Nigerian Journal of Technology
Vol. 40, No. 2, 2021, 2021, pp. 284–291.
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
http://dx.doi.org/10.4314/njt.v40i2.14

Implementing Fingerprint Authentication in Computer-Based Tests

A. E. Evwiekpaefe[a,*], V. O. Eyinla[b]

[a]*Department of Computer Science, Nigerian Defence Academy, Kaduna State, NIGERIA.*
[b]*Center for Information and Communication Technology, Air Force Institute of Technology, Kaduna State, NIGERIA.*

Abstract

The use of computers to conduct examinations is more effective than traditional paper-based examinations in terms of immediate availability of results and long term cost effectiveness. This however is faced with identifying and authenticating the real identities of the examinees so as to reduce impersonation. The study examined the existing authentication method available on the Computer-based test system of Air Force Institute of Technology (AFIT), Kaduna, Nigeria and proposed the fingerprint biometric technique as an additional method to authenticate the examinees. The fingerprint biometric authentication was developed using FlexCode SDK and implemented on DigitalPersona 4500 fingerprint reader – the recommended scanner by JAMB for fingerprint enrollment. The system was developed using PHP scripting language on XAMPP local server and MySQL database system. The results obtained showed that there is no need for a middleware to link the authentication module with the CBT because of the Single Sign-On technique implemented. This result thus improved the level of authentication and access to the CBT. This will therefore reduce impersonation and increase the level of awareness of CBT by academic stakeholders.

Keywords: authentication, biometrics, computer-based tests, fingerprint, impersonation

1. INTRODUCTION

The evolution of new technologies has drastically changed the mode of learning and assessment of students' performance. This does not exclude the practice of selection of candidates for matriculation into any Nigerian tertiary institution by the Joint Admissions and Matriculations Board (JAMB). Before the year 2015, the conduct of admission selection examinations called Unified Tertiary Matriculation Examination (UTME) was paper-based. The former registrar of JAMB, Prof. Dibu Ojerinde, itemized some reasons behind the proposal of Computer-based Tests (CBT) for the conduct of the examination [1]. These include security challenges, high cost of transporting the examination materials and curbing examination malpractices among the examinees.

CBT has a number of important advantages compared to traditional paper-based tests (PBT) such as efficiency, immediate scoring and feedback in the case of multiple-choice question tests [2]. Also, e-examination can improve the standard of student's examination whereas the conventional examination system using the pen and paper requires more effort on the part of students and invigilators [3].

Despite these advantages, CBT is not without its own challenges. Ensuring that examinees do not search computer directories or surf online to get answers is a challenge. In addition, guaranteeing that examinees do not engage in examination impersonation is almost impossible. Again, since the inception of e-learning, there has been a security breach as it poses various threats especially when exams are held electronically (online). Security is one of the challenges of both traditional and online-based examination systems. One way to mitigate security breach during online examination is to identify, authenticate and monitor candidates during online examination [3].

There is therefore the need to uniquely identify examinees in the course of examination undertaken. Over the decades, biometrics especially the fingerprint biometrics has been used to successfully identify and verify the unique identity of individuals. However, the successful application of the fingerprint biometrics with CBT in Nigerian higher institutions has limited use. This study therefore is aimed at minimizing the chances of examinees engaging in examination impersonation by implementing a biometric based authentication system that validates the authenticity of the examinees during CBT examination in AFIT. The study shall also implement a single sign-on technique to eliminate the need for a middleware.

[*] Corresponding author (**Tel:** +234 (0)803 560 0524)
Email addresses: aeevwiekpaefe@nda.edu.ng (A. E. Evwiekpaefe), v.eyinla@afit.edu.ng (V. O. Eyinla)

2. REVIEW OF RELATED WORK

Ajinaja [4] focused on using Component-Based software model in the development of a Computer based Test software. The CBT was developed using both the widely accepted Waterfall Model and Reuse-oriented software process models. The whole implementation of the software was achieved using Source Based technologies such as XAMP server, PHP, MySQL, JavaScript, Hypertext Markup Language and Cascading Style Sheet as template design.

Khlifi et al [5] observed that the main challenge facing the security of e-assessment and the e-learning environment is how to authenticate students because unauthorized persons can access and manage information. The authors proposed a novel security scheme that contributed in resolving this vital issue by introducing an efficient secure model for supervising online evaluation including e-assessment or e-exam. The scheme addressed this imperative problem by proposing an approach that integrated available databases authentication technologies in conjunction with e-learning environments for controlling unethical behavior during e-assessment process.

Alarape et al [6] study implemented a computer-based assessment security system using biometric facial data. The system was tested at Federal Polytechnic, Bida with some selected students. [7] developed a computer-based test centre using biometric fingerprint for verification/authentication and tied the MAC adders of all the system to the program server. The system also tied the computers with the server 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. The performance under test was found to be satisfactory when comparing Manual verification/authentication (average 6.6sec) to Biometric verification/authentication (average 1sec).

