Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2015; 3(1A):37-41 **ISSN 2347-9523 (Print)**

(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Research Article

Curbing Truancy and Impersonation in an Educational Institution Using Fingerprint Biometric: A Study of Ogun State Institute of Technology, Igbesa.

Ojo, Abosede Ibironke[1], Ojo, Matthias Olufemi Dada*[2], Oladejo Rachel Adefunke[3]
[1,3]Department of Computer Science, Ogun State Institute of Technology, Igbesa, Ogun State
[2]Department of Sociology, Crawford University of the Apostolic Faith Mission, Igbesa, Ogun State, Nigeria

***Corresponding author**
Ojo, Matthias Olufemi Dada
Email: femfemty@yahoo.com, matthiasolufemiojopublications@gmail.com

Abstract: This study applied the use of biometric (finger print) in curbing truancy and impersonation among the staff of an Educational Tertiary Institution. It implements an UML-Use Case Diagram. Goal of the content, Scope of the System, the Actors, the Staff, Register, Staff Enrolment, Log In, Finger print Page and the Administrator were the components in the System, implemented. It also explained the principle involved in the implementation of Biometrics. The study concluded that truancy and implementation affects the rate of productivity and created unnecessary irregularities in the work place. The application of finger print Biometrics would, undoubtedly, curb the problems of truancy and impersonation in work place. It is recommended that every Nigerian Organization i.e. Manufacturing Industries, Companies, and Government Ministries should begin to apply finger print Biometric to curb the problems of truancy and impersonation in their places of work.
Keywords: Finger print; Biometrics, Truancy; Impersonation and Implementation.

INTRODUCTION

Biometric is biotechnological ways of making identifications. There are several ways of identifying people using biometrics: Face, Voice, palm print, Hand Geometry, Iris, Retinal Scan, DNA, Signature, Gait and Keystrokes and Finger Print. However, this study applied the use of fingerprint biometric to curb the problems of truancy and impersonation in an Organization. Truancy is a frequent deviant behavior among the teaching and non teaching staff. Truancy has reduced the rate of productivity among staff and academic good performance among the students. Impersonation is another common problem, especially among the staff during staff auditing. There is a need therefore to put in place proper measure to curb truancy and impersonation among the staff of the institution. Finger print biometric method of identification was applied in the study, explanations and illustrations were given on how it can be applied to curb truancy and impersonation in the institution.

LITERATURE REVIEW

Biometric is a form of universal identification. ‘‘Biometric characteristics’’ is a general term used to describe a measurable physiological and /or behavioural characteristic that can be used for automated recognition.[1] A biometric system provides an automated method of recognizing an individual based on the individual’s biometric characteristics[1].

According to Prabhakar S *et al* [2] a biometric system is essentially a pattern- recognition system that recognizes a personal feature vector derived from specific physiological or behavioural characteristics that the person possesses. The term ‘biometrics’ is derived from the Greek words bio (life), and metric (to measure). Therefore, biometrics refers to technologies for measuring and analyzing a person’s physiological or behavioural characteristics[3]. These characteristics are unique to individual, and therefore, can be used to verify or identify a person

Biometrics is a characteristic and a process. As a characteristic, it is a measurable biological (anatomical and physiological) and behavioural characteristics that can be used for automated recognition. It is a process because it encompasses automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics[4].

A biometric typically operates in one or two modes: Verification or Identification. In Verification mode, the system validates a person’s identity by comparing the captured biometric characteristic with the individual’s biometric template which is pre-stored in the system database. In an identification mode, the

system recognizes an individual by searching the entire template database for a match[5].

According to National Security Agency (n.d), there are three steps involved in operation of a biometric system. The first step in the process involves an observation, or collection, of the biometric data[6]. This step uses various sensors, which vary between modalities, to facilitate the observation. The second step converts and describes the observed data, using a digital representation called a template. This step varies between modalities and also between vendors. In the third step, the newly acquired template is compared with one or more previously generated templates stored in a database. The result of this comparison is a 'match' or a 'non match'.

