www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21448-21458
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.43

Staff Monitoring System Using Biometric

Joseph Elijah[1], Dr. Amit Mishra[2], M. Usman Gana[3], Engr. Mathew Chukwu Udo[4], Prof. Abiodun Musa Aibinu [5]

[1, 2, 3] Department of Mathematics/Computer Science Ibrahim Badamasi Babangida University Lapai, Niger State Nigeria
[5] Department of Mechatronic Engineering, Federal university of Technology, P.M.B 65 Minna, Nigeria.
[4] Huawei Technologies Co. Nig. Ltd, No. 4 Lekki Road, Oriental Hotel Building II, Victoria Island, Lagos Nigeria.

ABSTRACT:- Millions of naira is been lost annually in organizations across Nigeria as a result of poor services been rendered to various clients in organizations, this is due to the facts that proper attendance management system is not in place in various organizations across the country. The management of staff's attendance record daily has become a difficult challenge. The effort required in generating monthly report and also knowing the cumulative numbers of staffs has become a major task as manual assessment produces errors, and also it is time consuming. For the stated reason, an effective electronic staff attendance system using fingerprint is introduced in this work. This system will take attendance electronically with the aid of a fingerprint scanner (fingerprint device) and the attendance records are stored in the application storage unit (database). Attendance is marked after staff identification. For identification of staff, a fingerprint scanner is used. This process eradicates the need for stationary materials for record keeping; this will eliminate the issues of impersonation. This paper proposes the use of fingerprint biometric system to eliminate the problem being faced by traditional paper and pencil attendance register being provided in organizations.
Keyword: Fingerprint, Biometric, Staff.

Introduction

Employee management is very vital in the administration and management of organizations. Increase in security breaches and transaction fraud in an organization are so negatively alarming that many organizations resort to utilizing personal verification and employee identification technologies. Fingerprint has been defined by Francis (2009) as the traces of impression from the friction ridges on the end of our fingers. Humans have various classifications of finger prints. According to Francis (2009), there are three classes of finger prints which are; loop, arc and whorl. Humans have been hitherto using fingerprints for personal identification, this have been very crucial in crime detection using forensic approaches for more than 400 years. It has been an established fact that no two individuals have the-same finger prints even identical twins and the prints of any individual remains unchanged throughout life. Therefore, the fingerprints validity serves as a basis for personal identification because this will overcome the limitations of the existing system where one person can sign for another. Using this system, No one can thump print for another. Finger prints are very unique feature in nature and that is why they are consequently utilized in personnel identification and verification (Francis, 2009).

For an organization to function effectively, it has to ensure proper record of attendance of personnel or employees be it an educational or financial institution. Using Ibrahim Badamasi Babangida University Lapai, Niger State Nigeria (IBBUL) as a case study, managing attendance records of staff (non-academic) of an institute is a herculean task. It is time consuming and it is difficult to ascertain the cumulative numbers of staff. To design a better attendance management system for staff so that records will be maintained with ease and accuracy was an important key behind initiating this project. This would improve accuracy of attendance records because it will save valuable time of the staff as well as registry unit in time of compilation and monthly report generation. There is a need for a system that would eliminate all of these limitations of the existing system.

Bowman, E. (2000) asserts that biometric technologies are "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic". Automation mechanisms can be categorized in two dimensions:

1. Mechanisms for scanning
2. Mechanisms for processing or comparing unit and an interface with different application systems.

Identification is the process of selecting characteristics from a group of stored template images; this produces a list of possible or likely matches. The identification system format includes fingerprint, iris, facial and retinal. To have an effective identification security, biometric identifications are extensively used from arrays of highly secure identification and personal verification solutions. This is because biometric system provides complete authentication as against the other identifications solutions. Authentication using finger prints has been in use for a long period of time and has more priority than other biometrics.

The Federal Bureau of Investigation (FBI) in 1924 compiled about 250 million finger prints files for the purpose of crime detection and forensic investigation and also the identification of unknown casualties. It is widely used in various disciplines of studies such as financial, medical, e-commerce and customer application as a secure and effective authentication method. In this work, the development of a staff monitoring system using fingerprint as a biometric identification and verification technique is proposed.

