Access Control to Protect Health Information for A.B.U.T.H Hospital

By
Muhammad Musa
JAN16/COMP/009X
School of Computing and Engineering

Supervisor
Prof. F. Tushabe

A Proposal submitted to the School of Computing and Engineering in Partial fulfilment of the requirements for the award of Masters in Computing (Computer Security options) of Uganda Technology and Management University (UTAMU)

December 2016

CHAPTER ONE

INTRODUCTION

1.0 Introduction

Electronic medical record is an important tool that helps medical professionals to use for the collection, extraction, management, sharing and as well as searching of health information. As a result of that, the need for health information security becomes very significance. Despite the help of EMR to medical practitioners by simplifying their work, there are still some barriers that hinder its full integration among which include, health care professionals do not actively participate in the development process of EMR access control which imposes them extra effort in its use [7]. The main objective of this research is to review how access control has been studied, designed and implemented in general and compare this to similar research in the healthcare domain, more specifically within Health Information Systems (HIS). This review will help identify what are the main issues regarding healthcare professionals' needs in terms of access control, and identify the barriers that usually prevent the successful integration of access control systems into EMR. If the improvement of access control development and usage can reduce some of the EMR integration barriers then we hypothesize that patient treatment and support can be improved.

Traditionally, some industries are more prone to attack than others banking and finance for example but recent events clearly demonstrated that healthcare is fast becoming the target of choice for hackers. Why may you ask? It's pure economics: the black market value of a private medical record can be worth vastly more than stolen financial data. The FBI have reported that partial EHRs are being traded for as much as $50, compared to just $1 for a stolen credit card or social security number [21]. This report clearly shows that there is an urgent need of conducting research for improving access control of health care information system such as Electronic Medical Record. The Research contains three variables Access Control, Authentication and Health care information systems. **Access control** is the process by which resources or services are granted or denied on a computer system or network.

Access control has a unique set of terminology that is used to describe its actions. Consider the following scenario: "Megan is babysitting one afternoon for Mrs. Smith. Before leaving the house, Mrs. Smith tells Megan that a package delivery service is coming to pick up a box, which is inside the front door. Soon there is a knock at the door, and as Megan looks out she

sees the delivery person standing on the porch. Megan asks him to display his employee credentials, which the delivery person is pleased to do. Megan then opens the door and allows him to pick up the box" [3], pg 255 of 590. This scenario illustrates the basic steps in access control. In this scenario, the package delivery person first presents his **identification** to Megan to be reviewed. A user accessing a computer system (eg Electronic Health Record) would likewise present credentials or identification when logging on to the system, such as a username. Checking the delivery person's credentials to be sure that they are authentic and not fabricated is **authentication**. Computer users likewise must have their credentials authenticated to ensure that they are who they claim to be, often by entering a password, fingerprint scan, or other means of authentication.

Hence, poor access control leads to higher percentage of intruding into the health information system. Once a system has a very good and authenticated access control, it will be harder for an intruder to break through and have access to information for alteration and other illegal activities relating to data security.

To understand the access control, Andrew Hawker gives a scenario with our normal houses. Assuming if someone calls at your home and asks to be allowed in, your immediate response will be to apply ***access controls***. You will first of all want to check on the person's identity. You may deem it prudent to do this by taking a look through the window, to see if you recognize your visitor *before* you open the door. If it is someone on official business, you may ask to see an identity card, or cross-examine them to find out whether they seem to be genuine. Once allowed to be inside your home, you will expect to place some restrictions on your visitor's behavior [9].

The same basic ideas is said to be applied to access controls in health care information systems. Check point need to be applied that is expected to screen and authenticate every user that need to have access to health information systems and this is to ensure privacy of patients' records and also to prevent an intrusion or attack to the systems.

Computer access control can be accomplished by one of three entities: hardware, software, or a policy. Access control can take different forms depending on the resources that are being protected. We have three access controls as follows:-

I. **Physical access control;** creates physical barriers that regulate how users come in actual physical contact with resources. For example making the physical location of data centers to be secured and protected against physical contact or hazard that could le to damages of the hardware.

II. **Network access control:** involves what access an authorized user has to network resources. For example corporate virtual data center is accessible via a network and for commercial organizations like banks or insurance companies only authorized users are allowed to have access to such their respective information.

III. **Operating system access control**: governs the access of users to files, programs, utilities, and hardware managed by the operating system [(Ciampa, 2009), pg 256].

This research will be on operating access control of health information systems that governs the access of users to files, programs and utilities using authentication mechanisms.

1.1 Problem Background

Ahmadu Bello University Teaching Hospital is one of the largest consultancy hospital that offer medical services to hundreds of patients daily. Although the hospital has health information system, there are a lot of activities that are manually being operated using paper, files and pen. Patients' registration process and access to health records are manual. This brings inconsistency, inefficiency and consumes a lot of time in searching and sharing health information within and outside hospital.

