Using Access Control to Protecting Health Information System

A Case Study of Ahmadu Bello University Teaching Hospital

By

Muhammad Musa

JAN16/COMP/009X

Department of Computing and Engineering

Supervisor

Prof. F. Tushabe

A Proposal submitted to the Faculty 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)

November 2016

APPROVAL PAGE

This is to certify that this proposal is undertaken by Muhammad Musa JAN16/COMP/009X. This has been presented in accordance with the regulation governing the award of Master of Science in Computing (Computer Security) Uganda Technology and Management University (UTAMU).

Prof. Florence Tushabe

[Project supervisor]

Date

DECLARATION

I Muhammad Musa with the registration number JAN16/COMP/009X solemnly declare that this proposal was gathered and written by me and with the aid of my able supervisor Prof Florence Tushabe.

Muhammad Musa Date
JAN16/COMP/009X

ACKNOWLEDGEMENT

I must from the onset, express my immeasurable marvelous gratitude to my supervisor for finding time in spite of his usually tight schedule to supervised me carrying out my research work.

My appreciation goes to the management of Nuhu Bamalli Polytechnic Zaria whom agreed to approved and permit me to go for study live, by considering me among many applicants whom apply for the same subject matter.

I reserved special thanks to Tertiary Education Trust Fund (Tetfund) for their financial support to sponsor my education. I want to thank you and May Allah continues to guide, lead and move Tetfund forward and allow them to achieve their desired goals.

I am also extremely grateful to my wife (Hauwa Ummar), my blood brothers Abdulkhaliq Muhammad, Yahaya Muhammad, Jamilu Muhammad, Yunusa Muhammad, Zainab Muhammad, Rabiatu Muhammad, Aishatu Muhammad, Fatima Muhammad, Khadija Muhammad, Saudatu Muhammad, Rahmatu Muhammad, Raliya Muhammad and my children Shukura, Mama, Ummitah, Mubarak and the entire members of my family whom contributed in one way or the other most importantly for your prayers, care and concern.

I reserved special commendations to my friends at Kampala whom I enjoyed being together with them throughout my studies in persons of Mubarak M Bala, Mahdi, Nura Google, Abdul Galadima, Alhaji Aminu (Liman), Sheriff, Muhd Isah, Maishanu, Mallam Harisu Garba, Muhd Auwa Isa, Oyoyo, Faisal, Maishanu, Rufa'i etc.

May Allah Blessed you all.

TABLE OF CONTENTS

Approval page i

Declaration ii

Acknowledgement iii

Table of Contents iv

List of Figures vi

CHAPTER ONE 1

1.0 Introduction 1

1.1 Background of the study 2

1.1.1 The case study organization 3

1.1.2 ABUTH Mission 4

1.1.3 ABUTH Vision 4

1.1.4 ABUTH Objectives 4

1.1.5 Challenges of ABUTH Health Information System 4

1.2 Statement of the Problem 4

1.3 Purpose of the Study 5

1.4 Specific objectives of the Study 5

1.5 Research questions 5

1.6 Conceptual Frame work 5

1.7 Significance of the Study 6

1.8 Scope of the study 6

CHAPTER TWO 8

2.0 Literature Review 8

2.1 Introduction 8

2.2 Terminologies in Medical IT Solutions 9

2.3 Theoretical review 10

2.3.1 Authentication methods 10

2.4 Conceptual Frame work 15

2.5 Data Access Control in Federal Medical Center Katsina State of Nigeria 18

2.6 Synthesis of the literature review 18

CHAPTER THREE 19

3.1 METHODOLOGY 19
3.1.1 Introduction........ 19
3.1.2 Research Design 19
3.1.3 Study Population........ 19
3.1.4 Sampling Techniques and Procedures 19
3.1.5 Data Collection Methods 20
3.1.6 Data Collection Instruments 20
3.1.7 Pre-TESTING (validity and reliability) 20
3.1.8 Data Analysis........ 21
3.1.9 Measurement of Variables 22
3.1.9 Artefact Design 22
3.1.10 Conclusion 23
References........ 24

