American Journal of Advanced Research, 2017, 1–1
Sept. 2017, pages 13-18
doi: 10.5281/zenodo.910819
http://www.ibii-us.org/Journals/AJAR/
ISBN 2572-8849 (Online), 2572-8830 (Print)

Design and Implementation of a Computer Based Test Centre Using Biometric for Authentication

O. Omorogiuwa[1, *] and F. N. Nwukor[2]

[1]Department of Electrical and Electronic Engineering, Ambrose Alli University, Ekpoma, Nigeria., [2]Department of Electrical and Electronic Engineering, Petroleum Training Institute, Effurun, Nigeria.

*Email: owenseme@yahoo.com

Received on May 12, 2017; revised on Sept 20,2017; published on Sept 21, 2017

Abstract

The aim of this study is to develop a web-based computer centre using biometric finger print for verification/authentication and tie the MAC adders of all the system to the program server, tie the computers with the sever through quantum mechanics distribution (QKD) for the intranet only, to prevent intruders via intranet; building a system that will not be compromised and with desired confidence. Visual Studio was utilized to develop the Front-end aspect of the Computer Based Test (CBT) authentication software while Visual Basic.NET was applied to develop the software. The Backend was designed using MySQL server application, thus all the data for the CBT authentication software are stored in the MySQL database. During processing, records are retrieved from the database and displayed in the Front end. The performance under test was found to be satisfactory when comparing Manual verification/authentication (average 6.6sec) to Biometric verification/authentication (average 1sec). All unauthorized users are blocked and appropriate warning messages sent to the client by the server when they initiate Login procedure. This eliminates external access from unauthorized persons sitting for the examinations. All systems can see the network Identification, but not all persons have access right to the examination.

Keywords: Biometric, Finger print, MAC (Media Access Control) Address, CBT (Computer Based Test), IP (Internet Protocol), Database

1 Introduction

Computer based centre (CBC) is the connection of computers to a designated server through a switch or an array of switches for conducting of computer based examinations. For a CBC to be operational the computers must be able to communicate with the server in real time, as such system security will be required to protect the integrity of the system. In a CBC system, we have the hardware and software. The hardware includes the computers, switch, cable connectors, servers etc. The software represents the program that runs on the systems, enabling the user and the system to communicate. There have been many security systems that are tied to user interface. CBC, for example has a one-way authentication/verification, two-way authentication/verification and an IP authentication/verification, but with this authentication/verification there is still intruder in the system. In this paper we will be using IP/MAC for surveillance and Biometric fingerprint for authentication/verification which will be tied to the CBT.

Examination is one of the best methods of evaluating the knowledge and ability of an individual (Adebayo and Abdulhamid, 2014). Its purpose is to assess how much each student has learned compared to fellow students in the same course or learning situation. Various examination methods are being used in higher education institutions to assess academic progress, such as paper-pencil-based examinations, assignments, presentations etc. With the increasing rate of examination malpractices in the educational sectors the school management deserve to inculcate a tight security means to ensure that these activities of examination impersonators are reduced. The activities of these examination impersonators have harmed the educational sector greatly (Luecht, 2005a; 2005b). With the recent advancement in Information and Communications Technology (ICT), there are some drawbacks that can affect computer based centres with hackers always looking for loopholes in how examinations are conducted. Several approaches (Todorov, 2007) for security have been adopted by various individuals and institutions, such as one-way authentication and two-way authentication systems, and IP address for authentication (Ahmad and Abu, 2013; Saliu *et al*., 2013; Nafiu, 2014). A major drawback with the use of IP address on a system/network is that, it can be changed by hackers and this can compromise the security of a network system there by encouraging malpractice (Beaver, 2013). Other well-known security methods are firewalls, pass-wording, mathematical algorithms of encryption and decryption scheme.

