A PROPOSED of SECURE MOTHER HEALTH CARD APPLICATION

Mayassa Fuad Abdulrazzaq¹, Dr. Shaimaa Hamed Shaker²

¹Dept. of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq
²Computer Engineering, University of Technology, Iraq
¹mayassa_f@yahoo.com; ²sh_n_s2004@yahoo.com

Abstract - Increasingly health care expenditure has led to an increase in calls for ways to reduce the cost of healthcare, secure and quick way to improve health service. Based on relevance of the best electronic record technology is the smart card technology. Therefore, this work is devoted for smart card technology and applications as a design and implementation for Mother Health Card Application (MHCA).

This work suggests a secure software based on authentication by using RSA 512 and RSA 1612 algorithms, integrity that used hash function SHA-1, passwords algorithm, and key generator function. Using the MHCA as card identification is to access control of mother's card. The work implements use of Java language with MySQL for database. This card provides many advantages like efficiency, time-saving, and effort-saving.

Keywords- mother health care, smart card, information system, secure access, authentication.

I. INTRODUCTION

A smart card is a plastic card that contains a microprocessor, memory and an interface to the outside world. The chip holds the data with appropriate security. This data is associated with the information or the value or may be both and is processed and stored within the cards’ chip, or the memory or the microprocessor. A microprocessor chip can offer complicated data security approaches such as adding, deleting or processing in its memory [1].

© 2015, IJCSMC All Rights Reserved
The business model is changed and smart card entered new fields providing new functionalities, especially at the end user terminal. In the medical sector, there are many countries that exploit the huge and vast applications of the smart card to improve the health care service [2].

The system of smart card in health sector will save money and time because all tests, results, and prescriptions would be placed in a file folder and medical staffs would not need to redo work already performed by an employee. So will get on a medical system to be utility, enormous adoption is required. On the other hand, the privacy of the data stored on the medical cars is protected by law.

The purpose of this paper mainly is to ensure secure access to the data for the patients and patients’ privacy. The mean of security here is: authentication, role based access, passwords to secure storage and some audit activity. The access to data is done by health role, physical security and the medical staff’s relationship to a patient. The framework for the hospital or health centers supports the authentication devices like biometric devices, cards (swipe and proximity). Within the framework combination engine manages and organizes message transfer between hospital application, databases and external system.

The aim of this paper is to design and implement a develop mother health card application to ensure secure access to the mother's health information through the Identify smart card applications based on healthcare information system.

The applications of mother health card system is a potential opportunity to increase efficiency and delivery of better healthcare service, faster and secure access to accurate health data, reduce fraud, streamline administration, improve communication between healthcare providers and patients, and enhance treatment quality and safety [3].

II. RELATED WORK

The smart cards in health care enable professionals in the hospital or health center to share information easily. This card contains two type of health card: patient card and professional card. The patient card contains patient ID and card access PIN, photo, prescription information, very important and necessary data (drugs, blood type, vaccination, and surgical operations with their dates, hospital name and summary information), identification (patient name, birth date, address, mobile telephone number), and insurance information. Therefore, the card becomes a patient’s medical history.

1- Peter PHAROWI and Bernd BLOBEL in [4] presented the advantages and drawbacks of health information systems and their awareness issues. The author reached that a good-balanced combination of cards and networks is the best way to face the challenges of health care and welfare requirements.

2- KARL JÄHN, ANJA GÄRTIG-DAUGS in [5] In Germany, these data of patients can publically accessed through integral system if that is not considered a breach for privacy of the end users.

3- H. Liyanage1, S. de Lusignan1in [6] The advancement led to generating a data in the last two years that exceed the entire data that has been generated in entire history of digital age. So big data as a term
that we use today is not correct to say as in future as the technology advancement can turns the big to a small or even very small.

4- L. Toubiana1, M. in [7] shows the aim of health information systems is to contribute to the high quality of care and the efficiency of care management, for physicians, patients, and medical research. With the growing deployment of health information technology (HIT), the question of effectiveness is still topical.