The manual system of operation lacks confidentiality and privacy this is because unauthorized personnel such as admin staff, askari (hospital security), and other non-medical staffs of the hospital can easily access patients medical records which violate patients' privacy and confidentiality.

Other challenges affecting the hospital are losing of patients' files, searching for a particular patient record among hundreds of files and many other problems. Also, the existing system is more on advertising the hospital activities and hence lacks an interactive and secured interface that can allow physicians, nurses, admin staffs and patients to have access to health information system electronically and within the privacy laws to enhance good service delivery.

This research will be carried out to develop health information system for Ahmadu Bello University Teaching Hospital (ABUTH) Zaria Kaduna State of Nigeria as a case study that will

be protected using two-factor authentication access control to ensure confidentiality and privacy of patient medical record. Figure 1 shows the existing system of ABUTH currently use by the hospital.

Figure 1: interface of ABUTH health information system

1.2 Statement of the Problem

With regards to the summary of problem background mentioned in paragraph above, this research will be focus on developing a system that will impose access control using two-factor authentication to ensure privacy and confidentiality of patients' medical record.

1.3 Purpose of the Study

The purpose of this study is to review the existing health information system of ABUTH and design a new system that will support the implementation of access control using two-factor authentication and authorization of users (Physicians, Nurses, Admin staffs and Patients) to ensure privacy and confidentiality of patients' medical records.

1.4 Specific objectives of the Study

The Specific Objectives of this research are as follows:-

1. To analyze the existing system and gather necessary requirements for designing a new health information system that will support users (e.g Physicians, Nurses, admin staffs and patients) to have an interactions with new system.
2. To develop access controls that ensures privacy and confidentiality of patients' medical records.
3. To develop a new system that will authenticate and authorize users to access health information based on the security policy and requirements.
4. To conduct unit testing and validate the prototype of the new HIS system.

1.5 Research Question

The questions expected to be answered by this research are as follows:-

1. How does the existing system will be use to gather requirements for the new system?
2. How access control will be inforce in the new system?
3. How the new system can be well develop?
4. How can we conduct the unit testing and validation of the new system?

1.6 Conceptual Frame work

In order to securely access information within a system three steps are usually required:

a) Identification (where a user says who he is, e.g. with a login username);
b) Authentication (where a user proves his identification given in the first step, e.g. with a password or a PIN number); and
c) Authorization (where access rights are given to the user). Whilst access control is conceptually part of the authorization process that checks if a user can access the resources he requested [7].

Figure 2: Diagrammatic representation of access control

Figure 1 above shows the conceptual frame work of access control to an information system, but we need to take note that even if the user *is* permitted access to the system, restrictions will be placed on the facilities which can be used (marked with a tick or a cross in the diagram). The pattern of access which is enforced in this way will be specially tailored for each user [9]. In the diagram above, organizational boundary means Health Care Information Systems. Access request is the request that is expected to come from authorized users. Access control is the policy and procedures concerning security matters that a user most certifies before having access to his or her information, which are identification, Authentication and authorization.

1.7 Significance of the Study

The significance of the study is based on the 3 areas below: -

1. The general Public will gain more confidence in attending the hospital because they know that the hospital records system ensures privacy and confidentiality.
2. The medical personnel will be able to fulfil their oath of sustaining confidentiality and privacy of patient medical record within their e-records.
3. More patients will come to the hospital because the system is secured and trusted.

1.8 Scope of the study

The scope of this dissertation is limited to developing a system for health care information system using two-factor authentication access control. The technologies discussed in the literature review will also focus on the same subject.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

As well as, Pourasghar's study underlined that the security mechanisms for protecting medical data in HIS environment were inadequate in six university hospital in Tehran (the capital city of IRAN) and all HIS investigated suffered from lack of policies for information security, weak authentication techniques, absence of functions for managing users and log files. Therefore, planning and implementing more effective security policies are necessary to overcome weaknesses in different dimensions of information security [24]. Trends in information technology encourages the heath sector across the world to imbibe the use of electronic system in recording, saving and sharing of patients within and outside hospitals but according to privacy laws. Patient health record is one of the sensitive information that needs optimum security protection. Also, medical staff should be aware of the security measures need to protect their patient data. Therefore, many efforts have been made *about the* security in healthcare information systems in recent years. Meanwhile, it was stated that these electronic environments raise new issues of ethics, security and privacy [24].

It can be seen that the underlying issues and for that matter aspects that are particularly important in relation to the security requirements of healthcare are data integrity, data confidentiality, data authenticity, and user authentication (identity verification). In this context, achieving secure user authentication forms the basis for all the other measures to be achieved [25].