Copyright © 2017 by authors and IBII. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

The goal of this paper is to develop a computer based centre using biometric finger print for verification/authentication and tie the MAC adders of all the system to the program server for the intranet/internet, to prevent intruders via intranet/internet while building a system that will not be compromised and with desired confidence. The proposed system will use finger print biometrics. This would help ensure that only registered student during registration with their finger print are allowed into the examination hall, start examination and submit examination. The system without registered MAC adders on the server cannot be used for the examination, a scenario where you are your own access key to your examination. As one enables his/her examination it registers as attendance signed and as you submit using biometric you also sign out the attendance, this could seem very convenient.

The developed system would contribute in preventing malpractices in the educational sector. Impersonation which has eaten the educational system, thereby encouraging laziness among students would be eliminated and standard of student educational performance would be increased. Up till now the JAMB UTME, does not encourage the use of fingerprint as mode of authentication, this has resulted in people sitting for examinations for others. With the adoption of fingerprint, irregularities will be eliminated as fingerprint authentication will also be employed during collection of results and certificates. Nevertheless, for some people, the use of fingerprint technology is very intrusive, because is still related to criminal identification. Moreover, there can be inherent errors in the system with the dryness (or dirty) of the finger's skin, as well as with the degradation due to aging. In addition, a fingerprint can be copied and used by hacker. Table 1 shows a comparison of other biometric options that can also be used. In general, most persons prefer to use finger print biometric than other biometric like iris and retinal scan because of the talk of the risk that it may affect the human eyes.

Table 1. Comparison of different biometric technology

Biometric technology	Accuracy	Cost	Devices required	Social acceptability
Iris recognition	High	High	Camera	Low
Retinal scan	High	High	Camera	Low
Finger print	High	medium	Scanner	Medium

2 Methods

The user is enrolled into the system using biometric and the enrolment is tied to the CBC program platform, this is stored as a template on the database. When a user attempts to enter the examinations platform, a biometric program will pop up for the user to put his finger on the scanner for verification/authentication and the main features of the object scanned are then extracted and converted into a digital representation. This file is then compared to the templates on the database. If a match is found, the user is granted access to the examination platform.

For this to be achieved, the front-end aspect of the CBT authentication software is designed with Visual Studio. The language used to develop the software is Visual Basic.NET. The backend is designed with MySQL server application, which is easy-to-use database software. All the data for the CBT authentication software are stored in the MySQL database. Then records are retrieved from the database and displayed in the front end. A connector called mysql connector is installed in the computer system to provide a way for the visual basic.net codes to be able to access the data stored in the database. The connector provides access to the tables and records and they are copied to the computer memory.

2.1 Finger Print Technique (http://www.androidauthority.com/how-fingerprint-scanners-work-670934/)

The minutiae extraction technique implemented is based on the widely employed Crossing Number method. For the image post-processing stage I implemented the minutiae validation algorithm. The fingerprint scanner that was use is capacitive scanners**,** as capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. The charge stored in the capacitor was changed slightly when a finger's ridge is placed over the conductive plates. An op-amp integrator circuit was used to track these changes, which was then recorded by an analogue-to-digital converter. Figures 1 shows the circuit diagram of the theory and architecture behind a capacitive fingerprint scanning chip while Figure 2 shows the flowchart of biometric finger print design.

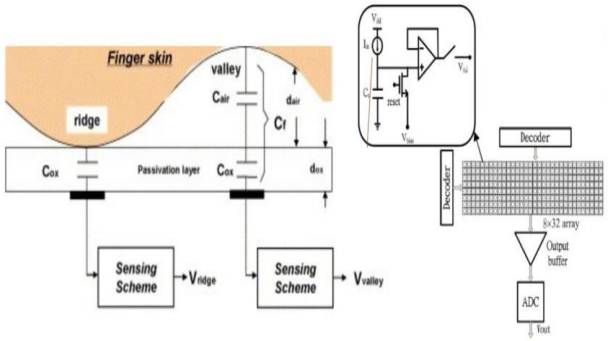

Fig. 1. The theory and architecture behind a capacitive fingerprint scanning chip

2.2 Enrolment / Verification of the Biometric System

This section shows the sequence of Biometric Encryption algorithm as illustrated in Figures 3 – 7.