Ibrahim et al [3] addressed the issue of accuracy in biometrics by proposing an image enhancement approach that incorporated SecuGen fingerprint in conjunction with electronic learning environments to curb unethical conducts associated with electronic examination in a university environment. Image enhancement was performed using crossing number concept to extract the enhanced images so as to improve the image quality. It was coded using Java (NetBeans IDE 7.4) to implement algorithms for enhancement, minutiae extraction and matching processing, where the resulting minutiae information was used as a method for identifying and matching fingerprints. Similarly, [8] authors improved on fingerprint enrolment of students to grant access for the conduct of e-exam.

Gil et al [9] described a fingerprint identification system (FIS) developed to be integrated in learning management system (LMS). Hence, a middleware is necessary to connect any LMS with their own FIS, which will provide them a scalable, robust, easy integration in any LMS. Ramu and Arivoli [10] proposed a framework that provided security to improve on-line examination by utilizing technologies such as biometric authentication based Keystroke Dynamics. The paper addressed this important problem by proposing a theoretical framework that incorporated available biometric authentication technologies in conjunction with Knowledge based authentication. Discussions on future research and possible implications of the proposed theoretical framework for practice were provided.

Garko and Ahmad [11] proposed a system that will help in identifying and verifying student during examinations with a view of minimizing exams malpractice. The paper observed that the introduction of fingerprint based exam verification system will help to easily identify students that registered for a particular course and can easily identify students that are eligible to enter the exam hall. Prototyping software development methodology was adopted in the paper. Visual Basic 6.0 was used to design the interfaces and Mysql was used as the back-end. The output from the system showed that, the proposed framework is more secured, more efficient, and has better performance when compared with the manual system of students' verification.

Joshy et al [12] focused on discussing a multi-factor authentication scheme specifically designed for securing online examination services without compromising user friendliness. The experimentation results clearly brought out the applicability of the scheme in real time with fine-tuning of network related parameters.

From the review of literature, the application of the fingerprint biometrics with CBT in Nigerian higher institutions has limited use. This study intends to narrow this gap. Therefore, this research is developed to eliminate the need for a middleware as found in study [9]. This is achieved by introducing a Single Sign-On approach. Also, our approach is web-based such that the client systems need no separate setup installation as identified in Ref. [7]. The study proposed fingerprint authentication against facial recognition of Ref. [6] because identical twins may pass facial authentication.

3. METHODOLOGY

3.1. Analysis of Existing System

This paper critically reviewed the authentication method of the existing computer-based testing system in Air Force Institute of Technology, Kaduna. The existing method of authenticating examinees is the use of login credentials only. One major drawback with the existing authentication method is that two independent candidates with the aim of impersonating one another can exchange user login credentials successfully to engage in examination malpractice.

3.2. Framework of the Proposed System

This study proposes additional authentication method with the existing credential-based method of accessing the CBT system as depicted in Fig. 1.

