherwise, IDMS informs HCSP-DB that patient ID is valid.

Figure 3.5 Message Flow to insert Prescription
8. Then HCSP-DB sends a positive response to the doctor and doctor can insert prescription for an authenticated patient.

3.4 Analysis of Security Features

3.4.1 m-healthcare Threats and Attacks

There are several threats and attacks involved with m-healthcare system, like electronic data transactions security, mobile user authentication, and the security and privacy of data stored in a mobile device [8].

Let us discuss a bit details about electronic data transactions security. Nowadays, almost every mobile device connects with the Internet through Wireless Access Point. It makes patient's data vulnerable to the attacker. The most possible risk can be man-in-middle, spoofing, sniffing, or session hijacking [7]. When a third person sits with a mobile device, connects to your wireless access point and listens to your network data and in the worst case captures your data, then modifies it and sends to the destination. If a patient data is modified before the diagnosis process, it will result in wrong diagnosis, which will lead to a wrong prescription that can be very harmful for the patient.

Authentication of the mobile user is very important while accessing sensitive patient data. Patient's private data must not be accessible to the third person other than the patient itself or the authorized physicians. After the authentication, the user will get access to the data depending on his/her access limit. It means that after the authentication the user will be authorized to access data. Also the security of the authentication data during transmission is vital. Because if the user information is viewed by third party, they may use it next time to access data [9].

In many cases sensitive patient data are downloaded to the mobile device and if the device is lost it may happens that the patient's data will be viewed by third person. The authentication process can secure the mobile data in some sense, but if we store the data in the mobile device as a plain text format, it can be retrieved by other applications or specialized tools that can read or modify the data. So, it is also very important to secure data stored in a mobile device [8].
3.4.2 Security Components

The key factors involved in the m-healthcare system, that is security and more precisely trust, is a greatly rated issue. Though the use of mobile phones in the area of healthcare domain is increasing everyday, but there are not so many secure m-healthcare applications that can be used. Patient healthcare data includes receptive data that is transferred over internet channel. Patient sensitive data need protection from security vulnerable by attackers.

Authentication

Authentication is the key issue for secure m-healthcare system. Many systems used password-based authentication, which is a very weak authentication process. A weak password can be retrieved by dictionary attack or brute-force attack. We used mutual authentication process in this system for strong authentication. It is a public key cryptography based authentication where mutual authentication offers public certificate of public CA. The mobile phones’ certificates are generated by the CA server. We used mutual authentication protocol FIPS 196 for the mobile client and healthcare service provider.

Confidentiality

In order to get access to the data, every user must go through the access control procedure which discloses data only to those users who have valid subscription. In this thesis, we used DES algorithm to encrypt users’ important data. We have also used a shared secret key to encrypt and decrypt data. Shared secret key is protected by using asymmetric key encryption. We used RSA’s public key to encrypt shared secret key. The healthcare service provider uses user’s public key (RSA’s public key) to encrypt shared secret key and transfers the encrypted shared secret key to the mobile client through an established secure channel. Only the particular user with the valid corresponding private key can decrypt shared secret key. In order to get access to the data, every user must go through the authentication and access control procedure, which discloses data only to those users who have valid subscription. So, a secured confidential communication is established between healthcare database server and healthcare client application. Therefore, important and sensitive medical data is protected from the attackers.
Integrity

Integrity of messages can be ensured by verifying the signature. We used here DSA cryptographic algorithm. In this algorithm message digest is used as digital signature of that message. So, message user and healthcare services provider are verified by digital signature, whether it has been changed or not. If the message is changed for any reason, then it will generate a different digital signature and the signature will fail to be verified.

Authorization

Authorization is a mechanism which allows a valid user access to the particular area of a system. It also determines their activities within the system. It is defined in a policy list. We have used role-based access control mechanism. Security policy server maintains role-based access control. When any user enters in healthcare application, then he / she has a specific role. This user role will be verified by security policy server and depending on the role, the user will get access to the respective area of the healthcare database server. If the user is not authorized to access an area depending on his/her role, then he/she will be denied from the access of that specific area. So, only authorized users can access the system.
Chapter 4: Operations/ Use of the System

In this chapter we describe different services provided by the m-healthcare application. We have also described different modules of this application in detail.