LIST OF FIGURES

Figure 1: interface of ABUTH health information system..3
Figure 2: Diagrammatic representation of access control (Hawker, 2005)..6
Figure 3: Dhamija and Perrig [11] used random art...13
Figure 4: Example of Passfaces...14
Figure 5:Model of the research conceptual frame work...17
Figure 6: HIS Access Control Model...22

CHAPTER ONE

1.0 Introduction

The widening use of healthcare information systems such as the Electronic Medical Record (EMR), which allows for the collection, extraction, management, sharing and searching of health information, is increasing the need for information security (e.g. confidentiality, integrity and availability) (FERREIRA, 2010). Although EMR can be an important support tool for the healthcare professional there are some barriers that prevent its successful integration. These barriers include the fact that healthcare professionals do not participate in the development of access control to access the EMR imposing them extra effort in its use (Ferreira). 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 EMR systems. 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 (Turgeon, 2016). 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 contain 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 (Ciampa, 2009). 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 (Ciampa, 2009), 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.

1.1 Background of the study

To understand the background of this research, let me give an example 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 (Hawker, 2005). 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.

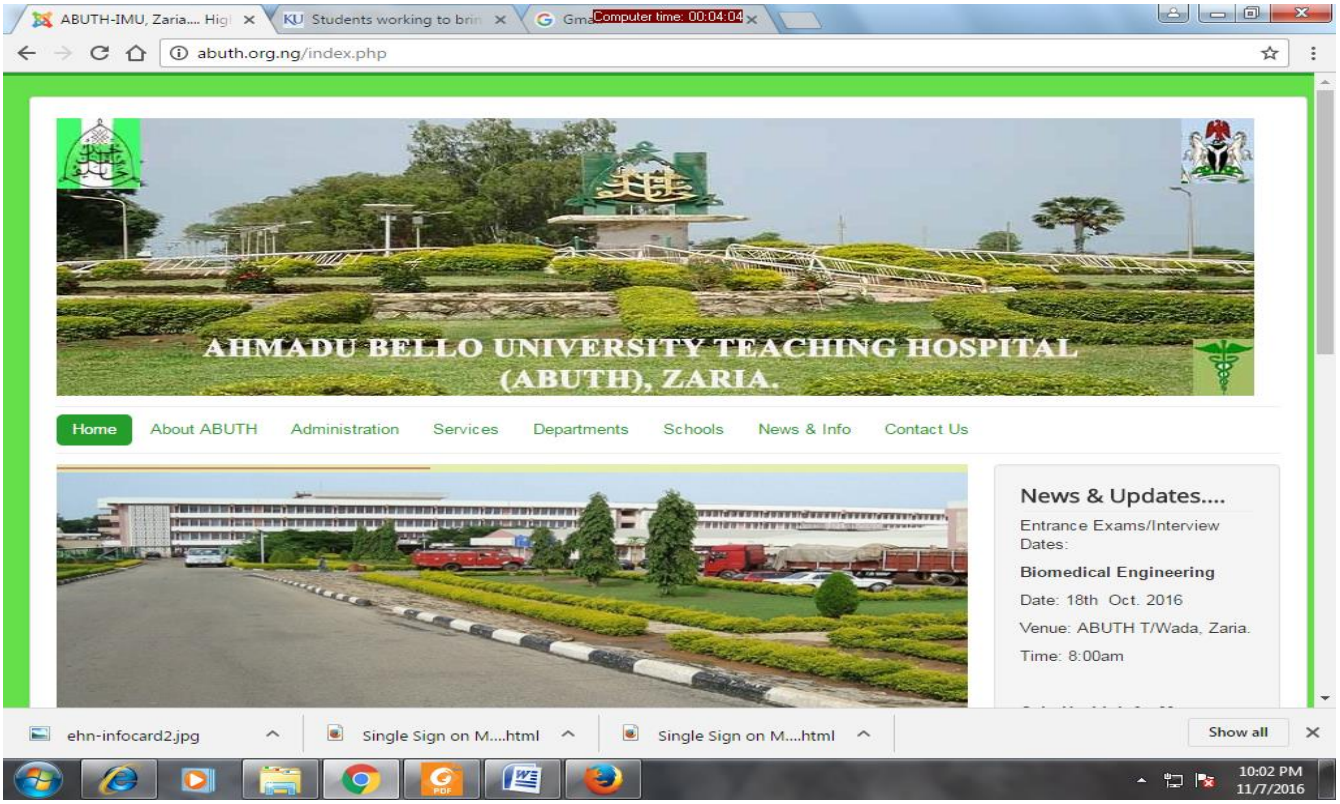
II. **Network access control:** involves what access an authorized user has to network resources. For example corporate virtual data center is accessible via a network and for commercial organizations like banks or insurance companies only authorized users are allowed to have access to such their respective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