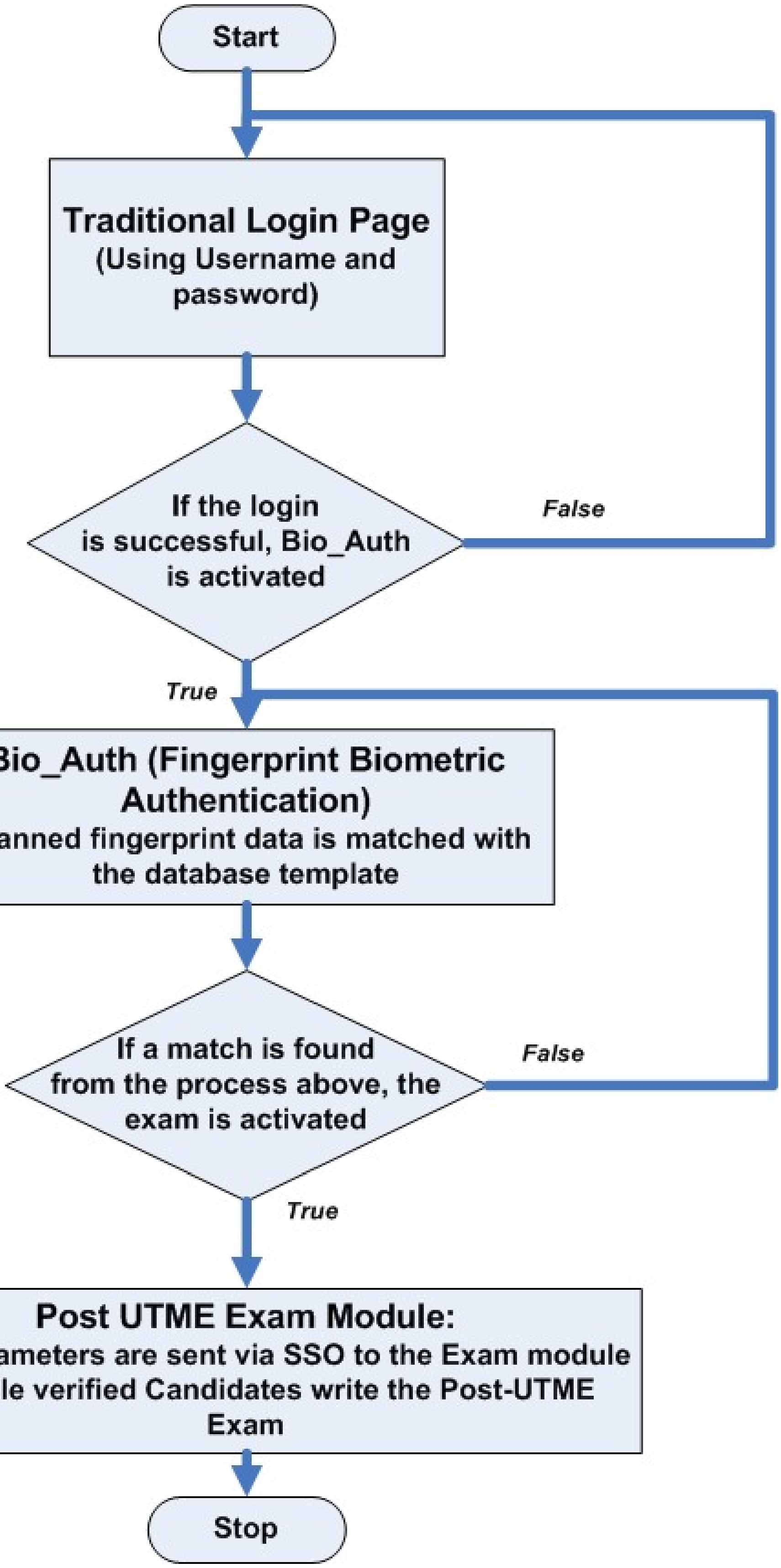

Start
Traditional Login Page
(Using Username and password)
If the login is successful, Bio_Auth is activated
False
True
Bio_Auth (Fingerprint Biometric Authentication)
Scanned fingerprint data is matched with the database template
If a match is found from the process above, the exam is activated
False
True
Post UTME Exam Module:
Login parameters are sent via SSO to the Exam module to enable verified Candidates write the Post-UTME Exam
Stop

Figure 1: Framework of the Proposed System

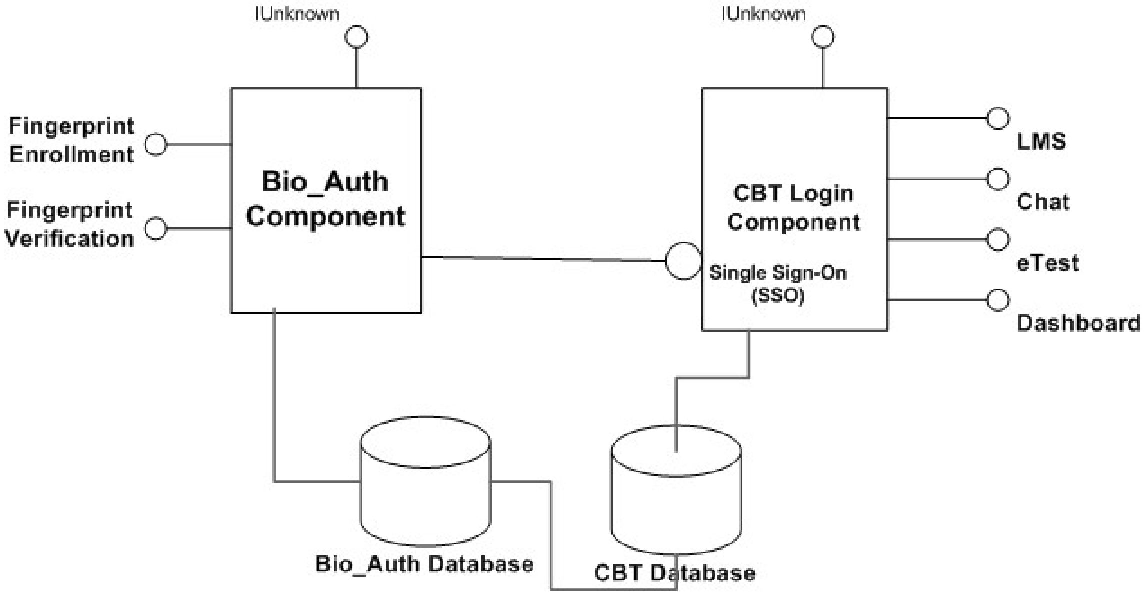


Figure 2: COM and OLE Diagram of the Proposed System

It implements fingerprint biometric authentication as a means of identifying the examinees.