4.1 Services Provided by the Application

All users of the m-healthcare application need to be registered in the system. The registration process has two different steps. First the user needs to fill a paper-based form with his detail information and signature. An administrator should insert these data into the system. Then, at the second step of the registration, users should register themselves with the system using their mobile client.

Several services are supported by the healthcare process. These include:

- **Book a doctor** - Patient can check doctor’s schedule and book a doctor by using his/her mobile application. Patients choosing a specific doctor in his/her area and confirming an appointment with the doctor.

- **Book a nurse** - Patient can also book a nurse. He/she checks the nurse’s schedule and book a nurse by using his/her mobile application. Patients are choosing a specific nurse in his/her area and confirming an appointment with the nurse.

- **Book patient’s schedule** - Doctor can select a specific patient and create a new appointment with this patient.

- **Access health records** – Patient have the ability to access his/her medical records from this healthcare application. He/she can view his/her medical health information from the medical record unit. But, patient can’t create, change or modify it. Only doctor / nurse can create any comment in this section.

- **Check prescription** – Patient can also check his/ her prescription from his/her healthcare application. Patient can also book a time with a pharmacy to collect the medicine.
- **Check diagnosis results** – Patient can check his/her diagnosis result using mobile application. Lab-technician sends the diagnosis result to the hospital database and then it will be viewed by doctor and patient.

- **Sale medicine in pharmacy** – Pharmacist can select a patient with his/her personal Id number and see the specific patient’s prescription. Then pharmacist sells medicine to the specific patient by using the application.

- **Book a laboratory and its schedule** - Patient can use this system to book laboratory. Patient can select a laboratory in his area and choose a time which is available from the laboratory schedule.

- **Create diagnosis record by lab technician**: Doctor sends diagnosis prescription to laboratory. Then lab technician makes the test result from patient’s sample and sends it. After that, specific doctor and specific patient can view the result.

### 4.2 Modules in the Application

#### 4.2.1 Registration Window

After filling the detail information on the paper form, the user will register his/her unique password from their mobile device. The registration form on the mobile device consists of three fields: user personal number, user email address, and user password. Personal number and email address are already registered in the system by the system administrator. Only the password of a user is registered in this phase of the registration process. A user needs to use this form for only one time and that is when he/she starts using the m-healthcare application for the first time.
4.2.2 Login Window
The main login form of the m-healthcare application has fields to be filled: user email address, password and his/her user type. User will be authenticated by their email address and password. And depending on user type, he/she will be authorized to use the specific component of the system.

4.2.3 Patient's GUI Tree
After proper authentication and authorization, user gets access to the system depending on his/her user type. Users of patient type will get access to create, view and modify his/her appointment with the doctor, nurse and the diagnosis laboratory. Also he/she will be able to view his/her medical records registered by different healthcare service providers. For
example, he will be able to view his/her prescription registered by the doctor. The detail GUI tree for a user of patient type is given in Figure 4.3.

![Figure 4.3 Detail GUI Tree for a Patient](image)

### 4.2.4 Doctor's GUI Tree

After login to the system, a doctor will be able to check their appointments and also will be able to select a specific patient to check his medical data and register different kinds of medical data on the specific patient. For example, the doctor will be able to suggest medicine to the patient or suggest future diagnosis work for the patient. The doctor can also communicate with the patient using the same system. The detail GUI tree for a doctor is given in Figure 4.4.
4.2.5 Nurse's GUI Tree

A nurse and a doctor have quite similar type of initial screens as both of them have appointment and patient selection options. But, after selection of the patient, the nurse has a different screen than the doctor. Because the nurse and the doctor have different roles, then a doctor and all the users of our suggested application get access to the healthcare database depending on their specific role. The detail GUI tree for a nurse is given in figure 4.5.
4.2.6 Pharmacist's GUI Tree
Pharmacist will be able to select a patient using this mobile application and he/she will have access to the prescriptions assigned to the patient. Depending on the prescription, he/she will sell medicine to the patient. The GUI tree for a pharmacist is given below.
4.2.7 Laboratory Technician’s GUI Tree

The laboratory technicians will be able to check appointments registered in the system. He/she will also be able to select a specific patient by checking his investigations or to register new medical records on the diagnosis that he/she has performed. The detail GUI tree for a laboratory technician is given at the Figure 4.7.
Chapter 5: System Implementation and Demonstration

In this chapter first we describe different development environments that are used to implement the m-healthcare application. Then we have the screenshots of the mobile client application with proper description of them.