1.1.1 The case study organization

The research will be conducted using Ahmadu Bello University Teaching Hospital Zaria Kaduna State of Nigeria. The Hospital is under the control of Ahmadu Bello University, Zaria (A.B.U). ABUTH is training medical students in different professions such as medicine, nursing, surgeon etc. Figure 2 shows the current interface of ABUTH health information system.



News & Updates....

Entrance Exams/Interview Dates:

Biomedical Engineering

Date: 18th Oct. 2016

Venue: ABUTH T/Wada, Zaria.

Time: 8:00am

Figure 1: interface of ABUTH health information system

1.1.2 ABUTH Mission

To offer highly specialized, excellent, prompt, affordable and accessible healthcare services that would meet the health care needs of our clients in an environment that promotes hope and dignity irrespective of status whilst developing highly competent healthcare personnel in an environment that stimulates excellent and relevant research.

1.1.3 ABUTH Vision

To be a tertiary healthcare facility that is second to none in Nigeria and comparable to any center in the world: delivering high quality healthcare services to our clients; training appropriate, skilled and efficient health workers; and conducting research for the advancement of healthcare.

1.1.4 ABUTH Objectives

- To provide a broad range of tertiary services to meet the health care needs of Nigerians.
- To provide technical support to primary and secondary health facilities within the area of operation.
- To provide facilities for the training of different cadres of health workers.
- To conduct relevant research into prevalent health and health related problems.

1.1.5 Challenges of ABUTH Health Information System

The current Health information system of ABUTH lacks an interface that can allow patients have access to their medical record. This research will be carried out to design a secured access control interface that can allow patients view and print their medical record online.

1.2 Statement of the Problem

People can be sick at anywhere they found themselves, which may need medical attention from a professional doctor. The Doctor will require knowing or having past medical records of such a patient in order to know where to start the treatment from. The problem that need to be solve by this research is to work with the medical personnel to develop a secured access control interface for health information system (HIS) of Ahmadu Bello University Teaching Hospital (ABUTH) Zaria Kaduna State of Nigeria, that can allow authorized patients to have access of their medical record from anywhere they are, provided that there is network connection.

1.3 Purpose of the Study

The purpose of this research is to bridge a gap between hospital and the patient in terms accessing medical records by coming up with a secured interface that can allow patients to access their medical record without necessarily coming to hospital physically, but at the same time within the privacy laws. Access Control has been described as “The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner”. Access Control can allow not only a person admittance to secure data, but also the type of access granted as well (Vincent, 2015).

1.4 Specific objectives of the Study

The Specific Objectives of this research are as follows:-

1. The research will review the current Health Information System use by ABUTH and came up with an interface that will identify and authenticate authorized patients so that to securely allow them have access their medical records.
2. Different authentication mechanisms is going to be studied and identify the secured one which will be applied for controlling data access in Health care information system of ABUTH such that to block unauthorized users or intruders from having a chance to steal or causes damage to patient health record.

1.5 Research questions

This research is expected to answer the following questions:-

1. What are the security and privacy requirements of Health Information Systems security?
2. How are the identified security and privacy requirements addressed through the application of access control?

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 (FERREIRA, 2010).