III. The Proposed Application of Mother Health Card

The architectural designs for hardware, software, actors, and database are presented. MHCA helps for the pregnancy mother by save the time and money, easy and quick pathway for diagnosis, easy to connect between the mother and the health provider, mother information and baby birth certificate are securely and privately data based and quickly retrieved at any time.

A. Design of Mother Health Card Application (MHCA)

A Mother Health Card Application is provided to the mother to present health care provider at each visit for an insured mother health service. The main steps of the design of mother health card application (MHCA) are as follows:

1- Analyzing and collecting the user requirement

2- Detecting all the program for Mother Health Card Application

3- Specifying the flowcharts for Mother Health Card program and terminal programs

4-Writing the program codes

The proposal is to classify the procedure into:

• Information is written by Admin (Information Technology professional) in the ministry of health; this Admin will setup the program in the health center and the hospital and create users and create ID for them. The Admin will create password for human resource, key management using (RSA) and database management.

• Information is written by Human Resource (HR) which contains the primary information for the mother. This information will not change and always do not need to be updated. So this person will create the password to the actors. Only the HR can access to this information.

• Information is written by the doctors who have the diagnosis for the diseases, give injections to the mother, and follow up mother health periodically. All this information is updated by the doctor and only the doctor can update or change this information.

This information which is stored in the MHCA’s database will be shown through admin to be used by staff. The staff will be logged in the system through password and user name. Admin who is IT
professional has the table below which is called Centers. This table contains the center name, ID, office name, and section… As shown in the fig 1.

So the IT professional in the Ministry of Health will setup the program in the health center and the hospital so create two key (public and private) to the center and the hospital. This information is stored in table called (r-report), as illustrated in fig.2.

Also, some information called (patient card) is stored in table; this is contained on ID and card serial number of the MHCA. As illustrated in the fig.3.

Then, the admin will give the password to the Human Resource (HR) to use the program and give him the tasks that he/she responsible about them such as register the staff. So if there is any problem in the program or in the card (such as format, reformat, harm, and loss card) the HR must return to the IT professional because only both of them have direct access to the system.

The HR manages MHCA by writing doctor’s information in the table called (personal_information); this table contains ID for the doctors, doctors’ information, and active (which show him the status if he/she is active or not active). As illustrated in the fig.4.
Fig. 4 Personal_information Table

B. Diagram Models of the MHCA Programs

Mother Health Card Application System (MHCA) illustrated in fig. 5

Fig. 5 Model Diagram of Mother Health Card Application MHCA’ program

C. Programs and terminal programs for the Mother Health Card Application

This application contains three programs; the first is for mother health card that installs first data on the mother, the second program is for reading information and editing of this information by actors in the health center, and the third program is for securing information and making sure authentication and confidentiality by using RSA, Hash function SHA-1, which depends on PIN for mother health card that depends on authorized access.

Program no. 1: This program is built in the Ministry of Health by the IT professional (Admin); the Admin setup the system in the health center and hospital, key generation, database management, and any update or any problem he is to solve. as illustrated in flowchart in fig. 6.
Program no.2: This program used only by health center staff (such as officer, doctor, dentist, lab technician...). It’s the program that responsible on specifying the card of the mother and key in the required data on this card. Then the doctors will receive their tasks.

All the staff in the health center do login to use the system by enter the username and password, the program will check if this username and password available in the staff table. As illustrated in fig.7.

First visit for the mother when pregnant, she will get on the MHCA by giving the basic information to the officer, who keys in her information after login. The officer can use the new card only once, at the first visit of the mother. Then, when the card is not used, the officer will enter the basic information to tag and determine hash for the information that writes on the tag. After determine hash will save the hash in database and card. As illustrated in fig.8.
After getting the mother on the MHCA, she can visit the doctors in the health center. At first, she visits the Doctor. After the doctor and medical staff like dentist, lab technician, and others can login the program by checks if ID of this card available in the table or not. In case this ID is not available the table, will display message showing this card is not in the database. While if ID is available in the database and table then the doctor will read the data from the tag. Then he determines hash for the information by use SHA-1 and compares hashed information in tag with hashed information in database. If equal, the doctor will write the report for mother’s diagnosis and save this report in the tag and database. As illustrated in fig.9.