This chapter will review related literatures concerning access control using authentication in health care information systems. Authentication process is categorically sub divided into three as follows:-

1. Something you know (a password);
2. Something you possess (a token);
3. One or more of your personal characteristics (biometrics).

In practice, according to [Andrew Hawker] above mentioned approaches are often used in combination. For example, to obtain cash from a cash machine you will need to use something you possess (a card) together with something you know (a Personal Identification Number).

Such combinations are considerably stronger than each method on their own, providing that they are independent of one another.

2.2 Terminologies in Medical IT Solutions

(Shin, 2012) in his thesis defined different medical terminologies in Information Technology as follows:-

DSS (Decision Support System): A system that analyzes data and support information needed to make decision. It enables accurate decision making in a variety situations.

DW (Data Warehouse): An integrated analysis system in which necessary data are obtained from separate systems and archive in centralized repository, so that users can have access to them at any time.

EHR (Electronic Health Record): An extension of the electronic medical record which aims at prevention of disease and improvement of diagnosis and treatment by computerized not only clinical data of a patient but also all health related records pf an individual.

EMR (Electronic Medical Records): A computerized system for managing and research all patients medical records. An electronic version of medical record that offers accurate and complete health information and supports decision makings based on medical knowledge replacing traditional papers charts.

HIS (Hospital Information System): A hospital's core system that enables sharing of accurate and consistent data with other departments of a hospital through integration of hospital information and computerization of work process. It consists of medical treatment information systems, administration information system, medical treatment support system, business administration system, etc.

OCS (Order Communication System): A system that offers a Database (DB) in which a variety of medical information and patients' data are stored and transfers a doctor's prescription to the corresponding medical department through a communication network. It is an information system that manages all processes from patient to medical treatment to billing and allows follow-up of procedures and result. It is often confused with HIS.

PACS (Picture Archiving Communication System): A digital medical image archiving and transferring system that digitizes the image obtained from a radioactive imaging device and transfers them along with medical record to each terminal though a network.

2.3 Theoretical review

Pedersen [15] Stated that, Privacy on the web is therefore highly associated with keeping information and transactions secret and restricted to certain users and entities. It is also a process that naturally requires authentication. For an indeed very thorough survey of literature on privacy in HCI (including a massive 315 references), we refer to Iachello and Hong.

2.3.1 Authentication methods

Pedersen [15] briefly outline different authentication methods currently employed on the Web. We present three common methods of authentication and discuss their advantages and disadvantages in terms of both security and various points of interest concerning usability factors. Specifically, we have a look at passwords and how to create and memorize these, public key cryptography (with focus on Diffie-Hellman and RSA), and lastly two-factor authentication.

i) Passwords

Password is a widely used method of authentication techniques that is use to verify and allow users having access to information systems or transactions. Password is being used in webmail, home banking, Facebook, ATM, online forum etc. The most important aspect to consider in using password is length of the password. This is due to the fact that the more the length the stronger the protection of the services it granted access to. [Miller] investigates this more generally concerning passwords. He collects results of various experiments measuring test subjects' abilities to memorize different situations, numbers and even sensory experiences. Miller's experiments are primarily focused on short-term memory, though, and he recognizes that the ability to remember a far greater number of characters or entities in general dramatically increases as we for instance increase the number of attributes attached to the objects to remember (face recognition, for instance, involves both the eyes, nose, hair color, etc.). So, for our immediate interest in passwords which have very few unique characteristics the optimal length of a password that it memorable by the user is somewhere around seven. Actually, many web-based services require that new passwords be between six and eight characters in length. [Yan et al.] Also investigate the tradeoff between using an easy-to-remember password that is often weak against common brute-force or dictionary attacks, and a complex randomly-generated password with the opposite properties. They argue that complex passwords may compromise security because users are more likely to write them down or even put them on a

piece of paper on their screen. They investigate that, passwords generated from different advice given and segment their subjects into three groups as follows:-

Group A

This group asked to generate a password of at least seven characters that contains at least one number.

Group B

This given a matrix containing random characters and numbers and is asked to randomly select eight characters from the matrix, write them down and memorize them.

Group C

This group is asked to create simple sentence of eight words and choose for instance the initial letter of each word as well as inserting a number or a special character somewhere in the password.

The results of the experiment show that the average length of the generated passwords was between seven and eight characters, and that attacks on group A's passwords successfully cracked around 30% of them while groups B and C both were well below 10%. Also, the difficulty and time consumption of memorization in group B was significantly higher than groups A and C. The authors therefore conclude that mnemonic-based passwords are both more secure and easier to remember, that length matters, that special characters should be enforced, and that compliance with the password advice given should be enforced by the system. Otherwise users will ignore that advice and select passwords more susceptible to attacks.

ii) Two-factor authentication

Two-factor authentication has come up in an effort to develop and bring more secure system. Two factor system of authentication uses the technology of something you know (eg Password) together with something you have (eg PIN generator like token or smart card). Also, something you have could be physical eg finger print, an iris scan or a small card containing some number of one time keys. Two factor system of authentication consider to be more secure than password authentication and very easy to use.

