CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The chosen methodology for the system development is System Development Life Cycle (SDLC) Model that is also known as Classic Life Cycle Model (or) Linear Sequential Model (or) Waterfall Method. Visual web developer 2010 (which includes a local web server) and Visual Basic.Net scripting language which is based Active Server Pages (ASP.NET) technology will be used as tools of development. The backend database will be implemented using Microsoft SQL server data management system, which is the best choice for distributed data Applications.

3.2 METHODOLOGY

There are mainly five steps involved in the methodology of the research. First, the research started with collection of principle data that have been used in the research from previous studies such as books and electronic books, related literature, relevant journals, magazines, electronic publications, and quantitative information to support this research study. Second, two types of questionnaires were developed for analysis requirements and system evaluation. Analysis requirements questionnaire was distributed to respondents in order to determine system requirements. Third, researcher develop the system using a Visual Web Developer 2010 (which includes a local web server) and Visual Basic.Net scripting language based on Active Server Pages (ASP.NET) technology for the purpose of a prototype development. The back-end database was implemented using Microsoft SQL server data management system, which is one of the best choices for distributed data Applications. 3DES algorithm was

embedded in the system for encryption of patient record to increase security and privacy of the HMS. Fourth, the system was tested at a hospital in Benghazi, Libya. Fifth, system evaluation questionnaire was distributed to collect data on effectiveness of the system. A descriptive data analysis was conducted on data collected.

3.3 SYSTEM ENGINEERING AND MODELING

As software is always of a large system (or business), work begins by establishing the requirements for all system elements and then allocating some subsets of these requirements to software. This system view is essential when the software interface with other elements such as hardware, people and other resources. System is the basic and very critical requirement for the existence of software in any entity. So, if the system is not in place, a system should be engineered and put in place. In some cases, to extract the maximum output, the system should be re-engineered and spruced up. Once the ideal system is engineered or tuned, the development team studies the software requirement for the system. The process as shown in Figure 3.1 will go through the following steps:

- Requirements analysis,
- Prototyping,
- Implementation and documenting,
- Testing,
- Maintenance.

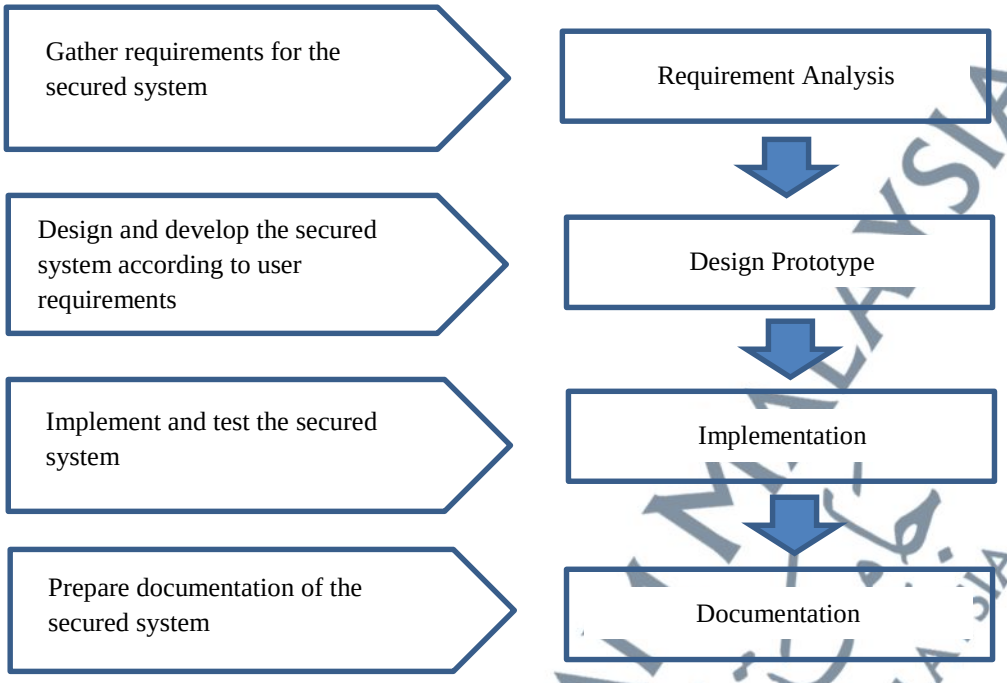

Figure 3.1: Model for the HMS Secured SDLC Methodology (Source: Adapted from Nalkar, 2013)

3.3.1 Requirements Analysis

Data for requirement analysis was gathered through questionnaire to 138 respondents in Benghazi Hospital, Libya.