3.3. *Proposed System Design*

The methodology used in this study is Component-based software engineering (CBSE). As seen in Fig. 2, the Component Object Model (COM) and Object Linking and Embedding (OLE) diagram, a call to the "requires" interface of the fingerprint device API (in this context – the Bio Auth component) makes the API process the request by capturing examinees fingerprint for either enrollment or verification. It then returns the desired services via its "provides" interface to the next component for further actions.

3.4. *Proposed System Development*

This study used the Flexcode Software Development Kit (SDK) to implement the fingerprint biometric authentication component of the system. FlexCode SDK provides advanced solution to retrieve fingerprint data from DigitalPersona fingerprint device specifically 4500 model. The functions in FlexCode SDK are not too basic, the functions concept are instant, you simply call the functions required for registering and verify fingerprints then the SDK does the registration process and verification process [7]. The native development environment is PHP. The system was implemented on Apache XAMPP server using MySQL as the database.

4. RESULTS AND DISCUSSION

4.1. *Fingerprint Biometric Enrollment*

Figure 3 shows the process of registering student's fingerprint. The data is stored in the database as a template.

The template generated during enrollment is used later for matching during verification process. A successful enrollment process is seen in Fig. 4.

As shown in Fig. 4, enrolment process is skipped. Fingerprint data templates are downloaded directly from JAMB and uploaded to the Bio_Auth database. These templates are later validated again candidates fingerprint scanned.

4.2. *Traditional Login (using credentials)*

The candidates login to the CBT system as seen in Fig. 5 using their JAMB registration number as username and a default password that will be given to them. Usually, the JAMB registration number is in the format of 8-digit numbers and 2-alphabets e.g. 96811559AH.

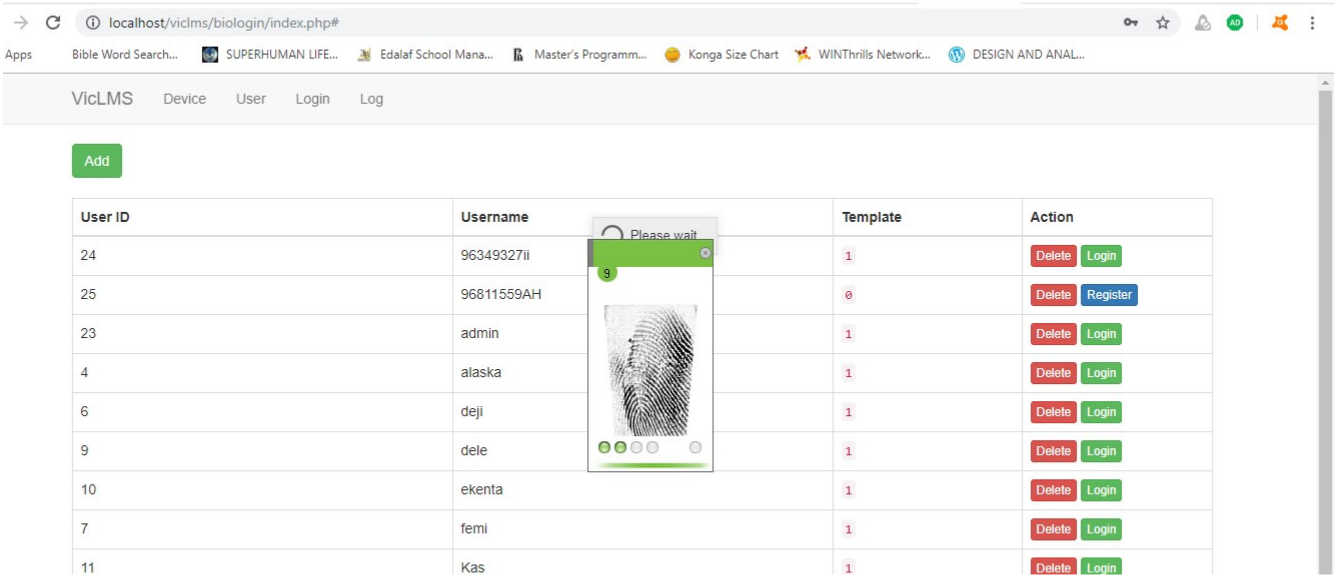
4.3. *Fingerprint Biometric Verification*

To identify a finger, after a successful login using credentials, the templates are used to compare the fingerprints scanned. Figure 6 shows the result of a fingerprint match (red indicator for a failed fingerprint match and green indicator for a successful fingerprint match.)

After a successful fingerprint verification, a success message is displayed with a link to proceed to the LMS/CBT application as seen in Fig. 7.

Clicking on the "Proceed to LMS" link takes the examinee to the CBT dashboard as seen in Fig. 8. This study implemented the option of Single Sign-On (SSO) method to pass the login parameters to the LMS login component. The component processes the credential and redirects the examinee to the LMS dashboard if the credential is valid or returns the examinee back to credential login page if invalid.