All the staff write on the tag there is procedure for this writing. When the staff put the MHCA on the reader, the reader will check the ID for this card to sure this card issued from this health center by check if the ID card available in the database. The if not available cannot accept it. If yes this card issued from this center will be encapsulation for data by set the data in card and transfer the data to
byte array (all this details will explain in chapter four). After the encapsulation will save the data in the card. As illustrated in fig.10.

Program no.3: This program used in the hospital, when the mother has birth will visit the hospital. There is just the doctor can access and use the program, the hospital don’t have any database only files.

File contain on ID center, center name, and sector name for all centers in the Baghdad. the other file contain on public and private key of the hospital and public key of the health center, these keys used in the encryption the information on the tag. In the start the program will read the information from MHCA to know all the health information about the mother, such as blood type, blood pressure, blood sugar, and some important tests, to help the mother in the birth and save time.

After birth the Doctor will check out the baby and enters all the result of check out in the card. After this he will add digital signature which contains center ID, serial number of the card, and sequence number of the pregnant woman, for the data by using RSA with hash algorithm type SHA-1, a digital signature will be obtained with privet key for the hospital. After this, it will encrypt the information by using public key for the health center and save the information that contain on the birth certificate for the new baby in the card. As illustrated in fig.11.
D. System Architecture of (MHCA) in the Health Center

This is at the health center where the employee or human resources, officer and doctors as well as a card reader and mother cards exist in the health center data that contains all information related to mother base and Career Level System. As illustrated in the fig 12.

![Fig.12 System Architecture of Mother Health Card Application in the Health Center](image)

E. System Architecture of (MHCA) in the Hospital

The system varies in the hospital for the health center and to the lack of access to the system by the employees except of the doctor who supervise birth. Also there is a file (because the hospital does not have a database) contains a public key and private key for the hospital and public key for the Health Center for using in the process of data encryption (birth issued by the hospital) statement, using the RSA and hash contains the serial number of the card in order to have digital signature by a doctor. After the birth, the mother should go to the health center with her card to update her status information. The information of her new baby will automatically transfer to the database, and to be added as newborn to the history of past pregnancy. As illustrated in fig 13.

![Fig.13 System Architecture of Mother Health Card Application in the Hospital](image)

IV. Implementation of Mother Health Card Application

The MHCA implementation is present in this section. Using java implementation for MHCA support the cross platform functionality of the system.

A. Simulation of the MHCA with security

This section includes all the steps required to simulate the MHCA. The admin add the name of hospital or/and health center to the main table which shows all health institutes in Iraq. Selectively admin will add according to presence of the MHCA system. Each hospital/health center will carry an ID number which will be in use for any future application. as illustrated in fig 14.
So if there is any problem (as losing or damaging the card) or need to format the MHCA only the admin can solve this problem by the interface that special for it, as illustrated in fig 15.

![Fig.14 Interface for MHCA system that Relevant to Admin](image)

**Health Center**

Human Resources manager in the health center has many jobs related to the staff and the mother (the pregnant woman). First the HR manager (mayaasa) and all the staff can login by enter username and password then click on (دخول). As illustrated in the fig16.

![Fig.16 login of the Human Resources Manager](image)

When HR manager will access the system (login), an interface will appear, this interface shows some important information related to the staff, such as their ID’s, names, passwords, and activity status. The latter means that the staff is available to use the system or not; i.e. when the staff is available, then “active” box will be ‘marked’. The HR gives the staff their passwords and has the ability to delete some staff or adding new one using the icons at the bottom of the interface. As illustrated in the fig 17.
1. The Officer

The officers’ task is registering the new card to the mother and key in the mothers’ information in her card by asking the mother about basic information. The officer after finishing registration, he/she cannot read any information from the card; this provides privacy for the mother and ensures access control to the MHCA even from the staff. First officer must login by entering username and password then click on (دخول). As illustrated in the fig16. Here officer name is (نهى).

Then the officer uses the interface of the basic information for the mother. Now the officer can input the mothers’ information, as illustrated in fig 18. So the officer cannot access to the card again after finishing the register for the mother card cannot access to the card again. If he/she try to enter, alarming massage is shown.