Weakness

According to Pedersen [15] two-factor authentications are vulnerable to man-in-the-middle attack.

iii) Graphical Authentication

Graphical password systems can be classified as either recognition-based, cued recall-based or pure recall-based [2]. Recognition involves identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. On contrast, pure recall is retrieval without external cues to aid memory. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage, for example, remembering a textual password that one has not written down. Pure recall is a harder memory task than recognition [13]. Between pure recall and pure recognition there is a different form of recollection: cued recall. An example of cued recall within graphical password systems is scanning an image to find previously chosen locations in it. Viewing the image cues the user about the locations. This is easier than having to recall something entirely from memory (i.e. free recall), but harder than simply recognizing whether a particular image has been seen before or not (i.e. recognition).

iv) Recognition based techniques

In recognition based techniques, users are given a set of pictures and they pick and memorize some of them. During authentication, the users need to recognize and identify the pictures they have picked earlier [13]. Song proposed an graphical authentication scheme based on Hash Visualization technique [19]. In their system, user will be asked to select certain number of images from a set of random pictures generated by a program (figure 4). Later, user will be required to identify the pre-selected images to be authenticated. The results showed that 90% of all participants succeeded in the authentication using their technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach, but has a much smaller failure rate.

Recognition based techniques weakness

A drawback is that the server needs to store a large amount of pictures which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Interface wise, the process of selecting a picture from picture database can be tedious and time consuming for the user.

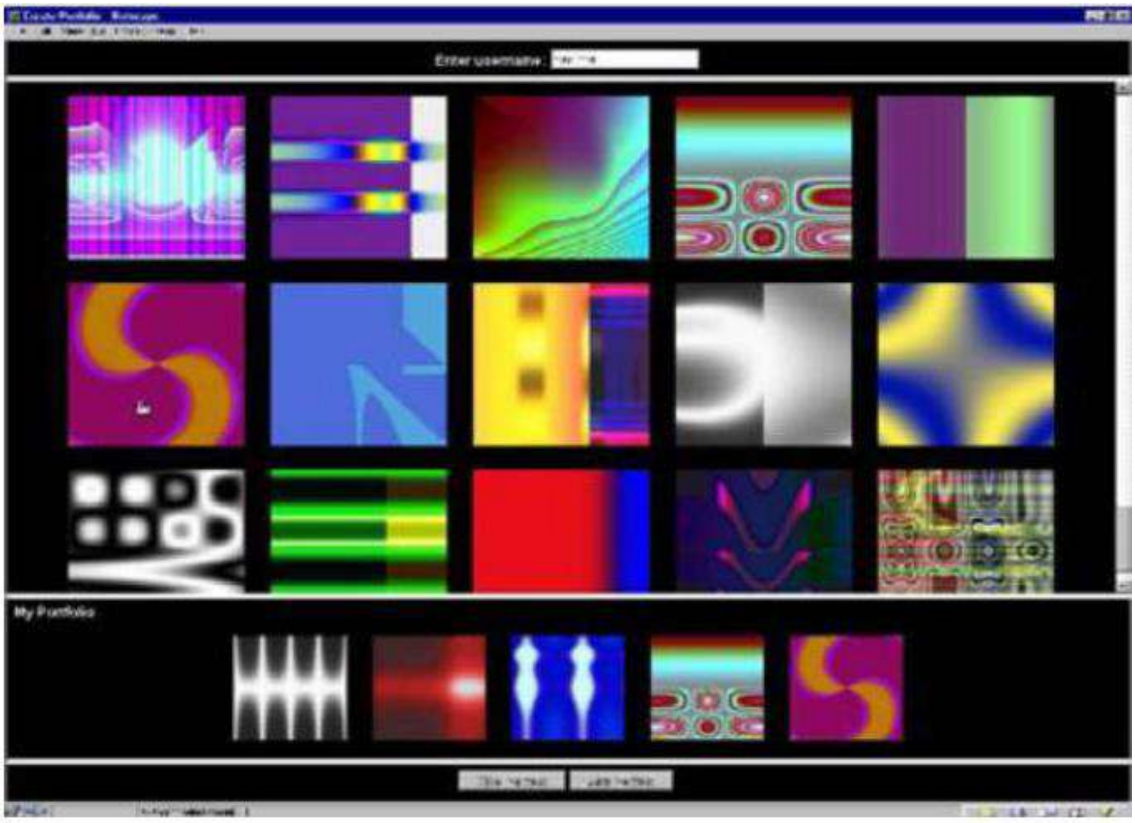

Figure 3: Dhamija and Perrig [11] used random art

[7] Devisetty, 2004 proposed the basic scheme is similar to the technique proposed by Dhamija and Perrig. The difference is that this technique uses the hash function SHA-1, which produces a 20 byte output. This makes the authentication secure and requires less memory. However, an image file still occupies more space than text even after hashing. The authors suggested a possible future improvement by providing the persistent storage and this could be deployed on the Internet, cell phones and PDA's.