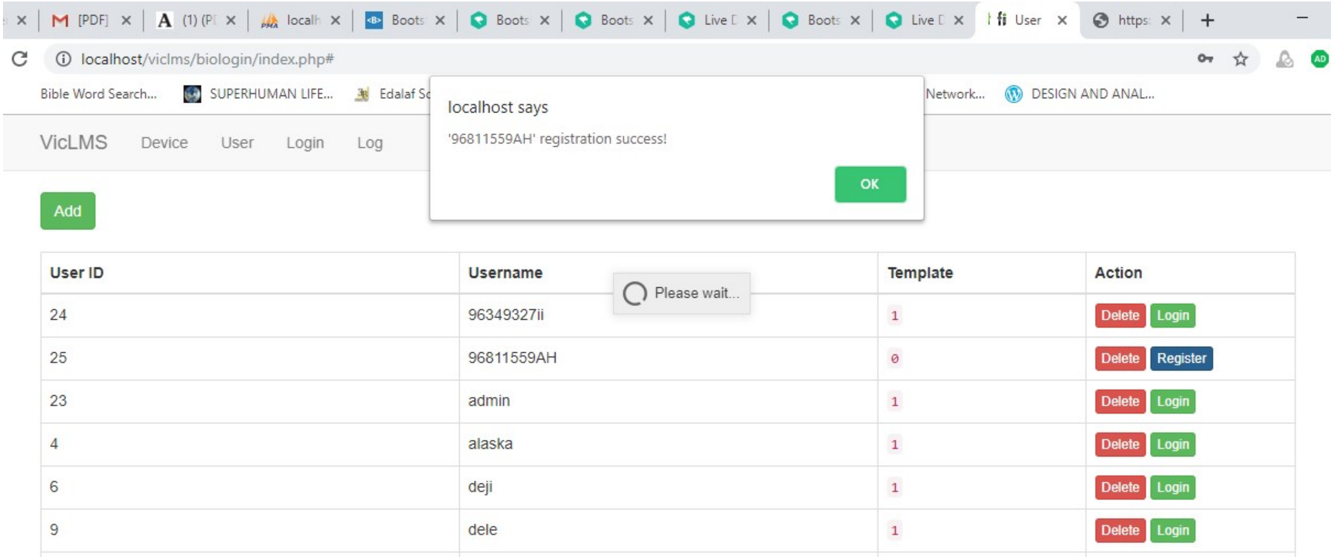
Implementing fingerprint biometric authentication is dependent on some factors. The fingerprint device available, the choice of programming language of the CBT, available SDK and the budget for the project can influence the implementation.



localhost/viclms/biologin/index.php#

User ID	Username	Template	Action
24	96349327ii	1	Delete Login
25	96811559AH	0	Delete Register
23	admin	1	Delete Login
4	alaska	1	Delete Login
6	deji	1	Delete Login
9	dele	1	Delete Login
10	ekenta	1	Delete Login
7	femi	1	Delete Login
11	Kas	1	Delete Login