3.3.1.1 Functional requirements

From the analysis of the survey, the main features to implement within the Hospital Management System (HMS) are:

- Register new patients and maintain medical record.
- The administrator can create new staff and edit the staff list.
- Book appointments for visit the doctors.
- Use medical record to follow-up of each patient by the doctors.
- Allow the doctor to prescribe medicines

- Show the medical acts of the patient.
- The login process can identify each user and administrator and grant them privileges.

3.3.1.2 Non-functional requirements

Usability: The system must be easy to deal with.

Understandability: The system should be easy to understand.

Reliability: The system should preserve the integrity of the data and the logic of the application.

Performance: The system must have a reasonable speed where many employees have to use the system at the same time.

Availability: The system should be available to all kind of users.

3.3.1.3 Users requirements

Administrator: Which will access the web application with a privilege that allows him to do tasks such: register a new patient, update medical record, invoices management and edit staff list.

Patient: The patient will be able to view, cancel and make a new appointment, as well as view his/ her medical record.

Doctor: The doctor will be able just to view his/her appointments and prescribe medicine for his/her patient.

3.3.2 Prototyping

The design must be translated into a machine-readable form. The code generation step performs this task. If the design is performed in a detailed manner, code generation can be accomplished without much complication. Programming tools like compilers, interpreters, debuggers and others are used to generate the code. Different high level programming languages like ASP.net, Java are used for coding. With respect to the type of application, the right programming language is chosen.

3.3.3 Implementation and documenting

Implementation is the part of the process where researcher programs the code for the project. Documenting the internal design of software for the purpose of future maintenance and enhancement is done throughout development. This may also include the authoring of an API, be it external or internal.

3.3.4 Testing

Software testing is an integral and important part of the software development process. This part of the process ensures that defects are recognized as early as possible.

3.3.5 Maintenance

The software definitely undergo maintenance. There can be many reasons for this maintenance to occur. Maintenance could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that could happen during.

3.3.6 Hospital Management System (HMS) Prototype

The Hospital Management System (HMS) homepage prototype is shown in Figure 3.2 below. Among the application of the system is that it will grant special privileges for the Admin user, therefore the Admin will access the web application with a privilege that allows him or her to do task with high privilege such as: register patient, update medical record, appointment management and create or edit staff list.

3.4 HOSPITAL MANAGEMENT SYSTEM FUNCTIONAL FRAMEWORK

Applying the security based framework to researcher system will definitely improve overall security of the HMS to maintain confidentiality, integrity and availability.

Certain controls were built into the system to harden the system and keep patient data safe. Researcher used best industry practices such as authentication, encryption, access control privilege, logging and encryption as shown in Figure 3.2.

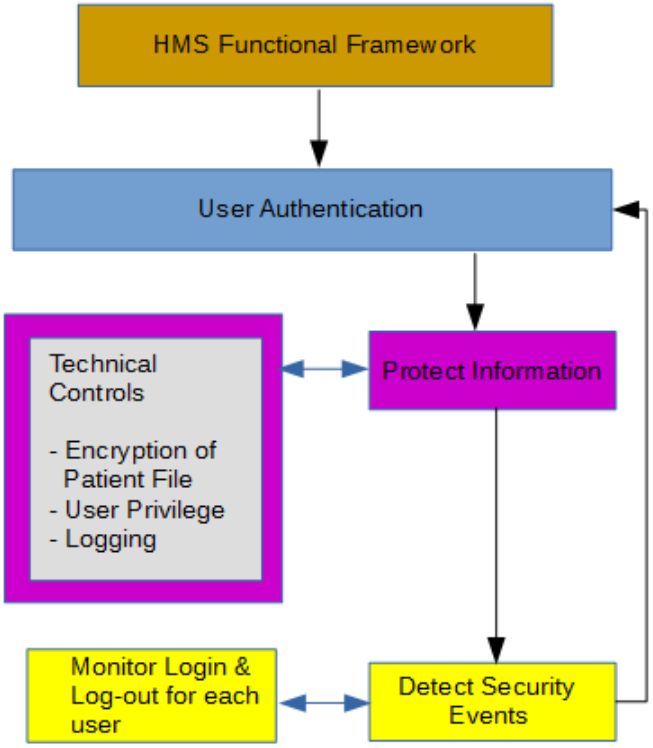

Figure 3.2: Functional System Framework

3.5 MEDICAL RECORD ENCRYPTION USING TRIPLE DES ALGORITHM

In order to secure the medical record within the hospital management system, an encryption method based on triple DES algorithm is proposed to settle the security issues of the data. Therefore the triple DES algorithm will be applied before to save the medical record and then when reading the data a decryption operation will be applied using triple DES algorithm.