v) Pass faces Authentication

Passface is a technique developed by real user corporation (www.realuser.com). The idea behind it is that, user will be asked to choose 4 images of human faces out of the 9 displayed on the authentication screen of which the faces are retrieved from the stored database as users future password. A user is said to be authenticated if he successfully chooses the correct 4 images correctly. The techniques is based on the assumption that, people can recall human faces easier than other object pictures. An example of Passfaces authentication interface is shown in figure 4.

Weakness of pass face authentication

[17] According to comparative study carried out by Sasse, 2000 identified that, passface had only a third of the log in failure rate compared to text based password. Their study also ratifies that passface log in need more processing time than text password which causes less frequency used by the users.

Figure 4: Example of Passfaces

v) Biometric authentication

According to Okoh 2015 [16] Biometric is the science or technology trends that identity of an individual based on the physical, chemical or behavioral attributes of the person. Hence, biometric is the science of identification or authentication of individual using physiological or behavioral characteristics. During the mid-19th century, biometric technology has been recommended and applied by law enforcement agencies to identify criminals. The main advantage offered by biometric technology is security and conveniences.

Two major phases of biometric.

Biometric system has 2 major phases to be under go for the successful implementation of the technology. The 2 phases are as follows:-

1) ***Enrollment Phase:*** **-** Enrollment is the process of identifying an individual based on their physical or biometric trails. During the enrollment process, biometric data is captured from the individual (eg Patients) and stored in a database along with identity of the individual.

2) ***Recognition Phase:*** **-** Jain et. Explain that, recognition phase is a verification process whereby biometric data is going to be recaptured from the user and compared against stored template in the database to identify or recognize the user for authentication purposes. Biometric system has 4 different patterns of recognition system which include Sensor, Feature, Extractor, Database and Matcher. The commonly used biometric technology currently in use include: Finger Print identification, Iris identification and face recognition.

Weaknesses of Biometric system (Error and failures)

- Errors:

The two major errors of biometric are:-

False Match Rate (FMR) and False Accept Rate (FAR). In some text books they are called False Positive and False Negative.

i) False Match Rate:- Refers to the probability of two samples of the same biometric trait from the same user falsely declared as non-match. This is meaning that, the biometric system mistakenly rejects a valid individual as an imposter.

ii) False Accept Rate: - This refers to a situation whereby the probability of two samples of different biometric trail is mistakenly recognized as a match. Hence, biometric system accepts an imposter as a valid individual.

- Failures:

  Biometric system has 2 major failures as follows:-

i) Failure to Capture (FTC) and

ii) Failure to Enroll (FTE).

2.4 Conceptual Frame work

Reference to literatures I reviewed and summarized in the previous paragraphs, I studied password authentication, Two-factor authentication, Graphical Authentication**,** recognition based techniques, pass face authentication and biometric authentication respectively. Strength and weaknesses of each one of them is studied. This research will be conducted based on web application health information system. The scope of the of the research is limited to developing an interface that will identify and authenticate patients to view their health information from anywhere provided that there is network availability. Hence, applying any authentication that require physical device to authenticate user before having access to his or her record will be tedious to users. Let me take biometric authentication as an example. Biometric has 2 phases as mentioned above enrollment phase and recognition phase. Both the two phases require a user to interact with biometric capture device before

one could successfully be authenticated. A patient can find himself in an urgent need of his medical record, where the biometric device is not present for the patient to be authenticated before having access to his data. Based on my understanding concerning the subject matter, two-factor authentication will be applied in the implementation of my research. Two factor is the combination of something you have (eg PIN) and something you know (eg Password). At this point, using a username and password is common in web application. Instead of that, I want to use three arguments as follows:-

- ✓ **Security Question**
- ✓ **Security Answer**
- ✓ **Patient Identification Number**

Figure 5 will show the pictorial representation of the relationship between the research variables and also serves as a model on how the system will identify and authenticate patients before they will be granted access to their health information. To make the system secure and accessible to patients, two security bridge need to be cross by the authorized user. First during enrollment process, patient will be allowed to ask himself a short question of not more than 4 or 5 words. Patient will also give the security answer to that question. The system will check and identify the user by matching the question and answer with the one stored in the database. If they are found correct, then the next security bridge will be patient identification number. Then if it found correct, user will be allowed to view and print out his or her records.