Figure 3: Fingerprint biometric enrollment process



localhost/viclms/biologin/index.php#

localhost says

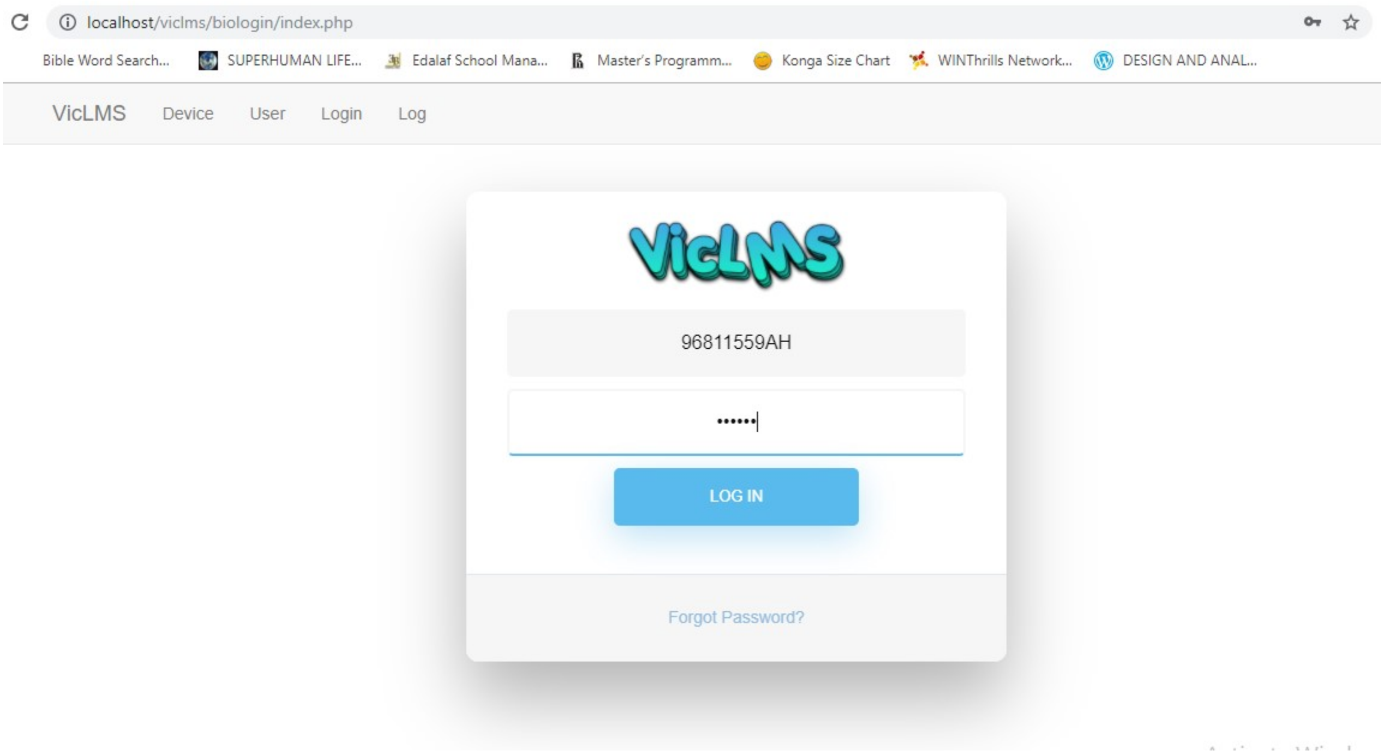
'96811559AH' registration success!

User ID	Username	Template	Action
24	96349327ii	1	Delete Login
25	96811559AH	0	Delete Register
23	admin	1	Delete Login
4	alaska	1	Delete Login
6	deji	1	Delete Login
9	dele	1	Delete Login

Figure 4: Successful fingerprint enrollment

Table 1: Performance evaluation with related studies.

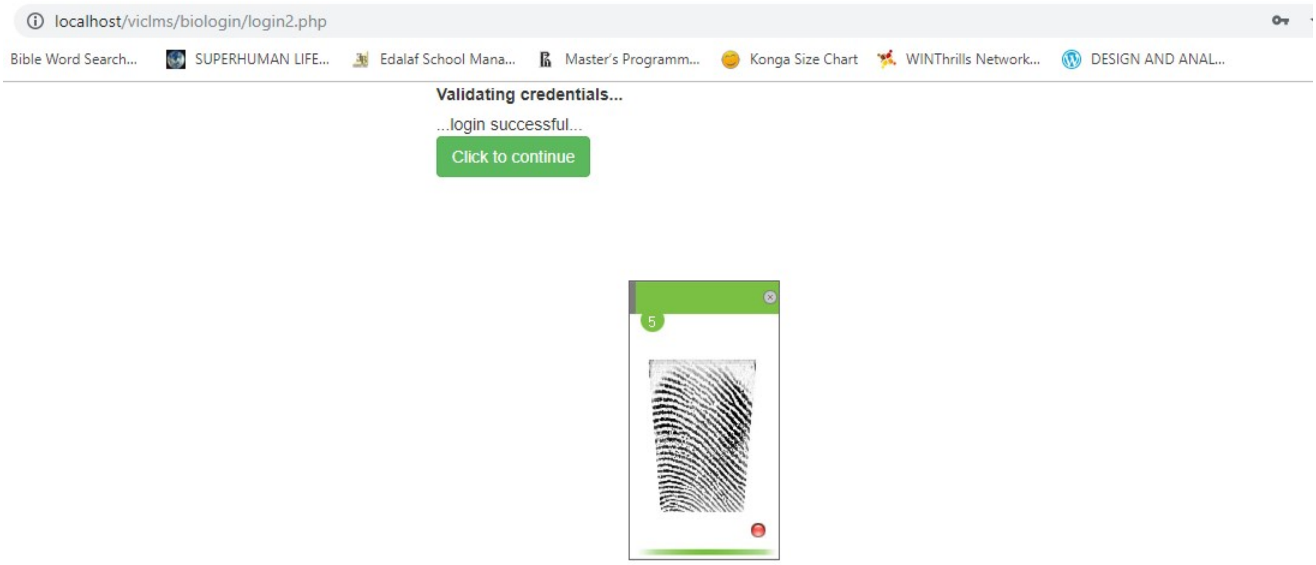
S/N	Author	Biometric	Fingerprint	Requires No middleware	Web-based	Remark
1	[3]	Yes	Yes	No	Yes	
2	[4	No	No	Yes	Yes	
3	[5]	No	No	Yes	Yes	
4	[6]	Yes	No	Yes	No	
5	[7]	Yes	Yes	Yes	No	
6	[8]	Yes	Yes	No	Yes	
7	[9]	Yes	Yes	No	No	
8	[10]	Yes	Yes	Not specific	Yes	Not implemented
9	[11]	Yes	Yes	No	No	
10	[12]	Yes	Yes	Not specific	Yes	Not implemented
11	This study	Yes	Yes	Yes	Yes	