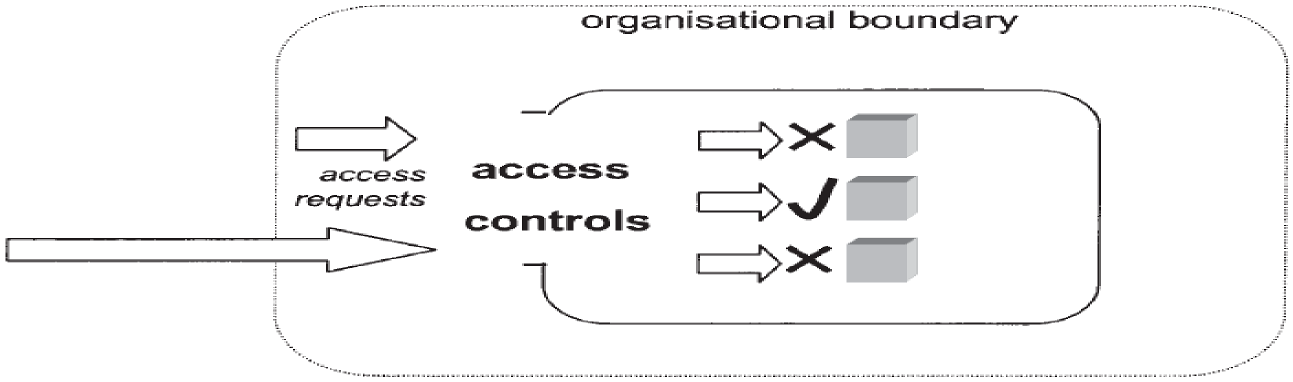


Figure 2: Diagrammatic representation of access control (Hawker, 2005)

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 (Hawker, 2005). 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 this research is to review the related literatures and come up with the solution to access control problems affecting Health care information systems and this is to ensure privacy and well protection of patient health record. National Committee for Vital and Health Statistics (NCVHS), a key advisory committee to the US Department of Health and Human Services. Define Health information privacy as an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data (Kotz, 2014). Also the Committee defined Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" (Kotz, 2014). Hence, imposing access control in health care information system is very significant.

1.8 Scope of the study

The scope of this dissertation is limited to application of access control using authentication in health care information systems. The research will develop and interface that can allow patients have access to their medical records. The technologies discussed in the literature review will also focus on the same subject.

CHAPTER TWO

2.0 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, 2010) [pg 11] 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, 2010) [pg 11] 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. (Pedersen, 2010) **[pg 12]**

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

Two-factor authentications are vulnerable to man-in-the-middle attack [Anders Bjerg Pedersen, 2010]

iii) Graphical Authentication

Graphical password systems can be classified as either recognition-based, cued recall-based or pure recall-based (Biederman, 1973). 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 (Norman). 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. (Norman) proposed an graphical authentication scheme based on Hash Visualization technique (Song, 1999). 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.