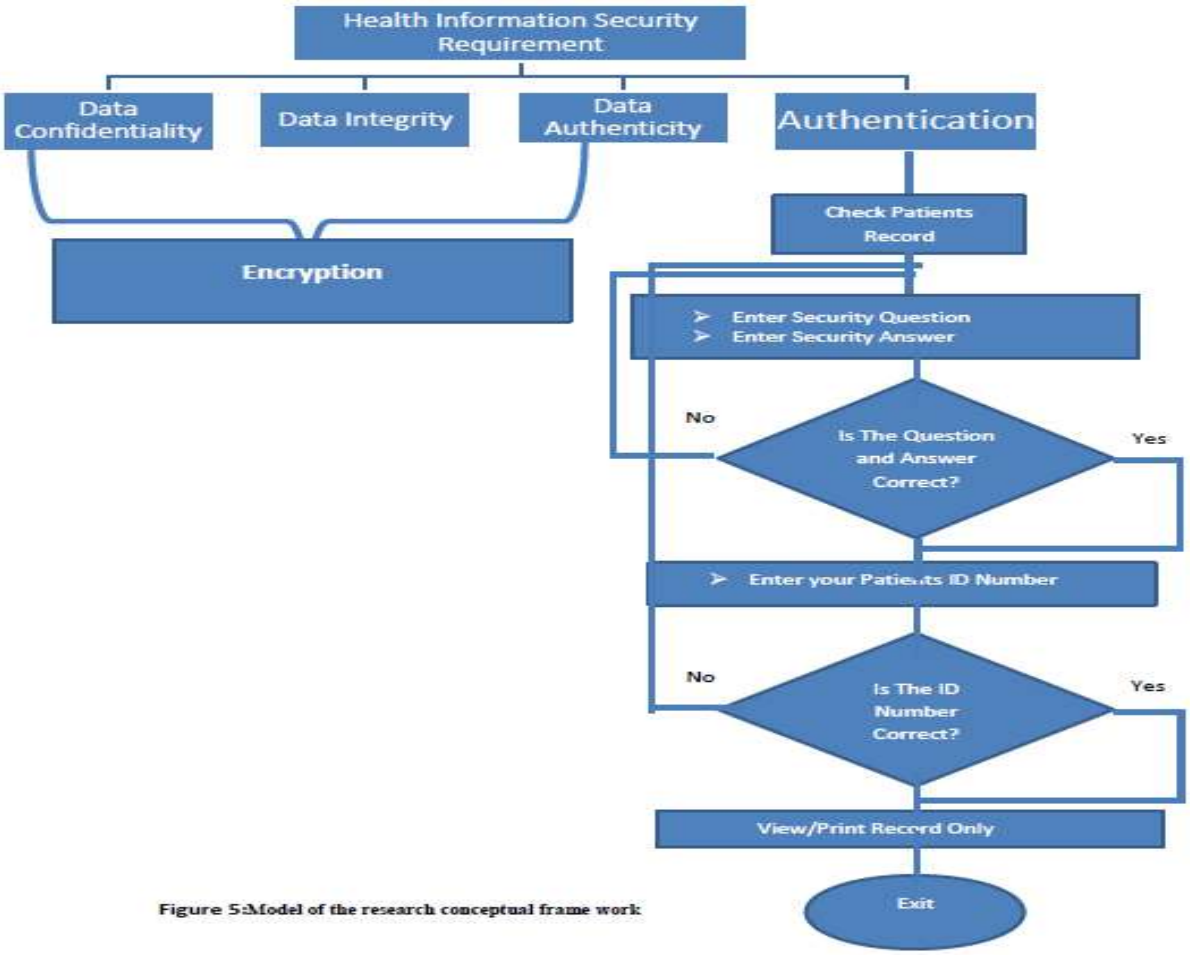

Figure 5:Model of the research conceptual frame work

2.5 Data Access Control use by Federal Medical Center Katsina State of Nigeria

Federal Government of Nigeria has 20 medical centers across the country, located in 20 different states under the control and supervision of federal ministry of health. Federal medical center Katsina is one among the 20 medical centers we have in the country situated at Katsina state. The center uses electronic medical record to store and share patient health record but locally accessible within the center from one department to the other. Patients have access to their medical record via email. Patient has to send written application requesting for their medical record. In the letter a patient has to specify the way he or she want the report, either hard copy or soft copy. If it is a soft copy, the report will be sent to you through your email address. This is the same method that is almost applicable in most of the Nigerian hospitals. One of the specific objective of this research is to review different authentication mechanisms and identify the secured one which will be applied for controlling data access in Health care information system, such that patient can have access to their medical record online.