96811559AH

••••••

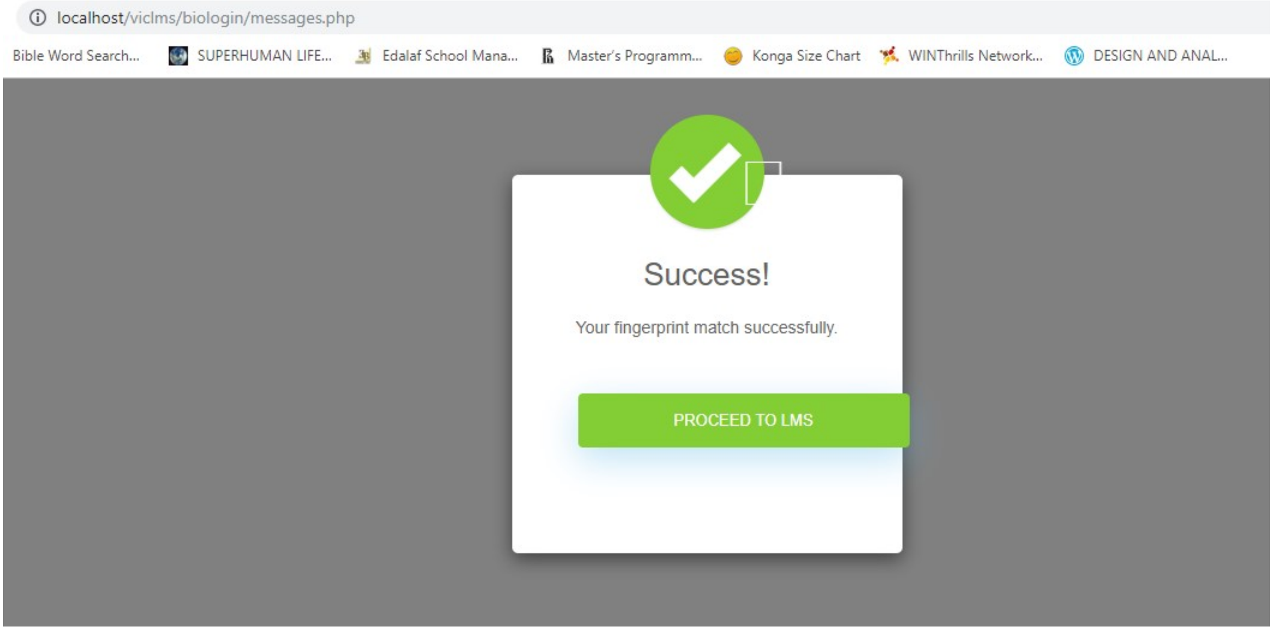
Figure 5: Login page using username and password



Validating credentials...

...login successful...