The examples of different biometrics are; Face, Voice, Palm print, Hand Geometry, Iris, Retinal Scan, DNA Signature, Gait and Keystroke[4]. The fingerprint was the biometric implemented in this study.

According to Jain AK *et al* [8] fingerprint matching is one of the most commonly used algorithm for extracting features that characterized a fingerprint. The different minutiae feature locations and types can identify different individuals. Evidence suggests that fingerprints were used as a person's mark as early as 500 BC and early Chinese merchant transactions and to differentiate children (Biometric Technology Introduction n.d) Fingerprint Identification is perhaps the oldest of all the biometric techniques. Fingerprints were used in the old china as a means of positively identifying a person as an author of documents. Their use in law Enforcement since the last century is well known. The Finger print technologies had the greatest potential to produce the best identification accuracy.

It has undergone an extensive research and development since the seventies [9]. The fingerprint involved obtainance of fingerprint through traditional method or optical fingerprint readers can be used. The fingerprints processing would then follow. Fingerprints matching techniques can be placed into two categories: Minutiae-based and correlation based. Minutiae-based techniques find the minutiae points first and then maps their relative placement on the finger. The correlation based method is also used. The correlation based techniques require the precise location of a registration point and are affected by image translation and rotation [9].

All biometrics are used to serve some purposes. Biometrics are used in National security, Enterprise and e-government services and personal information and business transactions. They can be used in terrorist identification, parenthood determination and missing children. Police also use fingerprint in crime investigation in crime scene forensics and to identify wanted criminals[10].

The biometric study (Fingerprint) conducted in this study aimed at identifying those who play truancy and impersonate others in educational organization.

RESEARCH METHOGOLOGY

In System Engineering, Use case is a description of the behavior of the system as it responds to a request that originates from outside of the system[11]. It describes series of actions that a system performs which yields observable results of value to the actor.

The UML-Use Case Diagram was used as the designed model and it shall take into consideration all the components in the system.

The Goal of the content: it used in order to curb impersonation and truancy, by allowing the staff in an organization to capture their entire fingerprints daily for attendance records keeping.

Scope of the System: Finger print as biometric is used to capture staff daily attendance.

The Actors: The entire staff and the Administrator.

The Staff: This refers to the employees in the organization, that must capture their fingerprints on resumption at work.

Register: This is a page where all the entire staff creates their account and even when new member of staff is being employed.

Staff Enrolment: This is a page where the entire staff needs to enroll for Finger capture. Each staff member is mandated to capture his/her finger finger.

Log in: The staff on resumption at work, go to the admin office to Log In into his/her account (User Login) by entering Username, Password and Title (designation) and clicks OK and Exit.

Finger Print Page: After the Log In page, the fingerprint page is brought forward showing Time In, Staff Id, Name, Department and where to place finger to be captured. The staff places his/her finger on the sensor to be captured. Once captured, the staff attendance is taken for the day.

The Administrator: This is second actor and his/her functions is to prepare the computer system and to control the Staff Log In.