2.6 Synthesis of the literature review

Reference to literatures reviewed so far, we studied different authentications technology and identify their weaknesses and strength. The research recommended two-factor authentication, and decide to improve on it using what you have (i.e Asking user a security question and answer) and what you know (i.e allowing a user to type his identification number). This is to change from usual username and password. The new idea will solve problems of cracking passwords and usernames, this is because both the security question and answer will be longer than usual username and password, and will be easily remembered and memorized by the users logically.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter gives a brief account on how the research is going to be carried out such that to achieve the objectives of the research and to answer the research questions. This includes the requirement gathering, System design, system implementation, system testing and evaluation. However, the development process is iterative, though it will be depicted as comparison of phases as shown in figure 6.

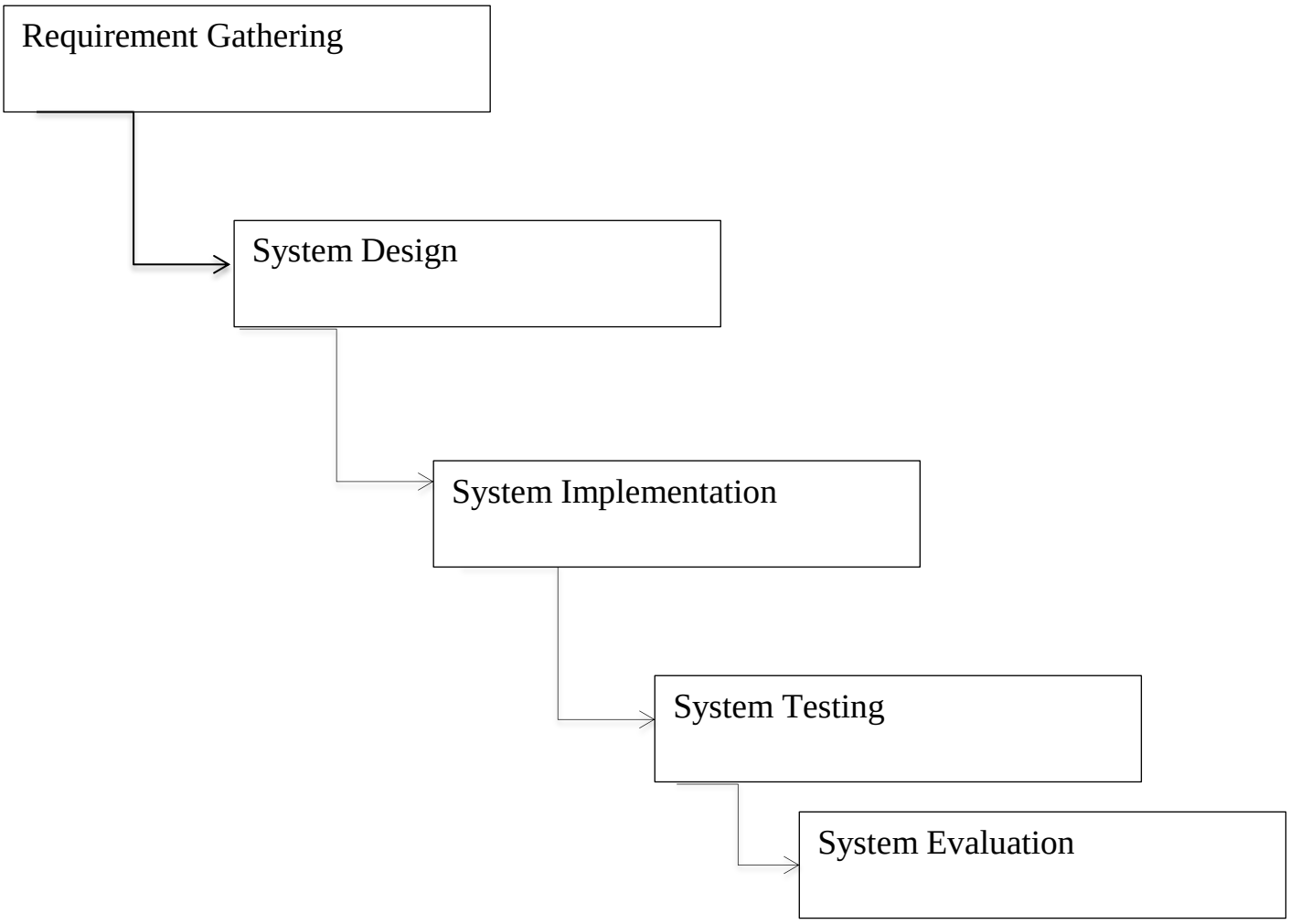

Figure 6: An illustration of a systems' development methodology for health information system (HIS).

3.1 System Development Methodology

Let us now describe the different phases and the related activities of system development life cycle or methodology that will be follow to achieve the research objectives.

Phase 1: Requirements identification

There will be a thorough study of the existing systems of Ahmadu Bello University Teaching Hospital in order to understand the loop holes before developing the HIS system. This will be achieved through document review, observation and interviewing the stake holders in the concern area.

