USING ACCESS CONTROL TECHNOLOGY TO PROTECT HEALTH INFORMATION SYSTEM IN AHMADU BELLO UNIVERSITY TEACHING HOSPITAL (ABUTH), ZARIA

Muhammad Musa

Department of Computer Science, School of Applied Science
Nuhu Bamalli Polytechnic, Zaria.

ABSTRACT

Hospital is a system; whereby different stakeholders have to work together for achieving a common goal. Existing Health Information System of ABUTH was reviewed and necessary requirement was gathered. Access Control Gaps and other security related issues were identified as existing challenges to hospital health information systems. The review revealed how medical personnel from different departments, having different areas of expertise jointly work together in diagnosing and treating patients. Based on the interrelation existing between ABUTH medical staffs, a new System is proposed, which is Accessible using 2-Factor Authentication by five actors which include Doctors, Pharmacist, Laboratory Technologist, Patients and Admin staffs. For the patients, a booking Module is Designed whereby Patients have authorization to fill and submit their booking details online (i.e. the summary of their sickness complaint); this is to help the doctors have a clear view concerning patients sickness before coming to the hospital and will help them to make proper planning of attending patients daily. Online booking will also solve long queues in the hospital by patients. The system allows Doctors to see, approve and serve patients. For privacy of patient, the access control of the new system is developed in such that, only doctors can access and update patient records. Furthermore, the new system is developed to run on newer version of windows and on different devices such as computer system, tablet phones and other android phones.

Keywords: Health, information system, Hospital, Access control, ABUTH

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 (Ferreira, 2007). The main objective of this research is to review the existing system of health information system of Ahmadu Bello University Teaching Hospital Zaria Kaduna Nigeria and add a module that will guarantee access control using two factor authentications to patients and the authorized staffs of the hospital. 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.

Effective and efficient planning, monitoring & evaluation of health services depend on reliable data (Cohn, 2006). Health information system depends largely on reliable and secured data. 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." (Ciampa, 2009).

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.

BACKGROUND OF THE STUDY

Our hospitals both primary health care and general hospitals in Nigeria are almost being operated manually with very few numbers of them using computing in some of their activities while mainly recording some information concerning immunization using Microsoft excel application package.

We have primary health care hospitals which are under the control of local governments' area councils. These are the small hospitals that are taking care of small minor illness from the grassroots level such as routine immunization, malaria, etc. almost all our settlement areas have one or more primary health care clinic. They have their medical practitioners, laboratory technicians and other health workers. When patients visit those primary health care clinics, they have to follow due process for formal registration. File has to be open for taking all the diagnosis and treatment record for the patients.

Primary health care clinics normally refer the cases that are beyond their control to general hospitals. The general hospitals are under control of state governments. When a patient is referred to anyone these hospitals, they will first of all cross check the patient medical history collected from the primary health care clinics. From there they will have a clear view of the patient medical

history of which will highlight the general hospital on how to proceed with necessary medical actions.

Both the primary health care and general hospitals in Kaduna state Nigeria are being operated manually using paper and pen for registration and capturing of patient medical records. This is the reason why most a times file missing cases if giving problems to most of the patients.

STATEMENT OF THE PROBLEM

The research was carried out using Ahmadu Bello University Teaching Hospital (ABUTH) Zaria Kaduna State of Nigeria as a case study. ABUTH is giving training to medical students in different professions such as medicine, nursing, surgeon etc. Figure 2 shows the current interface of ABUTH health information system.

Ahmadu Bello University Teaching Hospital is one of the largest consultancy hospitals with many areas of expertise in medical profession attending hundreds of patients daily. Although the hospital has health information system which is called Made in Nigeria Primary Health Care and Hospital Information System (MINPHIS) a desktop application accessible using Locally LAN, but still there are a lot of activities that are manually being operated using paper, files and pen. Other loopholes of the existing are summarized in the following: -

Difficulties Registering and Searching for Patients Records

Patients are manually registered and access to their health records also is manual. This brings inconsistency, inefficiency and consumes a lot of time in searching and sharing health information within and outside hospital. Also, there are some important stakeholders whom their activities are not captured in the existing system, example patients. Patients are among the hospital stakeholders, hence it very significance to integrate the patient among users of the hospital management system. Some department of the hospital complained that the existing system did not capture some of their important activities.