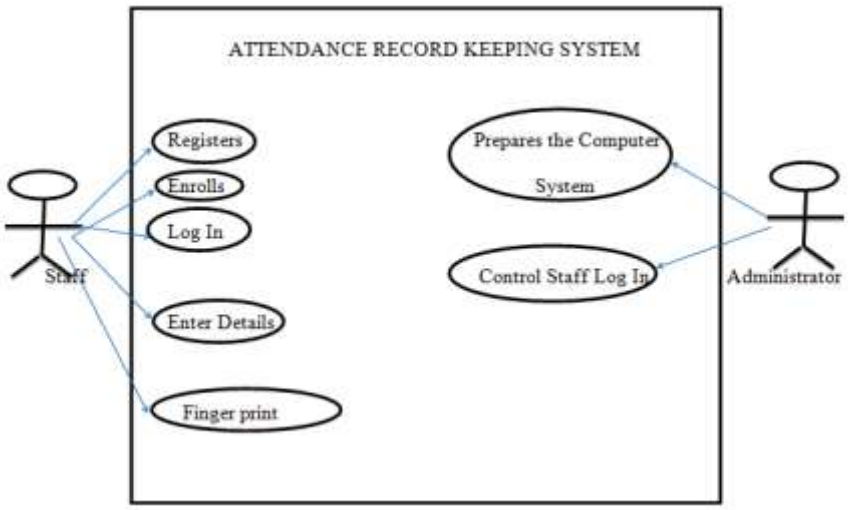

Fig-1: UML-Use Case Diagram

PRINCIPLE OF BIOMETRICS

Biometric devices have a scanning device's software that converts the information gathered into digital form. It has a database that stores the captured data and compares it with previously stored data. When converting the captured input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data in the database. All Biometric authentications require comparing an enrolled biometric sample, that is, biometric template against newly captured biometric sample.

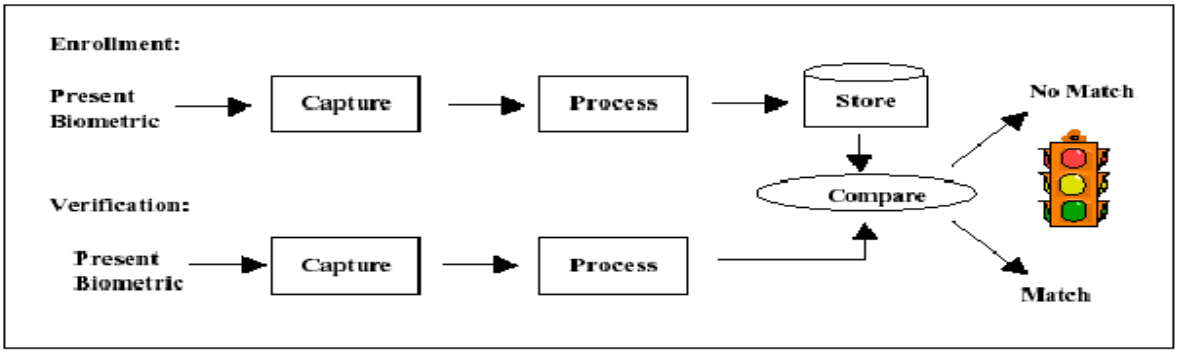

Fig-2: Basic Structure of A Biometric System

IMPLEMENTATION

Fig-3: Registration Page

Registration Page is where the entire staff registers their details or data once employed. Any newly employed staff is also bound to register his/her detail here.

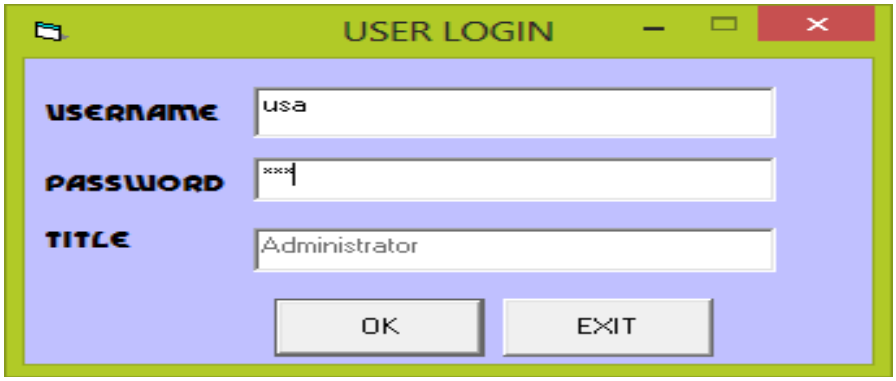

Fig-4: User Log In Page

This page shows the user Log In page where each member of staff will enter his/her name, password and job designation, and then click OK and Exit