Document Review

Documents such as files, application forms, patients visiting cards, journals and other necessary documentation will be reviewed to help me gather necessary requirement in applying access control to develop a secured HIS.

Interviews

Oral interviews will be conducted between the researcher, the nurses, the physicians and admin staffs of Ahmadu Bello University Teaching Hospital to help me gather necessary requirements in developing the HIS.

Observation

In this approach, observation approach will be applied to help me understand how manually the information concerning patients is recorded and use by the physicians and nurses. Observation is one of the important approach gathering requirements for system development whereby Systems Analyst participates in or watches a person perform activities to learn about the system.

Phase 2: System Design

The inputs from users and information gathered in requirement gathering phase will be the inputs of this step. The output of this step comes in the form of three designs; logical design, architectural design and physical design. Engineers produce meta-data and data dictionaries, logical diagrams, data-flow diagrams and in some cases pseudo codes.

Phase 3: System Implementation

The implementation will be achieved based on the logical and architectural design under phase 2 for the development of Health Information System. The Database system will be developed using MYSQL and the programming frame work of the system will be designed using HTML, CSS, and JavaScript. There will be Logical design where entities, attributes, data lengths will be made to remove the redundancies in the system and duplicates leading to physical database

design where MySQL with PHP script will be used to design the system that will enable get the graphical user interfaces to be used by the system as it is free software.

Phase 4: System testing

Software testing is a fundamental component of software quality assurance and represents a review of specification design and coding. Unit and module testing will be use during the process. During unit testing, individual functions will be tested to prove their functionality. This helped to reduce errors during module testing where units will be combined as one to form a module. A successful testing will be result into a complete system that was tested as a whole to check for its capabilities and also techniques like black box testing will also be employed so as to achieve the system's final objective.

Phase 5: System Evaluation

The evaluation process involved checking the implemented system whether it confirms inputs to the specifications. Several validation tests such as data and security will be carried out to ensure that the access control if functional to the system by validating data input from the users, authenticate, authorize and reject any data which is supplied in wrong format and prevent unauthorized users from accessing the system resources.

REFERENCES

[1] RealUser. Retrieved September, 2016, from www.realuser.com.

[2] Biederman, I. (1973). Searching for object in real world sense . *Journal of Experimental Psycology* , 22-27.

[3] Ciampa, 3. M. (2009). *Security + Guide to Network Security. Third Edition.* Boston, USA.

[4] Cohn, S. (2006). Privacy and Comfidentiality in the Nationa wide Health Information Network .

[5] D. (2010). The two path of PHR Hospital and Health Network. 44-46.

[6] Devisetty, A. A. (2004). Image Bqased Registration and Authentication System . *Midwest Instruction and COmputing Symposium*.

[7] FERREIRA, A. (2010). *Access Control: how can it improve.* Center for research in health information Systems and technologies.

[8] Ferreira, A. (n.d.). MODELLING ACCESS CONTROL FOR HEALTHCARE. 1-2.

[9] Hawker, A. (2005). *Security and Control in Information Systems.* USA: Tailor an Francis e-library 2005.

[10] Kotz, D. (2014). A Privacy Frame work for Mobile Health and Home Care Systems.

[11] M, K. (2010). Acitivity oriented access control to ubiquitos hospital information and services . *Information Sciences*.

[12] Managing the Security of Nursing in the Electronic Health Record. (n.d.).

[13] Norman, D. (n.d.). *The Design of Every day Things. Basic Book.*

[14] Okoh, E. (2015). *Biometric Solution in e-Health Security.*

[15] Pedersen, A. B. (2010). *Usability of Authentication in web application.*

[16]Perrig, R. D. (2000). A User Study Using Images for Authentication. *UNISEX Security Symposium*.

[17] Sasse, S. a. (2000). Are Passface more Usable than Password?: A Field Trail Invesitigation . *People and Computing XIV*.

[18] Shin, D. I. (2012). *Improving Trust and Securing Data Accessibility for e-Health Decision Making System by Using Data Encryption Techniques* .

[19] Song, A. P. (1999). Hash Visualization: A New Technique to Improve Real World Security. *Internation workshop on Cryptographic techniques and e-commerce.*

[20] Stallings, W. (n.d.). *Computer Security Principles and Practice, Second Edition.*

[21] Turgeon, J. (2016, May 24). *Securely Managing the internet of things for health care*. Retrieved from Security Info Watch: www.securityinfowatch.com

[22]UTAMU. (2014). Graduate Studies Guidelines on Proposal and Dissertation.

[23] Vincent, S. (2015). *A study of Access Control for Health Electronic Records, Master Thesis.*

[24] Zaria, A. B. (n.d.). *abuth*. Retrieved 2016, from www.abuth.org.ng.

[25] Managing the Security of Nursing Data in the Electronic Health Record.

[26] Biometric in e-health system.