UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

# Centralized Students' Authentication for Higher Education Systems in Nigeria

Musa Midila Ahmed
Physical Science Education Department,
Modibbo Adama University, Yola, Nigeria
Ahmedmm4me@yahoo.com

Submitted: 5/7/2021. Revised edition: 11/8/2021. Accepted: 26/10/2021. Published online: 16/5/2022
DOI: https://doi.org/10.11113/ijic.v12n1.325

***Abstract*—Increase in the adoption of ICT for service provision renders higher educational institutions in Nigeria vulnerable to numerous security challenges. The information security threats addressed in this paper encompasses identity theft and identification frauds. The high number of students patronizing these institutions seeking for knowledge results in the challenges of identifying authentic students. The use of students' identification number and password is no longer sufficient for authentication of students. Therefore, this paper proposed a centralized authentication model for higher education system (CAMHES) for Nigeria. The model uses multi-factor authentication combining students' identification number, students' fingerprint biometric and smartcard technology for students' authentication. The solution authenticates the identity of genuine students to eliminate impersonation in Nigerian higher education systems. Although, this solution provides authentication that is extremely difficult to replicate, it is recommended that the students' biometric data captured must be strictly kept safe.**

***Keywords*—Authentication, Centralized authentication, Fingerprint Biometric, Smartcard Technology, Higher Education**

## I. Introduction

Educational institutions manages lots of data ranging from personal, academic and healthcare information of both students and staff. Managing the security of students' data is extremely challenging for educational organizations because it involves both external and internal threats. Currently, higher institutions of learning such as polytechnics, colleges and universities have congested access to buildings and services in Nigeria due to the huge population of students in these institutions. Large group of students needs access to precious equipment and services in various buildings in these institutions. This makes it difficult to keep tract of those authorized or not into certain building and services. In addition, there is the need to prevent bad incidences such as vandalism, theft and misuse of these limited resources. However, enforcing effective security for Nigerians overpopulated educational institutions is quite challenging.

According to Ekpot, *et al.* (2020) [1], it is the responsibility of educational institutions' management to protect its students, staff and transaction data from any threat. The complex nature of security enforcement in education institutions leads to adoption of ICT for information security managements. The use of modern technology for security operation in educational institutions is necessary due to the large population of students and staff. Generally efficient students and personnel authentication serves as the foundation for protection of both tangible and intangible assets in any organization. Adequate authentication curtails potential and real threats, especially impersonation and identity theft as well as the basis for accountability in information management. Authentication solution should uniquely verify each individual including identical twins for education service consumption and certificate award.

The use of student identification number and pin for access control is no longer sufficient in view of the increase in applications security requirements. Consequently, biometric technology such as fingerprint is nowadays adopted for identification and authentication of persons in security critical organizations. The biometric data are relatively safer because of their uniqueness, which made it difficult to be stolen or forged [2]. Biometric fingerprint technology has been in use for over a decade in forensic to identify criminals by law enforcement agencies. However, its adoption for security enhancement in higher education institutions emerges recently to overcome the challenge of accurate students' identification. Adequate human identification is a necessary requirement for successful achievement of availability, confidentiality and integrity security goals in educational systems.

Biometric technology are nowadays used to uniquely identify person based on some physiological or behavioural characteristics. [3] identified nine (9) biometrics techniques widely used to recognize an individual. These are fingerprint, facial recognition, hand's design, hand's vein, iris, patterns of retina, voice and signature. The author singled-out fingerprint as the most reliable and legally recognized biometric technique. Advancement of computing leverages on the ease and inherently many sources up to ten fingers of fingerprint data for unique individuals identifications. The digital images of the fingerprint is captured by sensors for matching. The two popular matching technique used to compare fingerprint images are minutiae and pattern matching. The minutiae matching uses the location and direction of fingerprints' point for recognition. While the pattern matching compares fingerprint images to detect duplications.