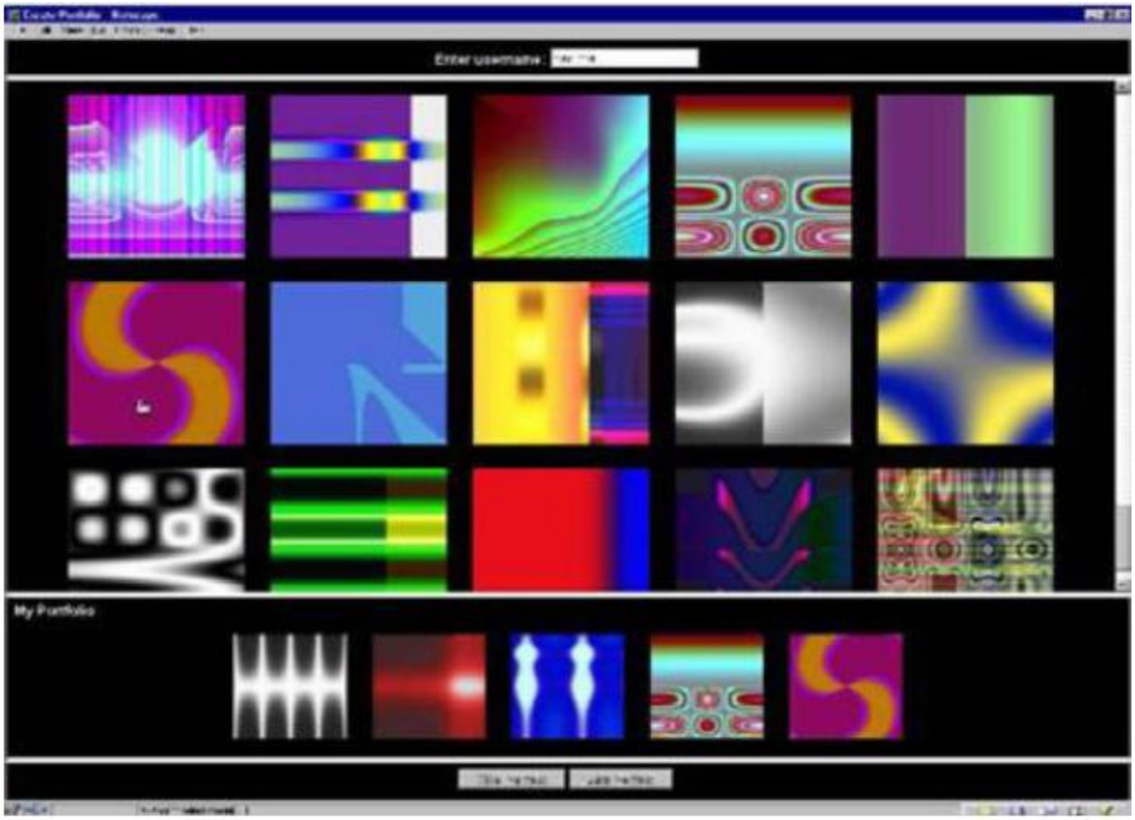


Figure 3: **Dhamija and Perrig [11] used random art**

(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

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

(Okoh, 2015) 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. Al, 2011] 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.