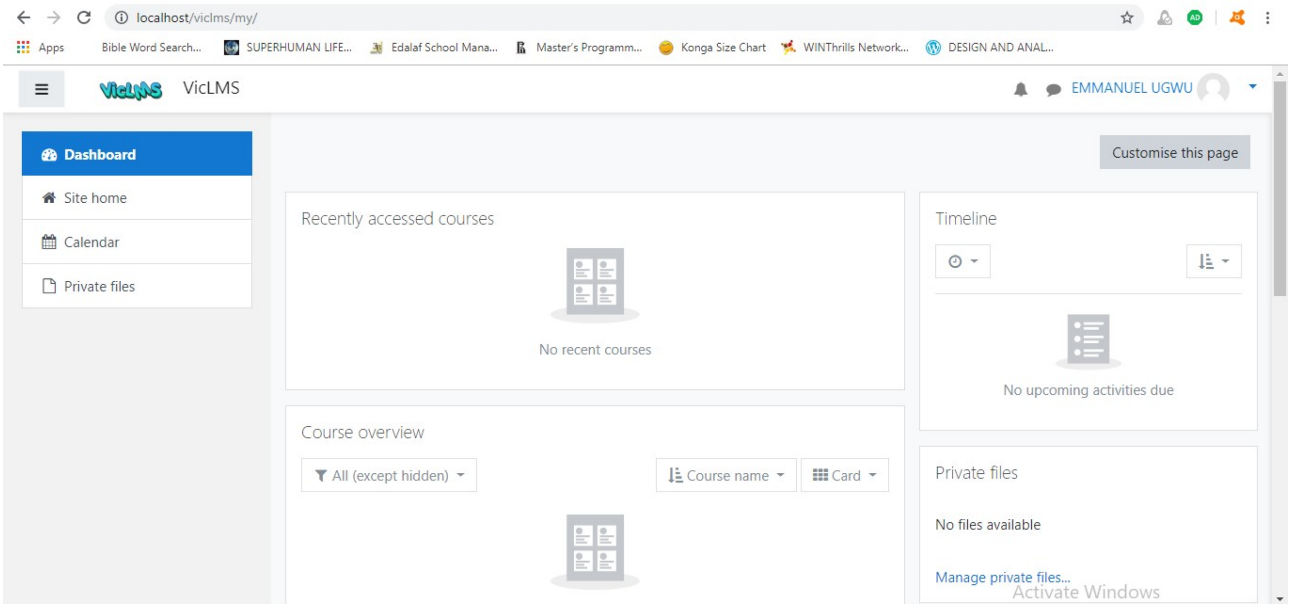
Figure 6: Fingerprint verification



Success!

Your fingerprint match successfully.

Figure 7: Success message with a link to access the CBT



No recent courses

No upcoming activities due

No files available

Figure 8: CBT Dashboard

4.4. Performance Evaluation of the Study Compared with Extant Literatures

A review of performance indices of related studies was done in comparison with the outcome of this research as found in Table 1.

The table above identifies the flexibility of implementation across the various related literatures. The result shows that this study takes into consideration the limitations of most of the works already done and improved on them to ensure better performance.

5. CONCLUSION

This paper understudied the existing CBT system in AFIT, Kaduna and discovered that the current method of authenticating examinees may affect the acceptability and authenticity of the results from the system. An authentication method using fingerprint biometric was proposed. The fingerprint biometric authentication system was developed using FlexCode SDK and it was implemented on DigitalPersona 4500 fingerprint reader. The CBT system was developed using PHP scripting language and the implementation was done on XAMPP local server and MySQL was database system used. The result improved the level of authentication and access to the CBT in AFIT.

References

[1] C. Okoronkwo. (2019, December) Appraising JAMB's Computer-Based Test. [Online]. Available: https://guardian.ng/news/features-appraising-jambs-computer-based-test/

[2] A. Boevé, R. Meijer, C. Albers, Y. Beetsma, and R. Bosker, "Introducing computer-based testing in high-stakes exams in higher education: Results of a field experiment," *PLOS ONE*, vol. 10, no. 12, pp. 1–13, 2015.

[3] M. Ibrahim, A. Othman, O. Adewale, and B. Balogun, "Design of a fingerprint biometric authentication technique for electronic examination," *International Journal of Computer Science and Telecommunications*, vol. 8, no. 2, pp. 8–15, 2017.

[4] M. Ajinaja, "The design and implementation of a computer based testing system using component-based software engineering," *International Journal of Computer Science and Technology*, vol. 8, no. 1, pp. 58–65, 2017.

[5] Y. Khlifi and H. El-Sabagh, "A novel authentication scheme for e-assessments based on student behavior over e-learning platform," *International Journal of Emerging Technologies in Learning*, vol. 12, no. 4, pp. 62–89, 2017.

[6] M. Alarape and M. Saheed, "Enhancing computer-based assessment security using biometric facial data," *Circulation in Computer Science*, vol. 2, no. 4, pp. 22–26, 2017.

[7] O. Omorogiuwa and F. Nwukor, "Design and implementation of a computer based test centre using biometric for authentication," *American Journal of Advanced Research*, vol. 1, no. 1, pp. 13–18, 2017.

[8] M. Ibrahim, A. Othman, B. Balogun, U. Musa, and C. Ujah, "Development of a fingerprint biometric authentication scheme in electronic examination," *International Research Journal of Advanced Engineering and Science*, vol. 2, no. 1, pp. 177–185, 2017.

[9] C. Gil, G. Diaz, and M. Castro, "Fingerprint identification in LMS and its empirical analysis of engineer students' views," in *IEEE EDUCON 2010 Conference,*, Madrid, Spain, April 2010, pp. 1729–1736.

[10] T. Ramu and T. Arivoli, "A Framework of Secure Biometric Based Online Exam Authentication: An Alternative to Traditional Exam," *International Journal of Scientific & Engineering Research*, vol. 4, no. 11, pp. 52–60, 2013.

[11] A. Garko and A. Ahmad, "Design and Modeling of a Student Verification System in an Examination in Nigeria using Biometric Fingerprint Technology," *International Journal of Advanced Academic Research: Sciences, Technology & Engineering*, vol. 3, no. 7, pp. 1–16, 2017.

[12] N. Joshy, G. Kumar, P. Mukhilan, M. Prasad, T. Ramasamy, and N. Harini, "Multi-factor authentication scheme for online examination," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 15, pp. 1705–1712, 2018.