I. LITERATURE REVIEW

One of the most exciting technical improvements of recent history is biometric authentication. It set to change the way in which the substantial number of individuals live, for many businesses to succeed squarely, security is the most important factor to consider and that is the reason why personal authentication has become very crucial than ever. Because of the rising issue of authentication and security breaches, businesses have imbibed the use of biometric systems for personal authentication. Finger print recognition is the most versatile and universal means of biometric authentication.

A. DEFINITION OF BIOMETRIC

The term biometrics comes from the Greek words bios, meaning life, and metrics, meaning measure. Biometrics can be defined as measurable physiological and/or behavioral characteristics that can be utilized to verify the identity of an individual, and it include fingerprint verification, hand geometry, retinal scanning, iris scanning, facial recognition and signature verification (Ashbourn J. 2000).

B. BIOMETRIC AUTHENTICATION

Authentication using biometric is regarded the automatic identification, or identity verification, of an individual using either a biological feature they possess (physiological characteristic like a fingerprint) or something they do (behavior characteristic), like a signature (Wayman and Alyea., 2000). Practically, the process of identification and authentication is the ability to verify and confirm an identity. It is accomplished by using any one or a combination of the following three traditional identification techniques: something you possess; something you know; or something you are (Ashbourn J., 2000).

TRADITIONAL IDENTIFICATION TECHNIQUES

- **Something you possess:** often referred to as a token and can be produced from a multitude of different physical objects. There are two basic types of tokens in use today: manual and automated. If a token is described as manual it means that the identification process requires some form of human intervention; in other words, a person will make the final decision of whether an identity is approved or not. Good examples of manual tokens are paper ID documents and passports. Automated tokens, on the other hand, do not involve human intervention in the identification process, but rather the identity is verified by a system/computer such as magnetic-stripe cards, memory cards, or smart cards (Ashbourn, J., 2000).
- **Something you know:** the knowledge should not be commonly held, but secret. Examples of regularly used secrets are passwords, pass-phrases, and personal identification numbers PINs.
- **Something you are:** recognizing an entity through what "they are" requires measuring one or more of their biological features. Biological features can be either physiological characteristics like fingerprints or behavioural traits like an individual's signature (Ashbourn, J. (2000), Wayman and Alyea 2000).

Table 1: shows the major limitations of traditional identification techniques, these include tokens, passwords and biometric.

Tokens	- Can be forged and used without the knowledge of the original holder. For example, a forger can "steal an identity" and create a fake ID document using another person's information. - Can be lost, stolen or given to someone else.
Passwords	- Can be obtained or "cracked" using a variety of techniques such as using programs/tools to crack the password. - Can be disclosed. If the password is disclosed to a person they will be able to gain access to information for which they are not authorized.

	- Can be forgotten which will place a further burden upon an organization's administration.
Biometrics	- Cannot be forged (Prabhakar, et al., 2003). - Can be destroyed, and a biometric characteristic's ability to be read by a system can be reduced. An individual's fingerprints, for example, can be affected by cuts and bruises and can even be destroyed by excessive rubbing on an abrasive surface (Tiwana, A., 1999). Also, Accuracy of Biometrics depends mainly on the software that is dealing with them.

Table 1: Major limitations of traditional identification techniques.

C. BIOMETRIC CHARACTERISTICS

According to Ashbourn J. (2000), biometric characteristics can be separated into two main categories; namely physiological characteristics and behavioral characteristics.

1. Physiological characteristics are related to the shape of the body. The trait that has been used the longest, for over one hundred years, are fingerprints; other examples are face recognition, hand geometry and iris recognition.

2. Behavioral characteristics are related to the behavior of a person. The first characteristic to be used that is still widely used today is the signature.

Generally, physical and behavioral characteristics used by biometrics include the following taxonomy (Zhang D, 2000)