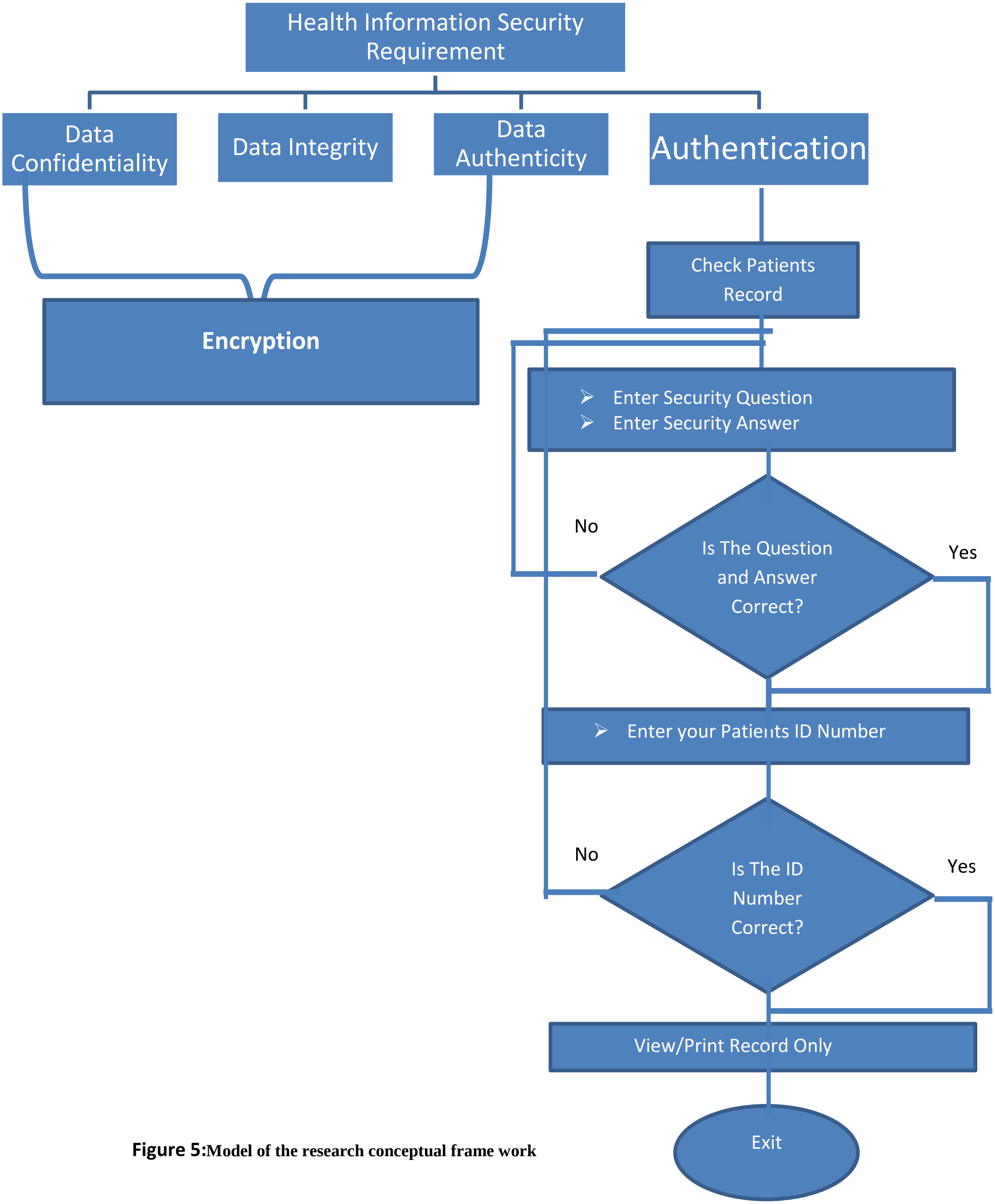

Health Information Security Requirement
Data Confidentiality
Data Integrity
Data Authenticity
Authentication
Encryption
Check Patients Record
➢ Enter Security Question
➢ Enter Security Answer
No
Is The Question and Answer Correct?
Yes
➢ Enter your Patients ID Number
No
Is The ID Number Correct?
Yes
View/Print Record Only
Exit

Figure 5: Model of the research conceptual frame work

2.5 Data Access Control in 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

3.1 METHODOLOGY

3.1.1 Introduction

Research method is a systematic process of collecting, presenting, analysing and interpreting data for the purpose of arriving at dependable Solutions to human problems. Methodology is therefore concerned with the study of the research methods. In a research of this nature, it is necessary to define the research design, area of the study, population of the study, sample size and sample size determination instrument for data collection, validation of instrument, reliability of research instrument.

3.1.2 Research Design

According to (Asika, 1991), Research design means the structuring of investigation aimed at identifying variables and their relationships to one another. A research design is very useful as it helps the researcher to develop a mental image of the structure for gathering the data and the analysis that will follow. The research study set out to assess the role of medical practitioners and patients as stakeholders to develop a secured access control system that can allow patients have access to their medical records online from anywhere they are.

The method employed shall be the survey method. Data collected from the questionnaire shall be presented with the aid of manual and electronic application such as the Statistical Packages for Social Sciences (SPSS), while the hypotheses would be tested using the T-test statistical method and linear regression method.

3.1.3 Study Population

The population of this research work will focus mainly on IT Staffs, Admin Staffs, Medical Doctors and Patients of Ahmadu Bello University Teaching Hospital, Zaria Kaduna State of Nigeria, 80 to 100 respondents will be selected.

3.1.4 Sampling Techniques and Procedures

Data for this project will be collected, using a non-probability sampling method. Here, the sampling selection is based on the subjective choice of the researcher as to which elements best provide desired basis and probability of good outcome.

3.1.5 Data Collection Methods

The sources of data for a research work is grouped into two, namely;

Primary sources

Secondary sources

Primary Data

Primary data is important for a research as the credibility and reliability of the research depend to the extent of the primary data used. There are different methods of primary collection which include surveys, observation and experiment. This research is planned to be conducted mainly on survey. Qualitative method approach will be use. The researcher will administer to collect the data from the target respondent. Questionnaire will be used as the main channel for primary data collection. The researcher will also use interview guide paper collect data from cloud users and cloud providers from various locations.