Not User Friendly

With interaction from the users of the current system, in the questionnaire passed through them, it was on a report rate that the system is not user friendly to them. In so meaning that it doesn't simplicity in navigation for data, learnability for novice user in that it requires one to go through a training of almost one month learning and knowing how to operate it. This is a big problem that a lot of time is spent and also besides other expenses during the training period. Therefore, this is a cost to the hospital all that time the user / stakeholder delivering nothing but only learning. Therefore, as a result from this, there is poor usability.

The Current System Does Not Support the Latest Operating Systems

The system operates only and only on windows 97 and below. This is a very big limitation when it comes to updates to currently existing windows, that it cannot be installed on such windows say Windows 2008, windows 7, Windows 8, windows 8.1, windows 10. Therefore, access control is a big problem.

Few Stake Holders Take Part

In terms of access control, the current system gives no room and for real hospital stake holders to take part of it as by their activities to be played. In real life we that there is a quite a number of stakeholders that should be participating in the user of

any hospital system ans such user could be : Patient (Cause the hospital cannot work without them), Doctors (we see these participating in cases of Diagnosing patient in so interacting with the patient so as to identify their problem), laboratory attendant (For any serious hospital, most patient should go through testing to professional determine what the patient may be suffering from and then give the appropriate treatment as by the international classification of disease from the test) and we also see the Administrators on the top of other stakeholder using the system for generating compulsion report for use in cases of decision making and as fact for hospital improvements.

No Mobile Support & No Global Access / Distributed Access

The current system does not serve the feature of Distributed access control by different user s remotely. In summary the system operates on a local area network (LAN). Of which this comes with its problems of cable plugin off at times which means there are disconnections. So, for the proposed system, these issues are addressed with the use of with an alternative of a Global accessed system with so enabling all the stake holders play their part from whenever they can be and remain accessing the service. This will be of a good advantage in a way that as by the current growing user of mobile Smartphones, user will not only need to access the system through desktop computers as it's the case with the existing system but will be able to do whatever they need to do with any of the device say Smartphone, Tablets, Laptops, Desktops. This will bring in efficiency and reliability to the services provided by the Hospital.

Access Control Weakness

Another problem with the current system is the Data / information security. It so meaning since all users regardless of the levels of operation they see everything it be in the boundary or not. For example, the Pharmacist sees all the work done by the doctor and can also do all the work as it should be done by the lab attendant or Patient. This is an implication that the system does not support data integrity and hence lead to user shying away from using it.

One user at a time

They current system can only be accessed by one user at a time, as the doctors login into the system only him / her can do work with it meaning the rest of the other Hospital Stake holders say the Pharmacist, Laboratory attendant, Administrator cannot make use of it until that one user is doe with all his works and then one of the other pending user can also get access and also takes his time as the other do wait for him to finish. In brief with this also a lot of time is spent by the user with the system hence making patient wait for so long which all in turn brings about inefficient.

The System is Very Slow

The current automated system is very slow and does not correspond to the automated needs of the current generation, because it takes a very long time before one can generate medical report. Hence, the system has to therefore be overhauled based on these current findings.

The Challenge of current ABUTH Health information System is that it's hardly used due to poor access control features, Not user friendly, does not support the latest Operating systems, few stake holders take part, no mobile support & no global access / distributed access, use by one user at a time

and the system is very slow. From that point of access control, since all the Hospital service starts with the patient, it's of a notice that there are long queues by patients in hospital at the time of registering new patient therefore it's unfortunate that a number of them loose lives just due to the delay in the registration process. And not only that but the process also involves corruption whereby only those who can give in some token to those registering can be attended to first before others, even if one come before the other. This brings about inequalities among patients and a poor service delivery image to the hospital. And finally, the worst part of it, there is poor follow-up of patient records right from the registration until after treatment is given out due to Lack of proper collaboration among hospital stakeholders yet their work is interrelated all due to access control and file system storage.