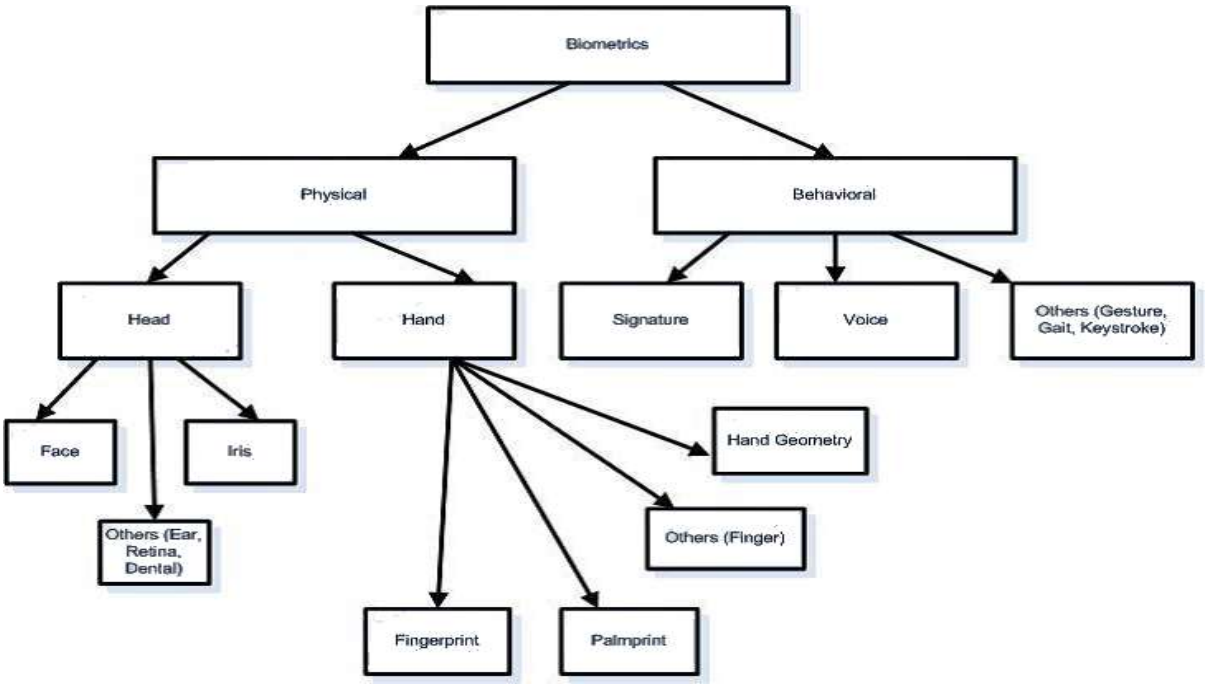

Figure 1: Physical and behavioural characteristics used by biometrics (Zhang D., 2000).

D. THE ACCURACY OF A BIOMETRIC SYSTEM

The Biometrics system accuracy is measured by:

1. False match or acceptance rate (FMR): the lower the biometric identification system's FMR, the better the security. FMR means the rate at which the biometric measurements from two different individuals are mistaken to be from the same individual (Prabhakar *et al* 2003).

2. False non-match or rejection rate (FNMR): the lower the biometric identification system's FNMR, the easier the system is to use. FNMR means mistaking two biometric measurements from the same individual to be from two different individuals (Prabhakar *et al.*, 2003).

In summary, all biometric systems work in similar ways, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system (Allan A., 2002).

Allan A. (2002), provides a list of some of the strengths, weaknesses and suitable applications for each biometric methodology in figure 2.