Secondary Data

This is the main data collection method, data will be collected in qualitative approach from different sources such as journals, periodic publications, newsletters, books, internet, organizational reports, pullouts and also the researchers' experience as a student of computing. These will help the researcher ascertain the weaknesses, challenges and study cases of Health Information Systems. Secondary data will be used to outline possible solution to improve access control in Health Information System using the appropriate simulation tool.

3.1.6 Data Collection Instruments

This data is collected through survey method. This data is original in nature. This data is collected by distributing the questionnaire & getting filled by the concerned respondents, for this purpose, online questionnaire as well as manual method will be used. Telephonic and/or personal interview conducted with the IT industry people, Medical Doctors and Patients of ABUTH.

3.1.7 Pre-TESTING (validity and reliability)

Validity refers to the degree with which a research instrument measures what it purports to measure as well as the population it is intended for. It refers to the truthfulness of the instrument and population of study. It implies that it should measure the characteristics it is intended to measure. The validity test used in this research is content (face) validity. Content validity is the extent to which the instrument measures the overall appearance and subject matter in line with the set of objectives of the study. In other words, the items set or statements made should reflect the purpose of the envisaged problem of the research study (objectives). Reliability on the other hand is the degree of stability of the measure of variables or research instruments. A test is said to be reliable if it measures the same variable at different times to the same set of respondents and results which are consistently similar. The test retest method involves measuring the reliability of the test twice to the same individual sample at different times. Thus the two scores obtained from the test are gathered together and correlated so as to determine the relationship that exist between the first test score and the retest score.

How to be it in ensuring that the validity of the research instrument is established, the content validity and construct validity were implemented such that the statement and questions were hypothetical in nature so that it measure exactly what it intends to measures. In establishing the reliability, the following will be implemented: The subscales will be designed with a 5-point like scale. (5 = strongly agree; 4 = agree; 3 = uncertain; 2 = disagree; 1 = strongly disagree) to determine users agreement with statement as regarding the test of the entire hypotheses. The scores will represent in each agreement in each statement.

3.1.8 Data Analysis

Data presentation gives a good description into the entire research work. It focuses on the statistical instruments used, since variables are involved in this research work, the data collected will be converted into normal or ordinal figures by the application of predetermined weighting on them. This is because data that are collected are presented in forms that would enable them to be easily analyzed in terms of interpretation. The method of presentation addresses how the data collected are disclosed to the public and presented to aid analysis

The researcher presented the data obtained via the questionnaire with the use of descriptive statistics comprising the sample percentage and tables, and pie chart presentation for adequate understanding of the data. The adoption of data presentation that will be used for this research work is the T-test method.

The data collected were sorted out into different categories of rows and columns, displaying facts and figures. For proper analysis however, only the data in direct relation with the hypothesis formulated were considered. Statistical Package for Social Sciences (SPSS) version 15.0 will be used in analyzing the data collected. This package was used to aid the analysis of the collected data for the study.

3.1.9 Measurement of Variables

Operationalization of the research topic is to identify the variables involved in this project that is the dependent variables and the independent variables. Therefore, these variables are classified into two namely: The dependent and the independent variable. Y is the dependent variable which has to do with the (effect), while X is the independent variable which has to do with (cause). In other words, X is the cause variable while Y is the effect variable. Therefore, to relate variables of this research topic; Health Information System is the cause, while access control is the effect of operationalization in this research.

3.1.9 Artefact Design

The objetive of this research after collecting necessary data from the case study is develop a secured access control system that will allow patients to have access to their medical record.