Recently, storage, sharing and transaction of biometric data across the internet is effected by smartcard technology. Smartcard has become a vital tool in human life. The multi-functional role of smart card particularly in security provision ranges from user identification to authentication for physical and logical access control to protected resources. According to [4], researchers have identified security as a factor that encourages the adoption of smartcard technology. Smartcards are widely used for authentication and access control to restricted area as well as payment wallet. Although, smartcards are not completely immune to privacy violations. [5] identified micro probing, software attack, eavesdropping, and fault generation as some of the smartcard tampering techniques. Micro probing attackers' targets is to get direct access to chip surface for monitoring and exploiting the integrated circuit. Software attackers intercepts the communication channel to leverage on any vulnerabilities identified. Whereas eavesdroppers monitors the traffic in violation of the confidentiality of the interacting parties. Finally, fault generation attackers who creates abnormal defect in the processor and use the mal functional point to access the system. In an effort to protect the privacy of smartcard processor, the authors provides counter measures against a range of these attacks.

In order to abide by the standards, laws and regulations of the Nigerian education sector, the proposed solution follows the identifiable students' information provided at the point of registration for admission into Nigerian higher institutions. This paper proposed the use of the fingerprint biometric capture in line with the joint admissions and matriculation board (JAMB) during registration for the identification and authentication of students in higher educational institutions in Nigeria. This is by creating an authentication model in the institutions for identification of genuine students in collaboration with the centralized admission processing systems (CAPS) of JAMB. It is important for higher educational organizations to invest a lot towards effective protection of students' data as well as efficient security enforcement and control access to its services and resources.

## II. RELATED WORK

Authentication is the process of verifying the true identity of systems' user. Authentication technology checks the credentials of users to evaluate if the credentials tendered corresponds with those in database of authorized users. Studies by [3] and [6] focused on the problems of attendance management systems. [3] reviewed literatures on fingerprint attendance systems and classified the systems according to implementation tools and techniques. Similar focus by [7] identified micro controller, biometric sensors, communication channels, and database storage as the hardware parts use for biometric based attendance tracking systems for education sector. [6] proposed an automated attendance management system using rapid application development (RAD) software development methodology. The focus of these studies is not on verification of identities to curtail impersonation and control access to critical aspects such as examination in educational systems. But to tracks the records of those that are present in educational services such as library, lectures, sports, etc.

Apart from the authentication for service attendance management system, access control to examination is another crucial problem in higher educational institutions. An effort to enhance user authentication in distance education by [8] provides a methods for continuous biometric user authentication in online examination by keystrokes dynamics. [9] designed a verification system that can differentiate between valid users from imposter. The authors used new verification system based on distance computed among Gaussian mixture model created by different writing task. The results shows 24.3% reduction in equal error rates compared to existing systems. The advantage of using the keystroke dynamics and/or computed distance verification system is that they don't require additional hardware apart from the keyboard. To improve remote proctoring method in distance education, [10] used facial detection by cropping out the face and facial recognition approach using eigenface-based face recognition algorithm to enhance the possibility of identifying suspicious behaviors in online examination. However, the studies focused on detecting examination malpractice not impersonation in online examinations. [11] collected and analysed published literatures and identified digital techniques to achieve authentication for online examination.

Investigating the underpinning theory helps in understanding relevant empirical facts about a phenomenon. Looking at the context from varying theoretical perspectives leads to higher order thinking that creatively establishes connections between different components. [12] proposed a smart class model to manage educational activities. The authors used a framework for smart class system that enables the use of facial recognition for login by students and faculties. [13] identified factors that can influence users' adoption to develop a model for smartcard technology. Similarly, effort to develop an adoption model by [14] reviewed ethical scenarios of smartcard usage. This results in formulation of smartcard technology acceptance model from ethical and social perspectives. With the aim of enhancing socialization in Indonesia, [15] used descriptive qualitative research method to discover that smartcard socialization prevents students' drop-out of schools.