3.5.1 Cryptography

Cryptography is a method of storing and transmitting data in an encrypted form so that only those for whom it is intended can read and process. It is a science of protecting information by encoding it into an unreadable format (refer Figure 3.3).

In order to secure the medical record within the hospital management system, an encryption method based on triple DES algorithm is proposed to settle the security issues of the data. Therefore the triple DES algorithm will be applied before to save the medical record and then when reading the data a decryption operation will be applied using triple DES algorithm in the HMS.

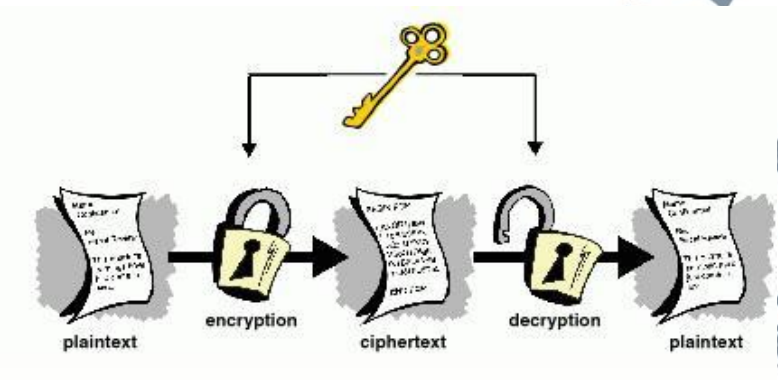

Figure 3.3: Basics of Cryptography (Source: Stallings, 2011)

3.5.1.1 Triple DES

Triple DES (3DES also called) is a symmetric cipher block chaining three successive applications of the DES algorithm on the same 64-bit data block, with 2 or 3 different DES keys as shown in Figure 3.4. Triple DES is EDE (encrypt, decrypt, encrypt). The way that it works is that take three 56-bit keys, and encrypt with K1, decrypt with K2 and encrypt with K3. There are two-key and three-key versions. Think of the two-key version as merely one where K1=K3. Note that if K1=K2=K3, then Triple DES is really Single DES.

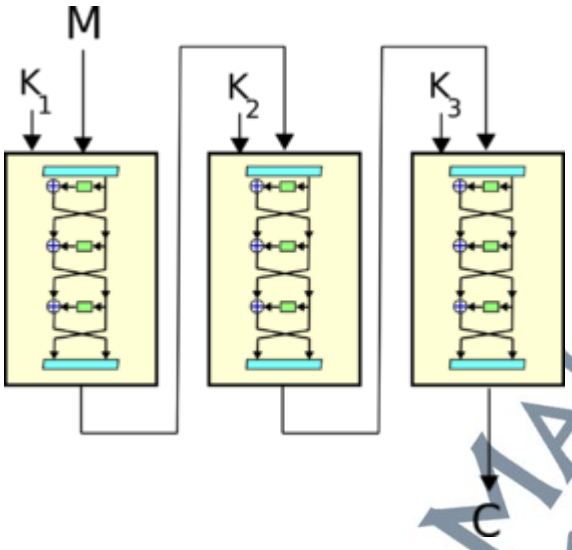

Figure 3.4: DES with three operations DES (Source: Stallings, 2011)

This use of three ciphers DES was developed by Walter Tuchman (head of project at IBM DES), there are indeed other ways of using DES three times, but they are not necessarily safe. Version Tuchman uses an encryption followed by a decryption to enter again by encryption.

Triple DES is generally used with only two different keys. The standard usage mode is to use fashion in EDE (Encryption, Decryption, Encryption, that is to say, Encryption, Decryption, Encryption), which makes it compatible with DES when using three times the same key. In the case of a hardware implementation that allows use of the same component to meet the standard DES and Triple DES standard. In the form proposed by Tuchman, 3DES is more formally written this way:

$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

Another variant is the Triple DES Carl Ellison, but it is not part of the standard set to 3DES:

$$C = E_{DES}^{k3}\left(T\left(E_{DES}^{k2}\left(T\left(E_{DES}^{k1}(M)\right)\right)\right)\right)$$

Where T ~ is a transposition function to increase the spread. This function takes as input a 8192-byte block, fills the seed of a pseudo-random number generator with the histogram of bytes and bytes mixture of the block through the generator output. The histogram is not changed by the permutations and therefore the reverse is possible. David Wagner has proposed an attack on the diagram of Ellison.

TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt-Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3. Sometimes this referred to as des-ede mode. A TDEA key thus consists of three keys (K1, K2, K3). The three keys are also referred to as a key bundle. The key bundle is 3 x 64 = 192 bits long.

ANSI X9.52 describes three options for the selection of keys in a bundle. Option 1, the preferred option, employs three mutually independent keys (K1 ne K2 ne K3 ne K1). Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ne K2 and K3 = K1). Option 3 is a key bundle of three identical keys (K1 = K2 = K3). Option 1 gives a keyspace of 3 x 56 = 168 bits.

Just split the 192-bit triple DES key into 3 separate 64-bit keys, working from left to right. For example, if triple-DES key is the 192-bit value (in hex format):

0123456789ABCDEFFEDCBA987654321089ABCDEF01234567

then split it into the three sub-keys, K1, K2 and K3, each of 64 bits:

0123456789ABCDEF FEDCBA9876543210 89ABCDEF01234567

|<------K1------>|<------K2------>|<------K3------>|

So the sub-keys are K1=0x0123456789ABCDEF, K2=0xFEDCBA9876543210 and K3=0x89ABCDEF01234567.

If someone encrypt something, then decrypt it and encrypt it again with the same key, that person just done the same as encrypting it once. Thus option 3 with three identical keys is simply the original 64-bit DEA algorithm with a keyspace of 56 bits, albeit done with three times as much effort. So, to carry out "single" DES using a Triple DES function, just set all three DEA keys to be the same. Note that this option is no longer permitted under NIST SP 800-67.

For example, if a single-DES key is 0x89ABCDEF01234567 then set the Triple-DES key to be

89ABCDEF01234567 89ABCDEF0123456789ABCDEF01234567

|<------K1------>|<------K2------>|<------K3------>|

Two-key triple DES is option 2 where someone encrypt with K1, then decrypt with K2 and finally encrypt again with K1. The keyspace is thus 2 x 56 = 112 bits.

For example, with K1=0x0123456789ABCDEF and K2=0xFEDCBA9876543210 someone would set the triple DES key to

be0x0123456789ABCDEFFEDCBA98765432100123456789ABCDEF.

0123456789ABCDEF FEDCBA9876543210 0123456789ABCDEF

|<------K1------>|<------K2------>|<------K3------>|

As mentioned above, a triple DES key is a bundle of three DES keys. A DES key is 64 bits long, but only 56 bits of these are used in the encryption process.

A triple DES key is therefore 3 x 64 = 192 bits long, but the keyspace is only 3 x 56 = 168 bits.

Note that if "triple DES" key is not exactly 192-bits long - i.e. exactly 24 bytes long, or 48 hexadecimal digits - then someone do not have a valid triple DES key.

The other 8 bits are meant to be used as error detecting or "parity" bits so, in principle, the validity of the key bit string can be checked (every byte should be of odd parity), but this is hardly ever done. Most people and most software packages, including CryptoSys API and CryptoSys PKI, do not bother to check the parity of the key and just ignore the state of the parity bits. Be careful, though, because this means that the keys represented by the following bit strings are treated as being equal, and will produce identical ciphertext output for the same plaintext input:

0123456789ABCDEF FEDCBA9876543210 89ABCDEF01234567

0022446688AACCEE FFDDBB9977553311 88AACCEE00224466

3.6 QUESTIONNAIRES

Two questionnaires have been constructed and distributed for this study as part of the research methodology. The pre-test questionnaire collects data about the general requirements for electronic medical record system in the health sector before developing the system. On the other hand, the post-test questionnaire collects data about the system after testing it in Khaled Bin Alwalid Hospital, Benghazi, Libya. Each questionnaire has 138 respondents out of 148 total population of staff working in the hospital and all

data are valid without any missing values. However, the 138 respondents chosen for this research is the total population of system users in the hospital. The other 10 respondents is not included in this research because they are not going to use the system in the hospital. In chapter 5, all collected data is discussed and analyzed in order to come out with the research results and to conclude if these results meet the research objectives.

3.6.1 Questionnaire Validation

3.6.1.1 Pre-test Questionnaire Validation

Table 3.1 shows sources where researcher derived questions for construction of pre-test questionnaire.