3 Test, Results and Discussion

3.1 Testing and Evaluation

The model is evaluated using the fingerprint verification/authentication to start examination and to submit examination during the examination period and a series of experiments were performed focusing on the effectiveness, speed and its usability. The usability testing technique is a technique for ensuring that the intended users of the system can carry out the intended task efficiently, with a limited time.

3.1.1 Test for Enrolment Time

The program was tested using 10 different persons; 5 boys and 5 girls, the time it takes for one person fall between 17sec to 35sec, average of 25.4sec per person, as shown in Table 2.

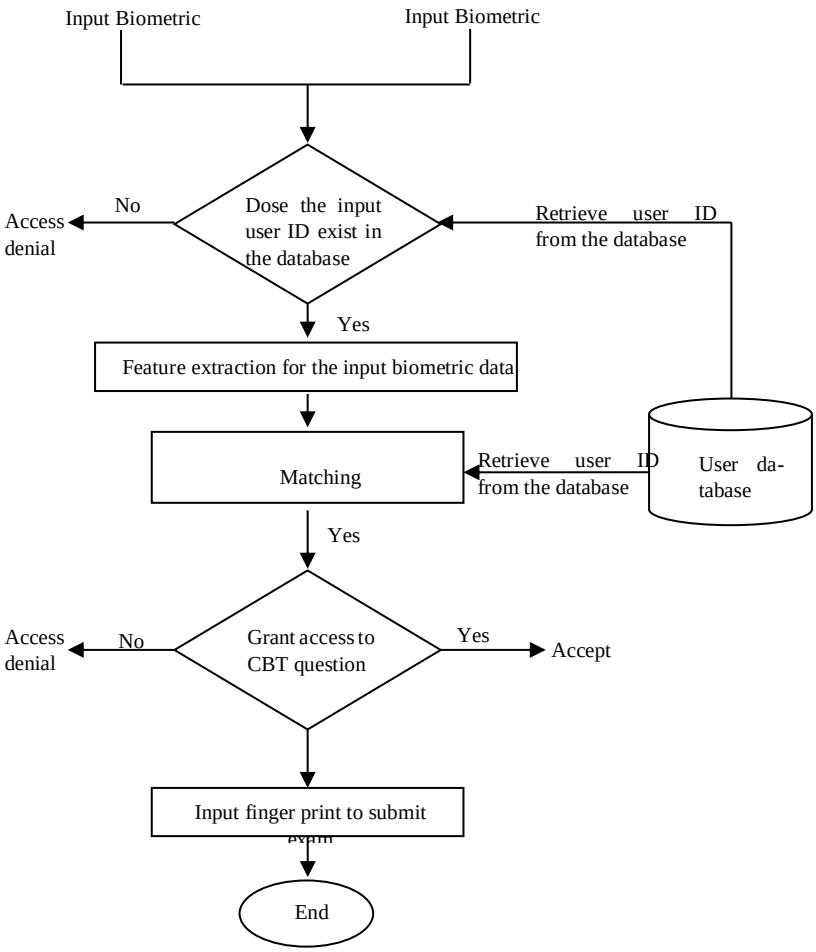

Fig. 2. Flowchart of biometric finger print design

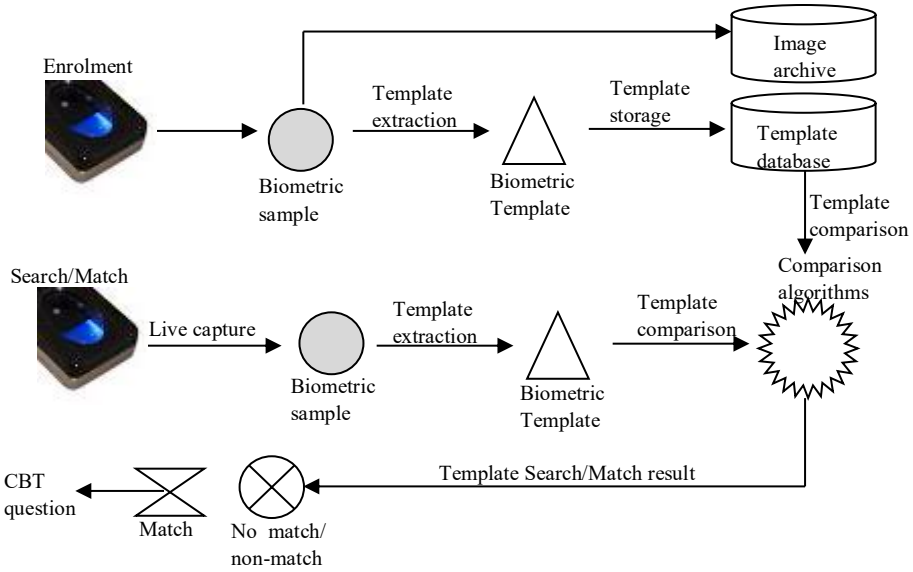

Fig. 3. Overview of the enrolment/verification process for Biometric fingerprint connecting to CBT