OBJECTIVES OF THE STUDY

General Objectives

To develop a web-based health information system whereby stakeholders (e.g Patients, Doctors, Nurses, Pharmacist, Laboratory technologist and hospital management) can conveniently interact with the system securely using 2-factor authentication such that to have full control over the access of patient health records and improve on the weakness of current.

Specific Objectives of the Study

The Specific Objectives of this research are as follows: -

1. To analyse the existing health information system of ABUTH and gather necessary requirement for developing a new compatible system that will allow health workers and patients have interactive access to medical records remotely.
2. To develop a system that will support 2-factor authentication for validating and authorizing stakeholders in order to access the health information system based on their levels (i.e. Patient, Doctor, Pharmacist, Laboratory Technologist and Admin). This is to ensure that users only access information he or she is supposed to view or access.
3. To test the new system to ensure that access control module and other functional requirements of the new system are working for having a bug free application software.

PURPOSE OF THE STUDY

The purpose of this study is to review the existing health information system of ABUTH and develop a new system that will support the implementation of access control using two-factor authentication and authorization of users (Patients, Doctors, Pharmacist, Lab technologist and admin staff). The purpose also is not just about designing the system, but also to put more effort and emphasis on applying access control to make sure that privacy and confidentiality of patients' medical records are maintained.

RESEARCH QUESTION

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

1. What are the requirements needed for a patient to be registered with the Ahmadu Bello University Teaching Hospital (ABUTH)?
2. What are the security requirements needed before users can have access to health information system?
3. What are the kinds of information that are allowed to be accessible by the users (e.g. Patients)?

4. What are the limitations of users in terms of authorization perspectives to update or delete patients' medical records?
5. What are the hardware and software requirement to develop and implement the new system?
6. What are the requirements of two factor authentication system?

SIGNIFICANCE OF THE STUDY

This research is significance to health industries in the sense that, electronic exchange of clinical information allows doctors, nurses, pharmacists, other health care providers, and patients to access and securely share a patient's vital medical information electronically. The new system improved the speed, quality, safety, coordination, and cost of patient care most especially in quick retrieval of patients' medical record. Provided below are the significant of the study per stakeholder involved:

To the Patient

- Since the new system will replace the old registration process of new coming patient, then patient will no longer spend time waiting up in queues.
- Quick attention will be given to every patient who attends to the hospital since every patient will be aware of the doctor to meet even before they come to the hospital and which also applies to the doctor too. i.e. by time and section (Morning, afternoon or evening) of meet.
- Each Patient will have a sure remote access to his medical records which can be of a referential use for him in case of any sickness happens on him.

To the Doctor

- Every Doctor will be able to know the exact number of patient he/she attended per day since the system keeps track of which doctor served which patient and at what time.
- On submitting of the patients complain/booking, the medical doctor will have a clear view of the patients' sickness even before the patient comes to the hospital.
- Since the doctor has many bookings done by different patients, doctor has room to determine which patient to work on first based on urgency of the complaint addressed.
- There will be proper allocation of patient to rooms by doctors.

To the Laboratory attendant

- The system will make the work for laboratory attendant small and clear since all the tests they have to carry out are prescribed by the doctors in a precise and concise manner.
- The system will bring about specialization of laboratory attendant just specific to their task than carrying out Diagnosis as Doctors and also carrying out testing as it's the case now.

To the Pharmacist

- Pharmacist will be able to know which drugs are more taken / given out and then ensure that they are in stock in so curbing the shortage for drugs in hospital.
- The system control unauthorised given out of drugs by pharmacist without doctors' prescription.

To the Administrator

- The system gives administrators' room to evaluate the work done by each Doctor, Laboratory attendant and Pharmacist just on a click.

- The system will help administrators to make decision on time based on the reports generated.
- Administrator will be able to know how many patients registered with the system with reference to the number of pins bought.

To the Hospital

- The effectiveness of the system in solving the addressed problems, will give a Strong reputation to the hospital in compulsion to other hospitals.

To the technology industry

- The system fulfilment is to addressed problems that will give strong significant to the ICT / Development team for providing a problem-solving solution for such an institution.