2. The Doctor

The mother after reserving her card will go to the Doctor (امنه). The doctor can enter the system by login username and password then click on (دخول). After ‘login’ of the doctor, he/she will ask the mother for some medical information about her health or diseases, and he/she will enter this information to the system, as illustrated in fig 19.
Finally doctor will have interface called (Reserve certificate of new baby) (استلام بيان ولادة)، as illustrated in fig.20. Because of the mother in this case is once pregnant, so the interface is empty from any data. After the birth the health center will reserve certificate of baby birth as explain in fig.22.

3. The dentist

The mothers’ teeth are very important especially during her pregnancy, so she must take care by periodically visiting the dentist during pregnancy and after giving birth to the baby.

4. The Lab Technician

During pregnancy the mother needs to do some tests that are important for her health. The doctor decides which test must be done. In this case the mother goes to the lab technician to do the tests. The lab technician (زينب) enters to the system by login her user name and password. Now will show the interface that contain on test type that need to do the mother.

   The hospital

When the mother gives birth she will go to the hospital with her card. This process is very necessary for the mother and her baby because of the many benefits obtained from the card application such as save time, rescuing mother life if she has any problem because all the tests and medical information are available in the card. When the doctor who supervised the birth process accesses the system, then only the important information of the mother will appear, i.e. not all the information. The card in the hospital appears as four sections which contain the medical and family historic, estimation,
tablets, and vaccine. So we will see the all information will be not active that mean the doctor cannot write on or change any things just she/he can read the information of the mother. Now the mother gives birth, and only this section (تقرير المستشفى) can the gynecologist who writes on the card. The gynecologist key in all the information related to baby.

At this stage, the mother can leave the hospital and go back to the health center where the doctor registers the new baby’s information and store the baby certificate in the database, as illustrated in fig.21. After the doctor login he/she will see the whole information of the new baby being transferred automatically.

![Fig.21 Update the information to the new baby](image1)

The health center receives birth certificate from hospital and stores it in the database, not all this information is accessible (appears as not active), as illustrated in fig.22.

![Fig.22 Receive the Birth Certificate in the Health Center](image2)

V. Discussion

Each of the hospital and health center has two keys (public & private) generated by admin. These keys are used in digital signature, hash function, and encryption/decryption by using RSA algorithm. Privacy for the data that stored in the card by using access control on it, as each actor can access just for her application. Even the doctor, who should know all medical information of the mother, can only read the medical information but cannot write or update any data. Even the officer after finishing from issuing the card cannot enter to the application and read mothers’ information because he/she had already finished her/his task and no need to read the data. Without the MHCA no access to the application can be made. This gives authentication to mothers’ information and important for the card. MHCA saves for time, money, effort, and life especially that the pregnant women during pregnancy need to rest. The admin in the Ministry of Health, he/she responsible about the application as he/she can solve any problem in the card or in the system, key generation for hospital and health center, and setup the program (setup the application just for 30 minutes).
IV. Conclusion

MHCA consists of all basic and medical information for the mother, in the health center issue new card through three minutes by the officer (according to speed of officer in key in), checking the mother by the medical staff and making all tests and checking of mother through few minutes (according to mothers’ case), and finally issues baby certificate in the hospital only take few minutes with transfer of the new baby information to the tag without entering it by anyone. All this procedure with high security is made by using hash algorithm, RSA algorithm, and digital signature. MHCA saves for time, money, effort, and life especially that the pregnant women during pregnancy need to rest.

ACKNOWLEDGEMENT

I would like to express the deepest appreciation to my supervisor, Assistant Professor Dr. Shaimaa Hamed Shaker, she continually and convincingly conveyed a spirit of adventure in regard to research . And an excitement in regard to learning quality of Assistant Professor Dr. Loay E. George, who guide, support and continuously coach me to last moment of this thesis.

Special thanks for Dr. Himmed and Dr. Mohammad Younis , computer engineering, Baghdad University for their cooperation and support to maturate ideas of this to end.

References