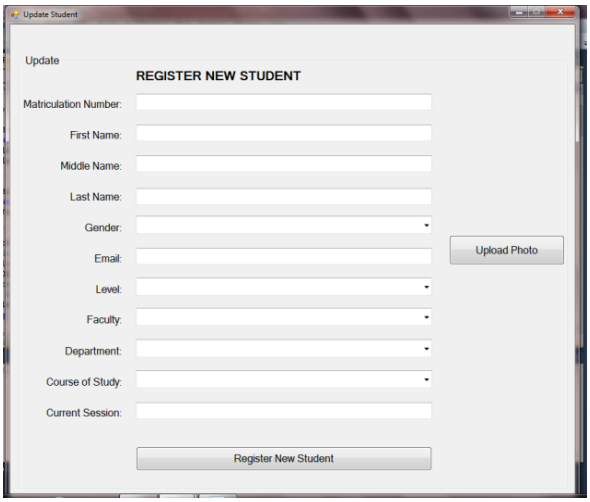

Fig. 4. Biometric fingerprint enrolment for new user sample

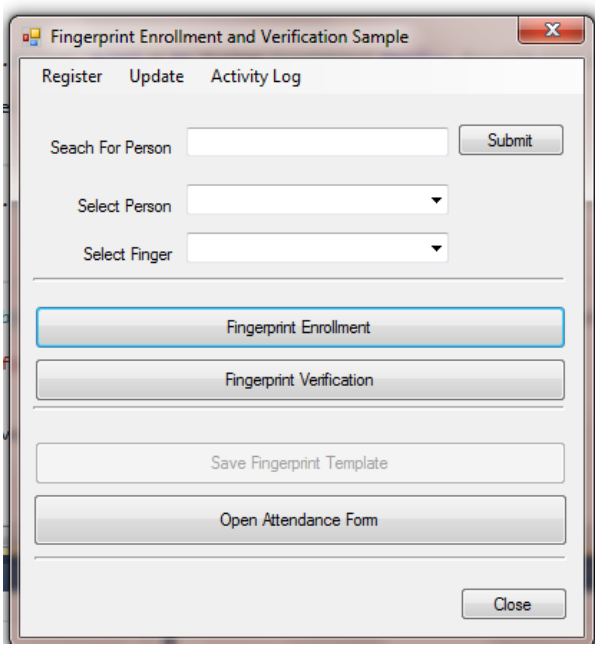

Fig. 5. Biometric fingerprint enrolment/ verification sample

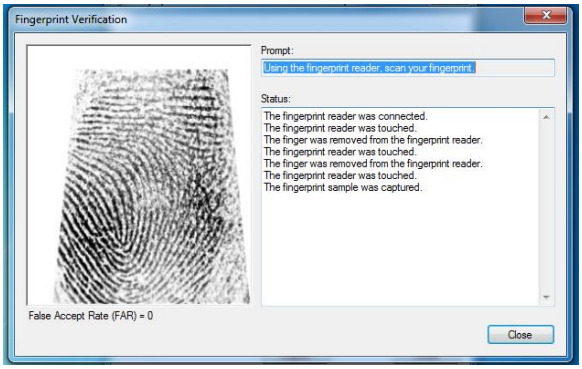

Fig. 6. Biometric fingerprint verification sample

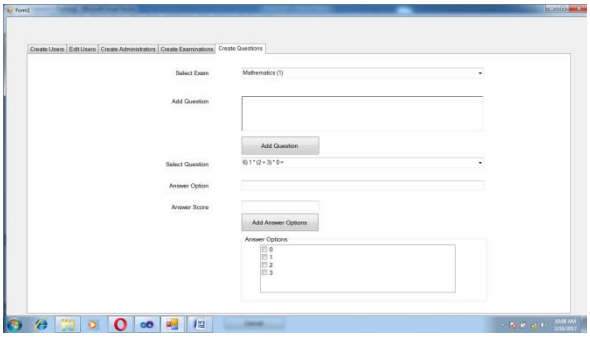

Fig. 7. Computer based test sample

3.1.2 Speed of Verification and Authentication

This test was used to measure the average time it takes to verify/authenticate students' manual with biometric and attendance signature with biometric signature, Table 3 shows the result of manual (average 6.6sec)/biometric verification and authentication (average 1sec) and manual signature (average 11.4sec), one will note that for biometric signature will be generated from the program.

Table 2. Time taken for student to enrol in biometric

Sample	Time Taken (sec)
Joy Osaretin	17
Blessing Agho	20
Abohwoyere Omokhua	33
Osatohawmen Osamuyi	34
Amarachukwu Anajemba	35
Vivian Anokwuru	26
Denoraah Zainab	20
Ashonofor Wilson	24
Chigozie Ebito	21
Eguavoen Iziegbe	24
Total	254
Total Average	25.4

Table 3. Manual/biometric verification and authentication

Sample	Manual verification/ authentication (sec)	Manual nature (sec)	Biometric Sig-verification/ authentication (sec)
Joy Osaretin	7	6	1
Blessing Agho	5	15	1
Abohwoyere Omokhua	5	7	1
Osatohawmen Osamuyi	9	10	1
Amarachukwu Anajemba	8	17	1
Vivian Anokwuru	4	13	1