METHODOLOGY

A review of the existing system of authentication was done using secondary data. The existing Health Information System of ABUTH was looked at and the necessary information collected and analyzed using the contents. Access Control Gaps and other security related issues were identified as existing challenges to hospital health information systems.

THEORETICAL REVIEW

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 Human Computer Interactions (including a massive 315 references), we refer to Iachello and Hong (Pedersen, 2010).

REVIEW OF DIFFERENT AUTHENTICATION METHODS

Different authentication methods currently employed on the Web have been briefly outlined (Pedersen, 2010). 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 shortterm 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 trade-off 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)**.**

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.

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 recallbased 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. Song (1999), proposed a graphical authentication scheme based on Hash Visualization technique. 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 number 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.

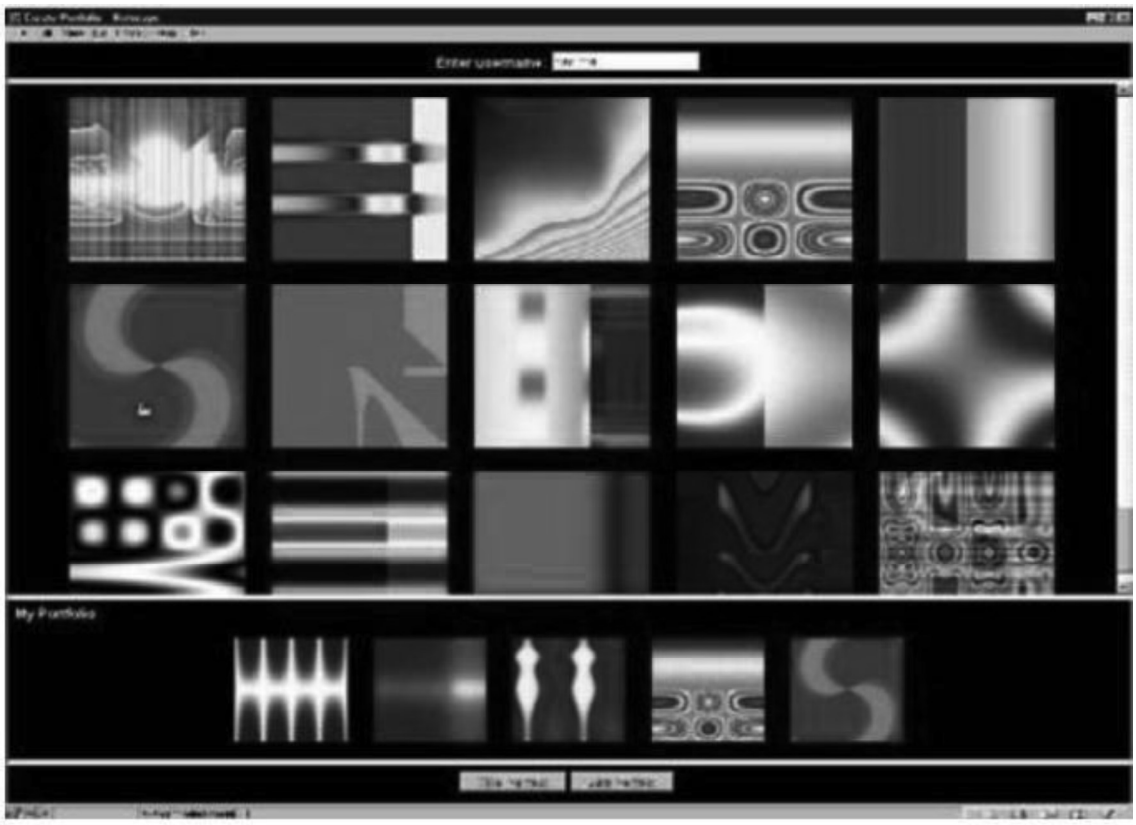

Figure 1: Dhamija and Perrig [11] used random art

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.

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 user's future password. A user is said to be authenticated if he successfully chooses the correct 4 images correctly. The techniques are 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 2.