Most studies reviewed focused on either improving class attendance management system ([7]; [7]; [3]) or authentication for online examination in distance learning education ([8]; [10]). Attempts to protect the privacy of smartcard processors by [5] identified the smartcard tampering techniques to provide counter measures against a range of confidentiality attacks. [16] used online survey to investigate students' acceptance of smartcard technology. The results shows usefulness, security, ease of use, among others as factors that significantly influence adoption of smartcard technology in Iranian universities. However, provision comprehensive security for higher education institutions is crucial. Therefore, studies toward efficient authentication of students in higher educational institutions is recommended. In view of the fact that authentication plays a necessary and vital role in the realization of confidentiality and data integrity security goals of any information systems.

## III. METHODOLOGY

According to [17], research methodology is a collection of principles and ideas that guide conduct of the research study. This paper presents centralized authentication modelling approach for higher educational institutions in Nigeria. The description of the new model allows efficient planning, provision and control of comprehensive security in Nigerian higher education systems. The comprehensive security concepts means that the information security must be provided in a holistic manner. Therefore, potential solution to security challenge should focus on multidimensional security provision for protection from any contemporary threats. Addressing security challenge in any organization requires understanding of the three essential information security goals; confidentiality, integrity and availability. Confidentiality is the security goals that requires the concealment of communication content from disclosure to unauthorized entities. Integrity in the information security context refers to the accuracy and completeness of information exchanged between authentic entities and availability is to ensure that information is accessible to all authenticated and authorized entities. However, all these essential security goals requires authentication for establishing the true identity of the authorized entities.

The development of the centralized authentication model consists of five (5) modules as follows:

**A.** **Input Module:** This aspect comprise of the device that reads inputs from the students' smartcard. The smartcard reader reads students identification number then forward it to the authentication module for authentication. Furthermore, the system redirects to the interface for users to scan students' fingerprint biometric for further authentication.

B. **Central Database:** The central database comprise of database server hosting multiple database tables linked to the smartcard scanners and input interfaces. The database might also be connected to the proxy stations for remote service provisions particular in large institution to ease students' validation for enrolment and authentication. The central database server host the database of the programs offered by the institution. Also, the server contains the database of all registered students for each programme.

C. **Validation Module:** This module establishes an interface with the JAMB's CAPS to check the validity of admissions presented by candidates to the institution. This module recognizes genuine admission by comparing the JAMB registration number and the biometric data of candidates with those offered admission in the JAMB's database.

**i) JAMB' Registration Number Validation**
This is a sub-module that verify the genuineness of candidates' admission by students' JAMB registration number. The task is to match students' registration number with that of admitted students in JAMB'S database. However, positive result in this part is not sufficient for official acceptance of candidates' admission.

**ii) Students' Biometric Validation**
This sub-module verifies the fingerprint biometric data of candidates to ascertain genuineness of candidates' admission by students' biometric data. The task is to validate students' biometric data with that of admitted students in JAMB'S database. Positive result in this part in addition to success in validation of students' registration number is sufficient for official acceptance of candidates' admission.

**D.** **Registration Module:** This module identifies admitted students after successful validation. Students' details are captured and recorded in the institutions database. In this stage, students are recognized by the institution officially and legally. Institutions assign students' matriculation number as well as captures students' fingerprint biometric data for authentication.

**i) Students' Matriculation Number**
This is a unique identification number assigned to all validated admitted students at the point of enrolment. Generally, obtaining matriculation is the formal process of enrolling into any higher institution in Nigeria. Therefore, all validly admitted students should obtain matriculation number printed on the students' smartcard to consume services rendered by the institution.

**ii) Finger Print data Capture**

To enhance the authentication of valid student, fingerprint biometric data of the students should be captured for institutions' database record. This enable multi-factor authentication of students to improve the information security of institutions in general.

E. **Authentication Module**: This module captures students' information such as matriculation number and fingerprint biometric data and compares the information with those recorded in the institutions' database. The role of this module is to authenticate the identity of students who want to access the institutions' services by multi-factor authentication. The students to be authenticated presents their unique matriculation number and place their fingerprint on the finger print scanner to capture the minutiae pattern extracted from their fingers.