Denoraah Zainab	9	11	1
Ashonofor Wilson	6	8	1
Chigozie Ebito	10	13	1
Eguavoen Iziegbe	3	14	1
Total Time	66	114	10
Average Time	6.6	11.4c	1

3.1.3 Test of Two-way Authentication with Biometric Authentication

Table 4 shows the time it takes to type in the username and the password in the two-way authentication (average 15.2sec) and the Biometric authentication (average 1sec).

Table 4. Result of Two-way Authentication with Biometric Authentication

Sample	Two-way authentication (sec)	Biometric authentication (sec)
Joy Osaretin	11	1
Blessing Agho	12	1
Abohwoyere Omokhua	18	1
Osatohawmen Osamuyi	18	1
Amarachukwu Anajemba	19	1
Vivian Anokwuru	14	1
Denoraah Zainab	14	1
Ashonofor Wilson	16	1
Chigozie Ebito	13	1
Eguavoen Iziegbe	17	1
Total Time	152	10
Average Time	15.2	1

3.2 Test of program to general requirements

The software developed was also tested and evaluated based on the following criteria;

(1) Ease of Enrolment.

(2) Fast to verify/authenticate.

(3) Adherence to Verification Rules for Examination eligibility.

(4) Fast communication between systems to server

The software was found to satisfy the above criteria given the following observations:

(1) The developed system also ensures that only students who are to sit for exams are allowed access into the examination platform.

(2) It was observed using star connection for the network (LAN) is the best, when one system goes down other will be working.