Table 3.1: Pre-test Questionnaire Validation

S/No	Questions	Reference
A1	What is your gender?	(Noureldin et al., 2013)
A2	What is your age?	(Noureldin et al., 2013)
A3	What's your nationality?	(Noureldin et al., 2013)
A4	What is your current degree of education?	(Nalkar, 2013)
A5	What is your current occupation?	(Brooks & Grotz, 2010)
A6	Do you know about electronic medical record?	(Brooks & Grotz, 2010)
A7	Have you used electronic medical record before?	(Brooks & Grotz, 2010)
B1	Electronic medical record is the most important phenomena of modern technology in the present day.	(Brooks & Grotz, 2010)
B2	Patient's data can be stored more efficiently through the electronic medical record.	(Adesina et al., 2011)
B3	Electronic medical record reduces the administrative burden for staff in the health sector.	(Cook et al., 2013)
B4	Electronic medical record security is more than the traditional paper record.	(Cook et al., 2013)
B5	I recommend using the electronic medical record system in the hospital.	(Cook et al., 2013)
B6	All staff in the hospital needs to give their full commitment to the implementation of electronic medical record to ensure its success.	(Cook et al., 2013)

S/No	Questions	Reference
B7	Please choose which information about a patient that is/are useful to be included in electronic medical record that can help to smooth your work in the hospital.	(Cook et al., 2013)

3.6.1.2 Post-test Questionnaire Validation

Table 3.2 shows sources where researcher derived questions for construction of post-test questionnaire.

Table 3.2: Post-test Questionnaire Validation

S/No	Questions	Reference
A1	What is your gender?	(Noureldin et al., 2013)
A2	What is your age?	(Noureldin et al., 2013)
A3	What is your current degree of education?	(Noureldin et al., 2013)
A4	What is your current occupation ?	(Noureldin et al., 2013))
A5	Are you a user of electronic medical records system prototype?	(Noureldin et al., 2013)
B1	It was easy to learn to use this system.	(Brooks & Grotz, 2010)
B2	The system is easy to be used.	(Brooks & Grotz, 2010)
B3	The information in the records can be created, edited, stored and managed more effectively by using this system.	(Brooks & Grotz, 2010)
B4	I was able to complete my tasks in a short amount of time by using this system.	(Brooks & Grotz, 2010)
B5	I could complete my tasks effectively by using this system.	(Musabi, 2010)
B6	I believe I could become productive by using this system.	(Musabi, 2010)
B7	The system has a user-friendly design.	(Musabi, 2010)
B8	Whenever I made a mistake using the system, I could recover information easily and quickly.	(Brooks & Grotz, 2010)
B9	This system has all functions and capabilities as expected.	(Brooks & Grotz, 2010)
B10	Overall, I am satisfied with this system.	(Brooks & Grotz, 2010)
C1	I believe that authentication is necessary to ensure the security of records (e.g. using user name, password, etc.).	(Inglesant & Sasse, 2010)
C2	I believe that unique passwords and user names that consist of letters, numbers and symbols help prevent unauthorized access to the system.	(Jenkins et al., 1977)

S/No	Questions	Reference
C3	I believe that same username and password cannot be used for various accounts.	(Inglesant & Sasse, 2010)
C4	I believe that it is compulsory to clear all browsing history before logging off computer.	(Inglesant & Sasse, 2010)
C5	I believe that it is necessary to logged off computer after finish using it.	(Gurav & Deshmukh, 2014)
C6	I believe that high speed internet will reduce the service delay (availability) and ensure safe delivery of records.	(Cucoranu, 2013)
C7	I believe that anti-virus or anti-malware programs and firewall must be installed in all computers and updated regularly.	(Cucoranu, 2013)
C8	I believe that by conducting system backup can keep records readily available and always safe in the event of incidents such as fire, cyber-attack, natural disaster or others.	(Gurav & Deshmukh, 2014)
C9	I believe that the use of encryption technology can protect records from being read by unauthorized people, regardless records that are locally installed or accessed over the Internet.	(Perumal, 2013)
C10	My hospital should implement effective security measures against various security threats to electronic medical records.	(Gurav & Deshmukh, 2014)

3.7 CONCLUSION

This chapter provided description of the materials used and methodology selected to develop the HMS prototype that is by adopting system development life cycle (SDLC) model, Visual web developer 2010 (which includes the local web server) and Visual Basic software and also questionnaires.