DOI: 10.18535/ijecs/v6i5.43

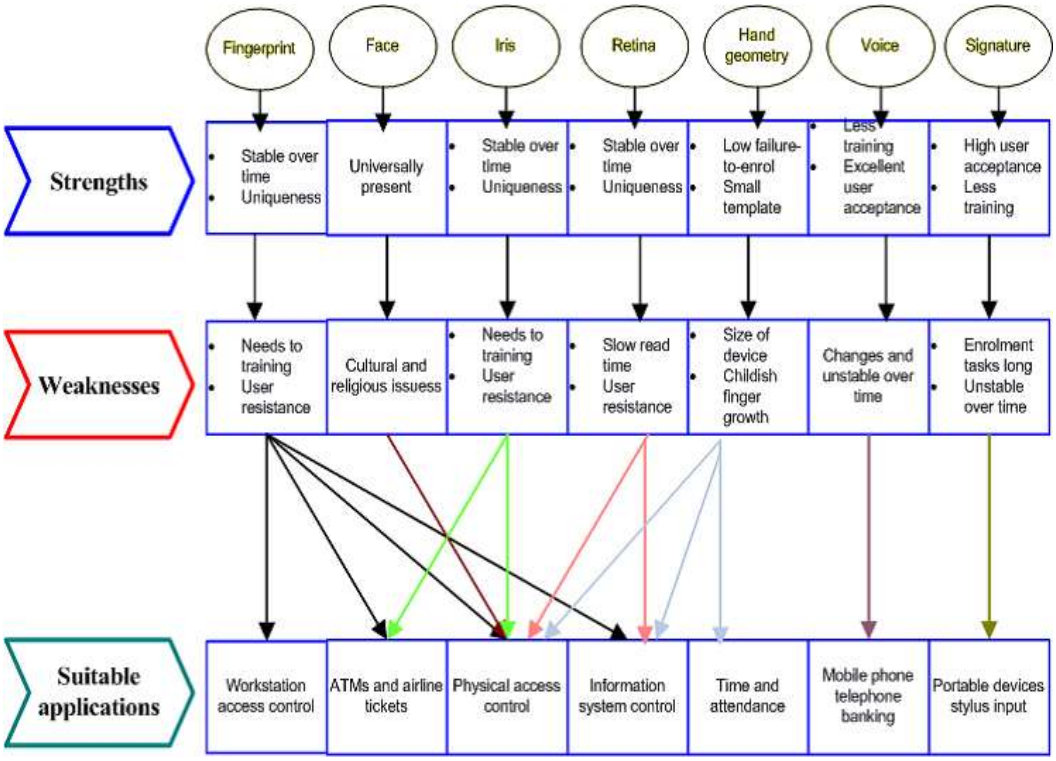

Figure 2: Strengths, Weaknesses and Suitable Applications. (Allan A., 2002).

There are several features of biometric that are in use in various applications today. Each biometric has its own strengths and weaknesses, and suitable applications for each biometric methodology. There are no particular biometrics which may successfully meet the requirements of all applications. Depending on the application's usage and the biometric characteristic's features we are able to suitably match a particular biometric to an application. Prabhakar *et al* (2003), assert that the fingerprint and iris-based technique have more accuracy compare to the voice-based technique. Nevertheless, in a phone banking application, the voice-based technique might be preferable as the bank could integrate it seamlessly into the existing telephone system.

E. FINGERPRINT AUTHENTICATION

According to Prabhakar *et al*, (2003) fingerprint-based identification is the oldest method which has been successfully used in numerous applications. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The pattern of ridges and furrows as well as the minutiae points can determine the uniqueness of a fingerprint. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

Fingerprinting is the oldest method of successfully matching an identity. A person's fingerprints are a complex combination of patterns known as lines, arches, loops and whorls (Biometric Technology, Inc, 2002). The most distinctive characteristics are the minutiae, the smallest details found in the ridge endings. Fingerprints cannot be forged and every individual has a unique print. Fingerprints have some advantages such as the prints remain the same throughout a person's lifetime, the fingerprinting is neither frightening nor emotionally disturbing and people's prints are unique. Fingerprints also have some disadvantages. There are searching through a huge database can be rather slow, dirt on the finger or injury can blur the print, a fingerprint template is rather large compared to other biometric devices.

On the finger is not encoded in the genes of an individual. Thus, fingerprints represent a stronger authentication mechanism than DNA. Fingerprints also remain as one of the most accurate biometric modalities available to date with jointly optimal FAR (false accept rate) and FRR (false reject rate). Erikson M. (2001), assert that most fingerprint verifications systems use minutiae matching point. Minutiae points are the points in a fingerprint image where the fingerprint ridges either or split up into two new ridges. Other than using the minutiae matching point, image matching and ridge-pattern matching method also can be used in verifications systems. According to some manufacturers, image matching is more secure than the minutiae matching but it is not the general opinion. According to other expertise, minutiae point matching is the fastest, simplest and most robust method available.

Fingerprints were one of the first biometrics to be adopted and have become synonymous with reliable personal identification. Among other biometrics technology, fingerprint has several advantages such as its universality, high distinctiveness and high performance. In universality, large majority of the human population has legible fingerprints

and can easily be authenticated. Because of its high distinctiveness, twins who share the same DNA have been shown to have different fingerprint since the ridge structure. Figure 3 Show the sample of a ridge structure.