(3) Student and course attendance report are available to the system administrator, it can be concluded that the developed system effectively addresses the needs of CBC removing malpractice from academic environment with regards to exams and student attendance. The system respond time was 1ms during system to server communication and less then 2ms during authentication; efficiency, and reliability at real time was very good.

4 Conclusion

Security is ongoing process where due care and diligence to protect examination need to be put in place, without security in network systems, most system will be highly exposed to a lot of dangers and threats. Different information technologists have developed several tools, design phases and other techniques to help in the development of standard computer based centre. Most of the technologist had not looked into biometric for authentication and MAC address System. One can recall that why one needs security in the examination to eliminate organised malpractice, a summary of comparison of biometrics is shown in Table 2 Managing the speed of manual verification and authentication with the biometric verification and authentication. The lapses recorded in traditional methods of recording and managing attendance has also be solve by generating attendance from the develop system, to ensure the integrity of such records; biometrics is a tool that cannot be neglected. Fingerprint authentication has thus been tested and proven as a veritable tool in achieving the much needed automation. The result shows that the average time taken per student using biometric and manual verification/authentication register are 1 and 6.6 seconds respectively.

The major strength of the developed system lies in its high scalability and flexibility, by careful examination, it can be inferred that biometric authentication could not only speed up the process of taking exams, attendance but reduce the error rate and produce faster verification/authentication process of student verification/authentication policy required for writing examination in a campus environment. This paper presented a simplified, low cost fingerprint based system solution to the management eliminating malpractice/irregularity in examination. However, it might also be necessary to investigate student through hybridized biometric features like face and iris for better performance.

5 Recommendation

It is highly recommended that the management of Universities take examination/irregularities issues seriously. Biometric verification/authentication promises to provide the global solution with a sound identity management system, which could eliminate malpractice from the University. If biometric security measure is not strictly adhered to in examination in the University and other places for signing in/out, it could pave way for malicious intruders to have access to the University. If examinations are not properly secured and falls into the wrong hands, it could spell doom for such a University. In addition, if security measures are not strictly adhered to, these could pave way for hackers and malicious intruders to have access to examinations.

Conflict of Interest: none declared.

References

Adam Mohammed Saliu, Mohammed Idris Kolo, Mohammed Kudu Muhammad, Lukman Abiodun Nafiu, (2013): 1(1) Internet authentication and billing (hotspot) system using MikroTik router operating system, *Int'l J. of Wireless Communications and Mobile Computing*: pp 51-57.

Adebayo O. and Abdulhamid, S. M. (2014): E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity. *Int'l J. of the Computer, the Internet and Management*, pp 12,18,1-47.

Beaver Kevin. "Hacking for Dummies®," 4th Edition 2013 by John Wiley & Sons, Inc., Hoboken, New Jersey. Pp 4, 9-13, 27-37, 81-154.

http://www.androidauthority.com/how-fingerprint-scanners-work-670934/

http://www.wisdom24x7.com/

Itakura, Y., Tsujii, S. (2005). Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures. *Int'l J. of Information Security*. Heidelberg (4)4, 288

Layton Timothy P. (2007): Information security design, implementation, measurement, and compliance Boca Raton, FL: Auerbach publications. pp 8-13, 40, 62, 68,92, 112.

Luecht, R. M. (2005a). Operational issues in computer-based testing. In D. Bartrum and R. Hambleton (Eds.), Computer-based testing and the Internet. New York: Wiley & Sons Publishing.

Luecht, R. M. (2005b). Some useful cost-benefit criteria for evaluating computer-based test delivery models and systems. *Association of Test Publishers Journal*. Retrieved from www.testpublishers.org/journal.htm Foster, D. (April, 2011). Personal communication.

Nafiu, L. A. (2014): Unpublished Lecture Notes on Net- Centric Computing. Federal University of Technology, Minna, Nigeria.

Thomas Robertazzi. (2012): "Ethernet", Basics of Computer Networking, pp 1-129.

Todorov**,** (2007): "Authenticating Access to Services and Applications", Mechanics of User Identification and Authentication Fundamentals of Identity Management, pp 760.