**i) Matriculation Number Authentication**

Students' matriculation number is one of the factors to determine the true identity of genuine students of the institution. This is the traditional identity data expected to be produce by all students. This part match the supplied matriculation number against the database records.

**ii) Fingerprint Biometric Authentication**

To improve the efficiency of the security system requires additional data that is hard to forge because it can only be produce by that specific person. Consequently, this leads to another authentication process using the uniqueness of fingerprint biometric to provide inherent identity information.

## IV CENTRALIZED AUTHENTICATION MODEL FOR HIGHER EDUCATION SYSTEM (CAMHES)

### 4.1 Admission Process

To enhance the efficiency of admission processing into tertiary institutions in Nigeria. The JAMB migrates the process to centralized admission processing system (CAPS) with effect from 2018/2019 academic session [18]. An overview of the major stakeholders' role in admission process is presented as follows.

### A. Candidates' Role

The role of applicants in the process of admission into the Nigerian tertiary institution is hereby classified into create profile, purchasing e-PIN, registration at computer-based test (CBT) center, write UTME/Post-UTME examinations, accept or reject admission and print admission letter.

**i) Create Profile**

The first step in the JAMB registration is the creation of profile by candidates. The created profile code enables candidates get access to JAMB e-Facilities dashboard for numerous candidates' services such as application for change of course or institution, printing results slip, data update, checking of admission and printing of admission letter. The JAMB profile can be created in three ways; by using short message service (SMS), by Unstructured Supplementary Service Data (USSD) code, and on the JAMB website.

- Using SMS: On the mobile phones' text message window, type 'NIN' space 'NIN Number'. Then send the SMS to 55019. This is the recommended method. However, this service will cost candidates 50 naira.
- By USSD Code: On your mobile phone dial *55019*NIN# to obtain the profile code.
- On the JAMB website: candidates can create new e-facilities account on JAMB website. However, this is not JAMB's recommended method.

**ii) Purchase e-PIN**

Sequel to creation of profile, candidates should proceed to make payment to obtain e-PIN. The procurement of e-PIN for JAMB registration can be at bank, CBT centers or JAMB offices.

**iii) Registration for computer-based test (CBT)**

After creation of profile and procurement of e-PIN, candidates are expected to visit any accredited JAMB CBT center for personal details and biometric data capture.

**iv) Write UTME/Post-UTME Examinations**

Candidates are expected to sit for JAMB's unified tertiary matriculation examination (UTME). In addition, some universities conduct post-UTME examinations.

**v) Accept or Reject Admission**

Candidates are expected to keep on checking their admission status in the e-facilities profile. Admitted candidates are expected to accept the admission to enable them print their admission letter.

**vi) Print Admission Letter**

Admitted candidates that accepted their admission can print their admission letter through the JAMB's e-facilities dashboard and proceed to the admitted institution for verification and documentation.

### B. JAMB's Role

**i) Registration of Candidates**

JAMB ensures that the accredited registration centers are up and running to enable online registration of candidates for both the UTME and DE candidates. After registration of candidates, the board announce cut-off points, examination dates and schedules timelines of admission activities.

**ii) Conducting UTME**

The biometric data of registered candidates should be verified at the CBT centers for writing the UTME examination. The board also conducts optional mock UTME examination for interested candidates to gain experience on how the examination system works.

**iii) Regulating Admission Process**

To adequately discharge its duties of administering entrance examination into Nigerian tertiary institutions, JAMB maintains e-facilities dashboard for candidates and institutions for efficient service provision. The e-facilities dashboard for candidates host services such as application for change of institution or course, checking admission status, printing admission letter, data updates, etc. Furthermore, the board trains chief executives, admission officers and registrars of tertiary institutions as stakeholders and maintains institutions dashboard on CAPS for efficient admission processing.