5.1: Development Environment

5.1.1 Eclipse SDK
Eclipse is a workspace where developers use multilanguage software in different developing environments. Mostly Java developers use it. Eclipse has extensible plug-in system for developing environment. We used Eclipse SDK (software development kit) with version 3.7.1. It is open source and free for download. Eclipse SDK is used by Java developers. It can be extended by installing plug-in for Eclipse platform.

5.1.2 Java Programming Language
Java is one of the mostly used popular programming language, as of 2012 [30]. It is a class-based, object oriented, platform independent programming language. It has lot of build-in security features. So developer gets some extra benefit by using Java from build-in support for multithreading to developing application. It is free to download software. Java is simple, easy to design, compile debug and also easy to write code [31]. This application is developed for Android platform. This application is written by Java programming language.

5.1.3 Android Mobile Operating System
In this thesis we will focus the development of secure m-healthcare application on Android Platform. Android is one of the most famous mobile phone OS that has come to the second position within the ten years of its invention. Android is an open source and free mobile platform. It has its own application security features. The Android applications are developed using APIs the same as Java which are developed by Google and Open Handset Alliance. Android developers don’t have any costly barrier for using this application. There are many Eclipse programs available in integrated development environment (IDE) for Android application developers. These applications are written in Java. The core libraries of Android applications include an e-mail client, SMS program, calendar, maps, browser, contacts, and
other features are provided most of the functionalities from the core libraries of Java programming language [21].

5.1.4 MySQL Database

MySQL is the most popular open source database which is scalable, reliable, high performance web base database. We can query specific information in a database and get return a record set data. We can easily connect MySQL database to several web programming languages, like PHP, ruby etc [32]. MySQL database is used as a database server in this thesis. All healthcare data (patients, doctors, nurses, lab technician, and pharmacists) is stored in this database server. We used different tables with different information and different type of insert queries in this thesis.

5.1.5 PHP

PHP is an open source script language and it is also free for download and use. It can provide security by encrypting data and provide advance features for developers. PHP is especially suitable for web development [33]. We use PHP as a middleware between MySQL database and mobile application (Android application).

5.1.6 JSON Format

JSON (JavaScript Object Notation) is a data interchange format. It provides human readable, simple support data which is completely language independent written over Java script [34]. In this thesis, JSON format is used to interchange data between web server (http) and mobile application (android application).

5.2 Relational Database Table

The system supports a hierarchical data structure in which all healthcare data and patient general health recodes are stored in a hospital central database. Figure 5.1 described the relation model of hospital central data base.

As their names indicate, the table called “hc_org_tbl” stores each organization using their zip code. Every user of this mobile application relates to hc_org_tbl by using their zip code. The tables called hc_staff_detail_info and patient_detail_info store each system user’s personal data with his/her unique system ID. Each organization staff information is stored in the org_staff_detail’s core data (hc_staff_id, hc_staff_type, personal_id, hc_staff_name, email, zipcode etc), encrypted password and salt. The same as the patient record stored in patient_detail_info core data (patient_id, Patient_ name, email, zipcode etc). Every patient
has his/her unique health record, which is stored in database server as patient_hc_data. This patient_hc_data is linked with the patient table by patient unique Id. Patient also relates with appointment_tbl by their unique id. Every medication has its barcode number, which is related as its system ID.

![Relational Database of the System](image)

**Figure 5.1 Relational Database of the System**

### 5.3 Screenshots of the Admin Form for User Registration

Administration of the hospital uses this form to register a user of m-healthcare application. The form is shown in the Figure 5.2. Admin fills the form from user’s given information. The registration form has two sections ‘User Data’ and ‘User Address’. User Id is automatically generated. User password will not be generated from here.
5.4 Screenshots of User Login and Registration Screen
On the mobile device the first screen is the login screen showed in Figure 5.3.
Users input their registered email address, password and select the user type from the dropdown box to register to the m-healthcare system. If a user uses the application for the first time and he or she doesn’t have a registered password, then he/she should choose the link ‘I don’t have account. Register Me!’ for the registration on the login screen. On the login screen the drop down box shows the screen showed in Figure 5.3, where the users choose their user type from the list of user types. If the users try to login with the correct email address and password, but with a wrong user type, he/she will not get access to the system.