Weakness of pass face authentication

According to comparative study carried out by (Sasse, 2000) identified that, passface (as shown in Figure 3) 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 2: Example of Passfaces

Biometric authentication

Okoh, (2015) Biometric is the science or technology trends that identity of an individual based on the physical, chemical or behavioural attribute of the person. Hence, biometric is the science of identification or authentication of individual using physiological or behavioural 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. ***Enrolment Phase: -*** Enrolment is the process of identifying an individual based on their physical or biometric trails. During the enrolment 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 Enrol (FTE)

CONCLUSION

Different authentication methods currently employed on the Web have been briefly outlined (Pedersen, 2010). We presented seven common methods of authentication and discuss their advantages and disadvantages in terms of both security and various points of interest concerning usability factors which include password authentication, 2-factor authentication, graphical authentication, recognition-based authentication, pass faces authentication and biometric authentication.

The research chose two-factor authentication, and decide to improve on it using what you have (i.e Asking for a user name and password) and what you know (i.e allowing a user to type his security code). 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 username/password and security codes are encrypted using triple step encryption (SH1, MD5 and salt) hence nobody can accesse the system unless he or she has three keys (User name, Password and security codes). In case there is security suspicion, an administrator has right to alter the salt value and everyone will be paused to have access to the again until when the matter is resolved.

REFERENCES

Adrian P. and Rachna D. (2000). A User Study Using Images for Authentication. *UNISEX Security Symposium*. University of California Berkeley.

Ahmadu Bello University Teaching Hospital website. Retrieved 2016 at www.abuth.org.ng.

Anders B.P. (2010). *Usability of Authentication in web application – a literature review.*

Asoke K. T. (2008). *Architecting Secure Software Systems*, online at UTAMU e-learning.

Biederman, I. (1973). Searching for object in real world sense. *Journal of Experimental Psycology,* **1**, 22-27.

Chuck E. (2011). Computer Security Fundamentals, Second Edition, e-Book, UTAMU e-learning.

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

Cohn, S. (2006). Privacy and Confidentiality in the National wide Health Information Network, *MSc Thesis*.

David A. G. (2002). *Theory and Problems of SOFTWARE ENGINEERING*, First Edition, e-Book, UTAMU e-learning.

David K., Sasikanth A. and Amit B. (2009). A Privacy Frame work for Mobile Health and Home Care Systems. *Presented at First ACM workshop on security and privacy in medical and home care systems*, Chikago Illinois, USA

Devisetty V. (2004). Image Based Registration and Authentication System. *Midwest Instruction and Computing Symposium*.

Ferreira, A. (2007). *Access Control: how can it improve?* Computer Laboratory, University of Kent, Center for research in health information Systems and technologies; 127,65-76.

Ferreira A. M. (2010). Modelling Access Control for Healthcare Information Systems, *PhD in Computer Science* University of Kentucky

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

Joel Howard. (2012). Analysis and Enforcement of Web Application Security Policies. Doctor of Philosophy, University of California.

Lillian R., (2009). Access Control in Healthcare Information Systems. *Thesis for the degree of Philosophiae Doctor (PhD), Norwegian University of Science and Technology Faculty of Information Technology.*

Mahnaz S. and Zahra G. (2015). Managing the Security of Nursing Data in the Electronic Health Record. *Acta Inform Med*.

Motahera S. (2013). *An Access Control Model for NoSQL Databases*, Graduate Program in Computer

Science, The University of Western Ontario.

Okoh, E. (2015). *Biometric Solution in e-Health Security.* Degree of Master of Science Information Security.

Ryan S. (2015). Authorized Access and the Challenges of Health Information Systems, *Degree of Master of Science in Computing Security*, Rochester Institute of Technology, Rochester, New York.

Sacha B. and M. Angela Sasse, (2000). Are Passface more Usable than Password? *A Field Trail Invesitigation*. Department of Computer Science, University College London

Sergio V. S., (2015). A Study of Access Control for Electronic Health Records, Degree of Master of Science, Governors State University.

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.*

Trondheim, A. (2009). Access Control in Healthcare Information Systems, *PhD Thesis*, Norwegian University of Science and Technology, Faculty of Information Technology January.

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