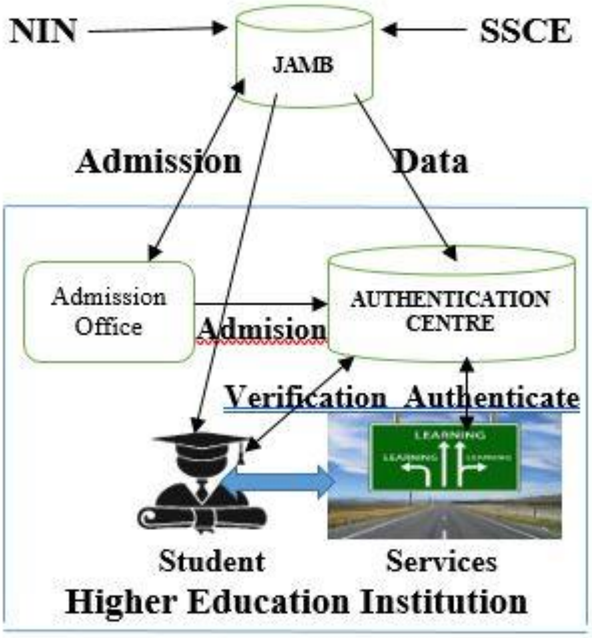

Fig. 1. Centralized Authentication System

### C. Institutions' Role

The tertiary institutions' dashboard in the CAPS provide interface to enable institutions choose criteria such as JAMB and post-UTME score, gender, and origin of candidates for admission. These criteria ease internal admission process by automating the roles of stakeholders, including admission officers and heads of tertiary institutions. The stakeholders leverage on the efficiency of CAPS in admission process eliminating favoritisms and promoting equal opportunity to qualified candidates. The adoption of CAPS for admission processing has indeed enhanced the integrity and simplified the process generally.

### 4.2 Authentication Procedure

Authentication is the process of establishing the true identity of systems' user. It is by comparing users' information with those in the database. Authentication security system usually depends on adequate identification and verification of users. The aim of authentication is to prove users' identity as such it is impossible to authenticate a candidate without adequate identification system. Identification in this context is carried-out at the point of registration for admission with the JAMB. During data capture of registration process, candidates provides detail information including all the ten (10) fingerprint biometric data. Fingerprint biometric data is non-transferable, which provides security against identity theft and identification frauds. The use of fingerprint identification system by JAMB creates the basis for efficient information security protection in all higher educational organization in the country. It provides higher accuracy and improves security especially at the point of candidates' verification and authentication.

**a) New Students' Verification**

Sequel to candidates' identification by fingerprint at the point of registration with JAMB, admitted candidates prints JAMB's admission letter from the CAPS's e-facilities and proceed to the admitted institution for verification. This enables admitted candidates receive the institutions' admission letter and proceed with other enrolment procedures. At the verification stage, candidates' data including fingerprint biometric data is recaptured and compared with the one in JAMB's database. Institutions' recognizes successfully verified students for issuance of unique organizational identification number and institutions' admission letter.

**b) Students' Data Capture**

Success in verification qualifies students to the institutions' data capture stage by presentation of unique organizations' identification number and institutional admission letter as an evidence. At this stage, students provide all the necessary information required by the institutions including fingerprint biometric data for storage in the database. These data is used by the center to provide fingerprint biometric smartcard for students' identity. The fingerprint biometric smartcard combines students' data including fingerprints with radio frequency identification (RFID) smartcard technology to make the system more secure on entry. Furthermore, in order to provide quick and reliable authentication for education services' consumption, the center issues fingerprint biometric authentication scanners to all security critical services provided by the institution. This ensures institutions' service is consumed by authenticated students only. The hardware captures the fingerprint biometric data of students and compare with those in the database to approve or deny access to the institutions' services.

**c) Students Authentication**

At this stage, all registered students has smartcard for both physical and electronic identification with their photograph on it. Generally, multi-factor authentication are of three categories; something the student know, something the student has, and something inherent with the student. First, the students know their identification numbers as an authentication factor. Second, the students has their smartcards with photograph and identification on it as an authentication factor. Third, students' fingerprint can be matched on one-to-one with those stored in the database for security critical services' authentication. Overall, the use of multi-factor authentication makes the system much more difficult for attackers to exploit.