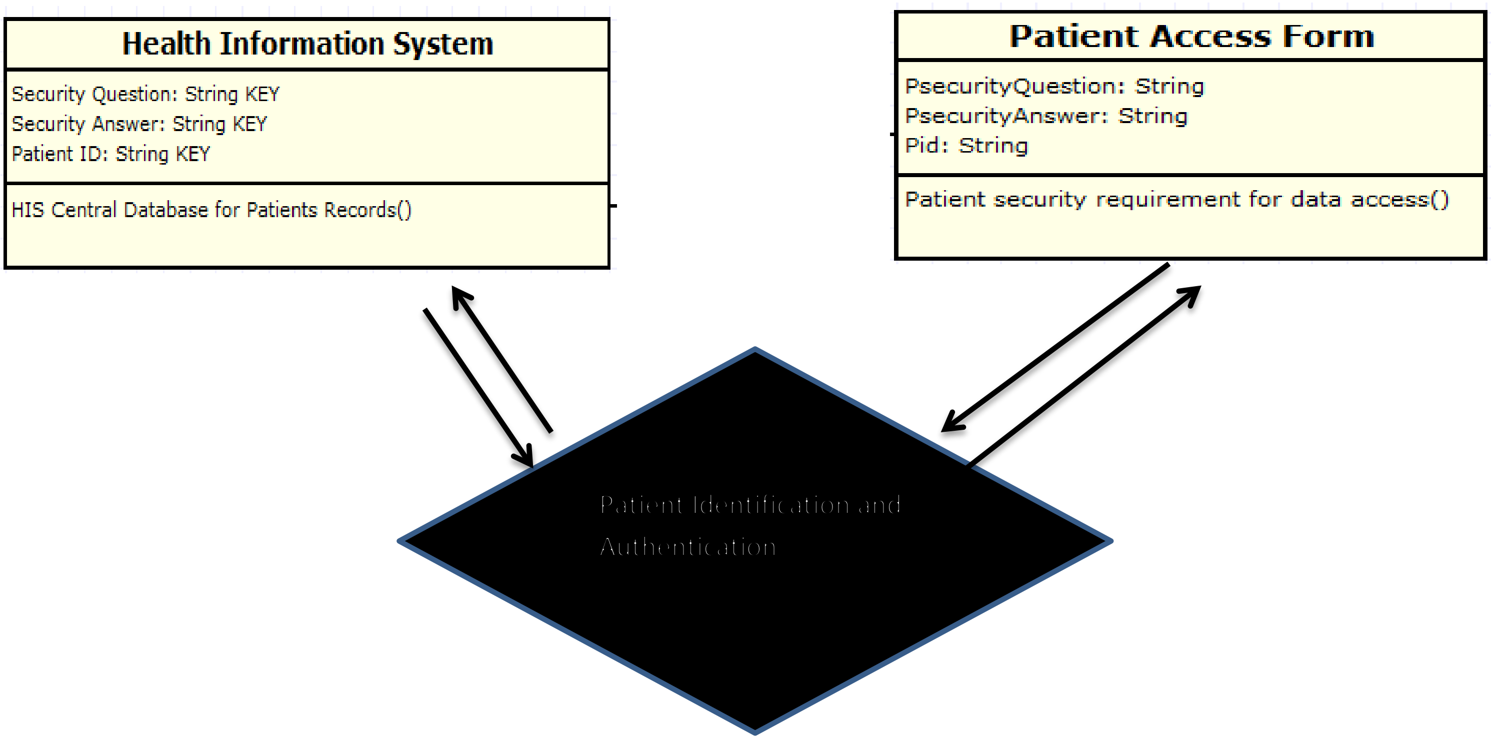

Health Information System
Security Question: String KEY
Security Answer: String KEY
Patient ID: String KEY
HIS Central Database for Patients Records()
Patient Access Form
PsecurityQuestion: String
PsecurityAnswer: String
Pid: String
Patient security requirement for data access()
Patient Identification and Authentication

Figure 6: HIS Access Control Model

Figure 6 above, shows how the extracted requirement will be used to develop the access control system. Health information system database contains all the necessary class and object required to house health records of patients. During the enrollment process, patient will be asked a security question and answer of which will securely save in the database. Patient ID with the security question and answer are the authentication parameters that a patient is expected to type for him or she will said be identified and authenticate for having access to medical record.

3.1.10 Conclusion

In conclusion, this chapter summarizes the various approaches researchers will use to achieve objectives of the study. Both quantitative and qualitative data analysis will be used since questionnaire and interview will be used to gather information from the selected respondents.

REFERENCES

RealUser. Retrieved September, 2016, from www.realuser.com.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] Biometric in e-health system.