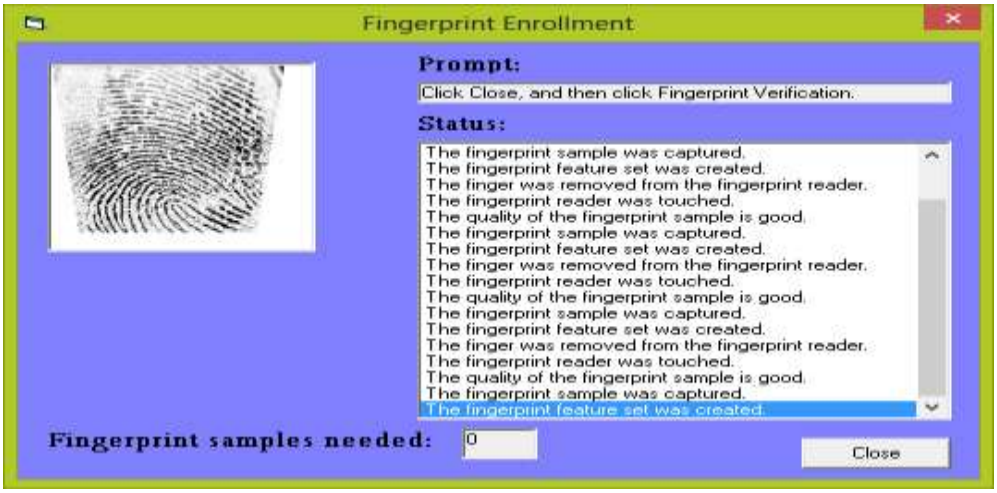

Fig-5: Sample of Enrolment Page

Enrollment Page is a page where the entirely staff's fingerprint is registered. Each member of staff is mandated to register their fingerprints so that their finger print can be stored.

Fig-6: Attendance Page

The Attendance Page is where staff's finger print is captured each day, after entering the other details or data in the page in order to take his/her attendance.

CONCLUSION AND RECOMMENDATION

Truancy and impersonation could lead to wanton damage to the organization goals and objectives. Educational institutional goals may be jeopardize by truancy. Truancy may reduce the staff productivity as a result of many work days being lost to truancy. Academic staff may not be able to cover the entire curriculum of study for each of the courses taught in the school. This may affect the academic quality of the school. Moreover, truancy, when not checked, is an injustice to the educational system. Staff collects salaries they did not actually work for. Impersonation, especially among the staff during seasonal auditing, has led to a lot of irregularities in the work place. We conclude in this study that the application of fingerprint biometrics would, undoubtedly, curb the truancy and impersonation problems in the institution of higher learning studied in this research work. It is recommended, therefore, that its application should be embarked upon and properly monitored by the school management for optimum results. The study also recommends the application of the same in every organization in Nigeria, i.e. Manufacturing Industries, Companies and Government Ministries. We are of the opinion that this would reduce the rate of truancy and impersonation, if well implemented.

REFERENCES

1. Jaiswal S, Bhadauria SS, Jadon RS; Biometric: Case Study. Journal of Global Research in Computer Science, 2011; 2(10):19-48.
2. Prabhakar S, Pankanti S, Jain AK; Biometric recognition: Security and privacy concerns. IEEE Security & Privacy, 2013; 1(2):33-42.
3. Thakral G, Cooper M; Passenger Acceptance: Fingerprint Scanning Vs Iris Scanning, 2004.
4. Jain AK, Ross A, Prabhakar S; An introduction to biometric recognition. Circuits and Systems for Video Technology, IEEE Transactions, 2004; 14(1):4-20.
5. Jain AK, Flynn P, Ross AA; Handbook of biometrics. Springer. 2007.
6. Roy B; Case against Biometric National Identification Systems (NIDS): Trading-off Privacy without Getting Security, A. Windsor Rev. Legal & Soc, 2005; 19: 45.
7. Maltoni D, Maio D, Jain AK, Prabhakar S; Handbook of fingerprint recognition. springer. 2009.
8. Jain AK, Hong L, Pankanti S, Bolle R; An identity-authentication system using fingerprints. Proceedings of the IEEE, 1997; 85(9):1365-1388.
9. Matyáš Jr, V; Biometric authentication systems. 2000. In verfügbar über: http://grover. informatik. uni-augsburg. de/lit/MM-Seminar/Privacy/riha00biometric. pdf.
10. Daugman J; Face and gesture recognition: Overview. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1997;19(7):675-676.
11. Folajimi YO, Ojo AI; Towards Increasing Students' Performance In Multiple Choice Examinations: An Adaptive Web Based Quiz System. Afican Journal of Computing & ICT, 2012; 5(5).