### 4.3 Discussion of the Model

The centralized students' authentication model consists of four (4) parts: JAMB, Admission office, Authentication center and Institutions' services.

The Joint Admission and Matriculation Board (JAMB) is established by the federal government of Nigeria on 13th February 1978 to administer entrance examination for potential undergraduate candidates into Nigerian universities. By August 1988, the federal executive council empowered the board to handle the matriculation examination into all Nigerian tertiary education institutions. The board developed and migrated to its centralized admission processing system (CAPS) to enhance the efficiency of admission process into tertiary institutions in the country as from 2018/2019 session. The success achieved from inception of CAPS generally as well as in the information security perspective is highly commendable. However, tertiary institution need to complement on the success of CAPS by investing in authentication of admitted students to curtail impersonation and/or identity theft at the point of enrolment.

All tertiary institutions in Nigeria established admission offices who serves as the institutions' representative in the selection and administration of students' admission to the organization. The recent transition of the admission process from the tradition paper-based process to the online admission process system ease the role of office. The system handles the process from registration of applicant to admission offer. The admission officer is officially responsible for setting admission criteria, cut-off point, screening of candidates and selection of recommended candidates for JAMB's approval. This office should provide the list of admitted candidates to the authentication center for verification and validation.

Generally, authentication is the procedure of establishing the true identity of systems users. It starts at the point of enrolment by validation of admitted students into the institution to ensure that they fulfil every security requirement. Each institutions' centralized authentication system can interface with the CAPS of JAMB to validate the admissions presented by candidates at the point of enrolment. On successful validation, admitted students' detail information with fingerprint biometric data are registered in the central database. In addition, the authentication center issues all registered students with unique matriculation number written on students' smartcard. Students scan the smartcard and/or enter the matriculation number for system to compare against the information stored in the central database during authentication. The central database of the institution becomes the authentication point for institutions' service consumption.

Higher education institution invest lot of money for human and materials resources acquisition to provide services to students and community. The centralized authentication system mediate between the students or users and the organizations services. Users who attempt to access the services submits students' matriculation number and the authentication systems redirect to the biometric scanner interface to capture students fingerprint. The system authenticates and grant access to users whose digital information matched with those authorized to consume that particular service in the database. Generally, the authentication process is summarized as follow; user request for institutions' service, the authentication systems checks for access right of that student and respond either success or failure. Successful authentication enables students to enjoy the institutions' services.

## V CONCLUSION

The use of biometric technology by both governments and non-governmental organizations (NGOs) is gaining acceptance in view of its efficiency and reliability. Application of fingerprint biometric in Nigerian education systems is a new innovation to achieve the desired security enhancement. The JAMB introduced the fingerprint biometric as part of the CAPS's data capture requirements for candidates to resolve many categories of examination malpractices in the admission system. Hitherto, the UTME is the initial target of abuse by some applicants. Now, candidates are identified by their biometric data to sit for the examination instead of mere registration number and names.

To eliminate impersonation at all level of the higher education system, there is the need to extend the application of biometric technology to authenticate the identity of genuine students. Although, the adoption of this technology is in its early stage in Nigerian education systems, it is crucial to keep biometric data safe. In addition to measures taken by institutions to protect the stored data, students should be aware of the need to keep their biometric information safe, particularly over the network. Biometric technology provides students' authentication service that is extremely difficult to replicate. However, one of its major disadvantage is that once biometric data is hacked, it leads to serious consequences. This is because it is not like password that can be changed, biometric data cannot be changed as such it must be strictly kept safe. Finally, evaluation of the centralized authentication model is recommended to evaluate its efficiency and accuracy in higher education systems of Nigeria.

## ACKNOWLEDGMENT

I acknowledged my family, council and management of Modibbo Adama University, Yola Nigeria for their support and encouragement toward publication of this article.