### 5.4.1 Password Registration Screen

After clicking ‘I don’t have account. Register Me!’ at the login screen the user will be redirected to the registration screen where the user will provide his/her personal number, registered email address and a password to register his/her password with the system. Before registering the password on the mobile device, every user needs to be registered with the system through an administrative registration by a physical meeting with the administrator. The user provides his/her personal number, personal email address and other personal details to the administrator. The administrators don’t enter password for any user. The user password is registered by the screen showed in Figure 5.5.

![Figure 5.5 Password Registration Screen](image)

### 5.5 Patient Panel

In this section we have provided the screenshots for the patient’s application panel.

#### 5.5.1 Patient Login and Home Screen

Figure 5.6 shows the patient login where a patient has entered her full email address, password and chooses the user type ‘Patient’. When she touches the login button, he/she gets
access to his/her home screen, which is shown in Figure 5.7. The patient has two options at the home screen: Appointments and Personal Medical Records.

5.5.2 Patient Appointment Options
After selecting the appointment option at the home screen, patients are redirected to the ‘Appointment’ screen (shown in Figure 5.8) where the patient has three options: ‘Create Appointments’, ‘Show Appointments’ and Cancel Appointments’. Figure 5.9 shows Create Appointments option for a patient, where a patient can select ‘Book a Doctor’, ‘Book a Nurse’ or ‘Book a Time for Diagnosis’ option.
5.5.2.1 Create Appointments Detail

Figure 5.10 shows ‘Book a Doctor’ screen. Patient can choose a doctor at the medical center where he/she is registered. In the same screen the patient selects a date for the appointment and selects a time slot from the list of free slots on that specific date. Figure 5.11 shows the appointment booking options with a nurse, where the patient can do the same type of operation as with the doctor booking screen.

Figures 5.12 and 5.13 show laboratory booking options. When a patient selects ‘Book a Laboratory’ on the create appointment screen, he/she is redirected to the Laboratory Area screen (Figure 5.12) to select the area where he/she is interested to book a laboratory for diagnosis. After selecting the laboratory area, the patient is redirected to the ‘Book a Laboratory’ screen (Figure 5.13), where the patient selects the Lab Technicians, Date of Appointment and the Time Slot for the appointment.
5.5.2.2 Show Appointments Detail
In the Figure 5.14 ‘Appointments’, patient can see on his appointments with doctor, nurse or laboratory. For getting the detail information, patient needs to select specific data or items from the table. Then ‘Appointment Detail’ (Figure 5.15) will be opened and patient can see his / her appointment details as Figure 5.15.

![Figure 5.14 Appointment List Sorted by Date](image1)

![Figure 5.15 Single Appointment detail](image2)

5.5.2.2 Cancel Appointments Detail
Patient can cancel the appointment from this application. First patient needs to select Cancel Appointment, then patient has to select the specific date from ‘Appointments’ (Figure 5.16)

![Figure 5.16 Appointments List](image3)

![Figure 5.17 Appointment Detail for Cancelation](image4)

table, which one he /she wants to cancel. After selecting, it shows the detail information about the appointment, as the Figure 5.17. Patient can check the detail appointment information
before canceling. If patient selects Cancel Appointment, then the appointment will be deleted from the appointments table.

5.5.3.4 Patients Personal Records
From the ‘Personal Medical Records’ (Figure 5.18), patient is able to see his / her prescriptions, doctor comments and diagnosis result. If patient wants to see the detail information of this, then he/ she can select the specific field.

![Figure 5.18 Personal Medical Records](image)
![Figure 5.19 Lists of Prescriptions Sorted by Date](image)

If patient selects ‘View Prescription’, then it shows all of the prescriptions which were created by doctors, like Figure 5.19. When patient selects any of the date from the prescriptions then patient can see the detail information as Figure 5.20.