### A. Abbreviations and Acronyms

**ICT:** Information and Communication Technology
**JAMB:** Joint Admission and Matriculation Board
**CAPS:** Centralized Admission Processing Systems
**RAD:** Rapid Application Development
**USSD:** Unstructured Supplementary Service Data
**SMS:** Short Message Service
**NIN:** National Identification Number
**CBT:** Computer-Based Test
**UTME:** Unified Tertiary Matriculation Examination
**e-PIN:** Electronic Personal Identification Number
**DE:** Direct Entry
**SSCE:** Senior School Certificate Examination
**RFID:** Radio Frequency identification
**CAMHES**: Centralized Authentication Model for Higher Education Systems

## REFERENCES

[1] Ekpoh, U. I., Edet, A. O., & Ukpong, N. N. (2020). Security Challenges in Universities: Implications for Safe School Environment. *Journal of Educational and Social Research,* 10(6), 112-112.

[2] Jain, A. K., & Kumar, A. (2012). Biometric Recognition: An Overview. *Second Generation Biometrics: The Ethical, Legal and Social Context,* 49-79.

[3] Walia, H., & Jain, N. (2016). Fingerprint Based Attendance Systems-A Review. *International Research Journal of Engineering and Technology,* 3(5) 1166-1171.

[4] Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2011). Smart Card Security; Technology and Adoption. *International Journal of Security,* 5(2), 74-84.

[5] Kömmerling, O., & Kuhn, M. G. (1999). Design Principles for Tamper-Resistant Smartcard Processors. *Smartcard,* 99, 9-20.

[6] Antoh-Baffoe, C. (2017). A Proposed GSM Biometric Attendance Management System for Ghana Education. *International Journal of Advanced Networking and Applications*, 9(3), 3421-3427.

[7] Hoo, S. C., & Ibrahim, H. (2019). Biometric-based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements. *Journal of Sensors*.

[8] Flior, E., & Kowalski, K. (2010, April). Continuous Biometric User Authentication in Online Examinations. *2010 Seventh International Conference on Information Technology: New Generations*. IEEE. 488-492.

[9] Escobar-Grisales, D., Vásquez-Correa, J., Vargas-Bonilla, J. F., & Orozco-Arroyave, J. R. (2020). Identity Verification in Virtual Education Using Biometric Analysis based on Keystroke Dynamics. *TecnoLógicas,* 23(47), 193- 207.

[10] Zhang, Z., Aziz, E. S., Esche, S., & Chassapis, C. (2018). A Virtual Proctor with Biometric Authentication for Facilitating Distance Education. *Online Engineering & Internet of Things,* Springer, Cham, 110-124.

[11] Wiklund, M., Mozelius, P., Westin, T., & Norberg, L. (2016, October). Biometric Belt and Braces for Authentication in Distance Education. *European Conference on e- Learning. Prague, Czech Republic. Retrieved from: https://search-proquestcom.contentproxy.phoenix.edu/docview/1860070766*.

[12] Siddiqui, A. T., & Masud, M. (2017). A System Framework for Smart Class System to Boost Education and Management. *arXiv preprint arXiv:1707.02924*.

[13] Taherdoost, H., & Masrom, M. (2009, June). An Examination of Smart Card Technology Acceptance Using Adoption Model. *Proceedings of the ITI 2009 31$^{st}$ International Conference on Information Technology Interfaces,* IEEE, 329-334.

[14] Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2012). Smart Card Technology; Awareness and Satisfaction. *Journal of Computing,* 4(6), 128-132.

[15] Santari, A. N., & Sunarya, D. M. (2017). Public Relations Strategy for Disseminating Indonesian Smart Cards. In The Ministry of Education Indonesia. *International Journal of Pure and Applied Mathematics,* 117(15), 873-883.

[16] Taherdoost, H. (2017). Appraising the Smart Card Technology Adoption; Case of Application in University Environment. *Procedia Engineering,* 181, 1049-1057.

[17] Mills, J., & Birks, M. (2014). *Qualitative Methodology: A Practical Guide*. Sage.

[18] Oloyele, I. O. (2021). Centralized Admission Processing System (CAPS). Joint Admission and Matriculation Board https: www.jamb.gov.ng/caps.