![Figure 5.20 Single Prescription Detail](image)
![Figure 5.21 View Doctor’s Comment Detail](image)

Patient can also see the detail information of doctor’s comments and patient diagnosis result.
5.6 Doctor Panel
We implemented doctor panel where doctor can perform different kinds of activity. We are describing all of these activities here.

5.6.1 Doctor’s Home Screen
In ‘Doctor Screen’ (Figure 5.22), doctor can check appointments and select patients. Doctor can check all of patient appointments from the field ‘Check Appointments’. When doctor wants to act upon a particular patient, then doctor needs to select the field ‘Select Patient’.

![Figure 5.22 Doctor's Home Screen](image)

5.6.2 Doctor's Appointment Options
Doctor is able to check all appointments and also check specific appointment from doctor’s appointment screen. In the field “Check All Appointments” doctor can see all of all of the patients’ appointment time with the doctor.

![Figure 5.23 Doctor’s Appointment Options](image)
5.6.3 Check Specific Appointment

After selecting ‘Check Specific Appointment’, it views the ‘Search Patient’ screen, as Figure 5.24. Here doctor has to write the personal number of particular patient. Then doctor can see the detail particular patient’s appointment information.

Figure 5.24 Search Specific Patient

Figure 5.25 Specific Patient’s Details

5.6.4 Doctor's Activities for a Specific Patient

After selecting ‘Select Patient’, doctor needs to write ten digits personal number of particular patient and sees the particular patient operations screen, shown in Figure 5.26. Here doctor can do different kinds of activities with the selected patient. Doctor can create prescription of medicine and prescription of diagnosis, write patient’s medical information, book a time for new appointment, show patient medical history, and also send a SMS and e-mail, if he /she wish.

Figure 5.26 Doctors Activities for a Specific Patient
5.6.4.1 Prescription Options
After selecting Medication, doctor have ‘Patient’s Prescription’ (Figure 5.27) screen where doctor can create prescription as Figure 5.28 and show prescription of the selected patient.

5.6.4.2 Create Comments for a Specific Patient:
In the Figure 5.29, doctor writes comments about medical information of the select patient.
5.7 Nurse Panel

In the nurse panel, nurse can perform similar activities like doctor. But nurse has some limitations, such as nurse can’t create prescription, send SMS and e-mail for any patient. But, nurse can create comments about patient health information. We will not describe detail nurse panel, all other screen/activities are the same as for doctor.

5.8 Lab Technician Panel

In lab technician panel, we have Check Appointment and Select Patient fields. Lab technician can check all of the appointments times which are booked by the patients by using mobile application. Lab Technician can also select a patient by patient’s ten digits personal number. Then, lab technician inserts the results of patient’s tested sample and create a report of diagnosis.
At the pharmacy or medical store the pharmacist will use his/her registered email address and password and will also select user type pharmacist from the drop down box. After login the pharmacist will see the pharmacy screen (Figure 5.32).
Chapter 6: Conclusions and Future Work

6.1 Conclusions
An m-healthcare application has a set of services. Users of smart mobile devices can use those services by installing the application on their devices. Few years ago m-healthcare didn’t exist and the people need to go physically to medical service center for getting each service and physician also provided paper base service. After introducing m-healthcare application, it makes people life easier and comfortable. Patient can retrieve his/her medical information at anytime and anywhere by using his/her mobile phone. The mobile healthcare communication between patient and healthcare professionals will increase efficiency and reliability significantly.

6.2 Future work
As we have described, we have implemented an integrated m-healthcare application which is capable to register different kinds of information to the healthcare database server. Our research has opened many new fields of future work. For example, the same mobile application that we have implemented can be enhanced with remote patient monitoring capabilities for the elderly or disabled people. In that case the wireless sensor devices should be used to collect patient data. Then the collected data can be transferred to the patient’s mobile phone. After that, mobile phone can transfer data to the healthcare database server. Also a new research can be done with respect to privacy issues of m-healthcare application’s users.
References


[30] Java (programming language),
\[http://en.wikipedia.org/wiki/Java_%28programming_language%29\]

[31] What is the use of Java, \[http://www.roseindia.net/java/use-java/uses-of-java.shtml\]


[34] Introducing JSON, \[http://json.org/\]