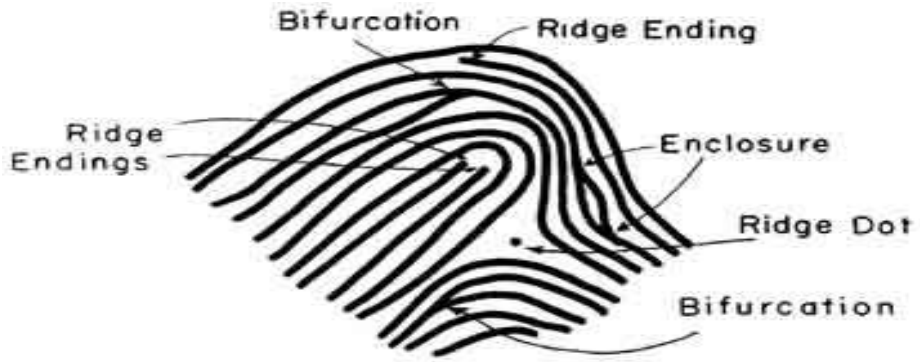

Figure 3: Minutia sample structure

i. UNIQUE FEATURES OF THE FINGERPRINT

Francis (2009), assert that fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the epidermis on the palmar, that is palm and fingers or plantar (sole and toes) skin, consisting of one or more connected ridge units friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal papillae".

ii. FINGERPRINT PATTERN

There are a numerous strategies through which fingerprint identification can be done, among which verification through minutia points is the simplest and easiest method. According to the current most widely used Galton–Henry system, the fingerprint is divided into five classifications. These are arch, tented arch, left loop, right loop and whorl.
(i) Arch: Fingerprint lines start from side of the finger and end at the other side, do not return and on the core points and delta point.
(ii) Tented Arch: Like an arch fingerprint, but graphic Center upward rise in the vertical direction, equivalent to a core and a delta on the same vertical line.
(iii) Left Loop: Circular pattern that is fingerprint lines access from one direction then back from the same direction after a rotation around. To the left is Left Loop. There is a core and a delta at the lower left.
(iv) Right Loop: To the right is Right Loop. There is a Core and a delta at the lower right.
(v) Whorl: At least one fingerprint stripe rotate into a closed curve around the center, there are two core points in center, a triangular point on each side when the cores are not in the same vertical line.

Figure 4: Examples of fingerprint recognition (Francis, 2009).

The minutia based algorithm is widely used for fingerprint authentication. It focuses on the endings of ridges and bifurcations. Consequently the central area in fingerprint image is very important and this algorithm keenly relies on the quality of the input images. Global and local characteristics of fingerprints are used for identification of individuals (as shown in figure 4). Global features are the ones that can be seen with naked eye like ridges, pattern area and delta while local characteristics are the minutia points.

iii. MINUTIAE FEATURES

The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges.

Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint (as depicted in Fig 5). Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

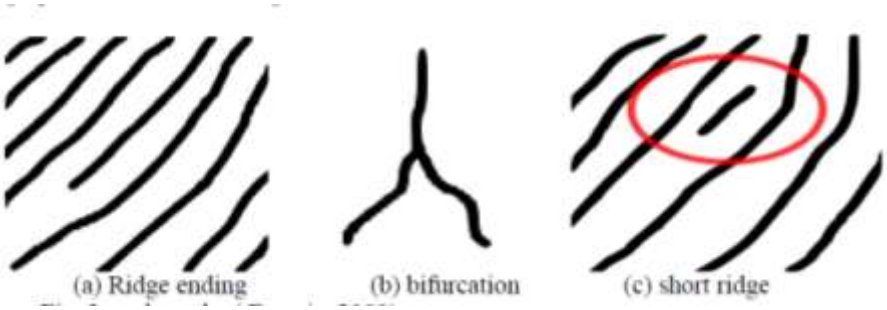

Figure 5: Ridge ending, bifurcation and short ridge diagrams respectively (Francis, 2009).

The minutia based algorithm is widely used for fingerprint authentication. It focuses on the endings of ridges and bifurcations. Consequently the central area in fingerprint image is very important and this algorithm keenly relies on the quality of the input images. Global and local characteristics of fingerprints are used for identification of individuals. Global features are the ones that can be seen with naked eye like ridges, pattern area and delta while local characteristics are the minutia points. Fingerprint ridges are not continuous as there are a number points at which ridges change and end and these points are called minutia points. The unique identifying features are provided by these minutia points. A raw image is taken from the sensor and algorithms are implemented on the image to enhance it and further extract the minutia points directly from this representation. This procedure provides a much more efficient and reliable result as compared to other methods of fingerprint verification.

iv. FINGERPRINT MATCHING

According to Francis (2009), Fingerprint matching is the process used to determine whether two sets of fingerprint come from the same finger. One fingerprint is stored into the database and other is employee's current fingerprint, as shown below.

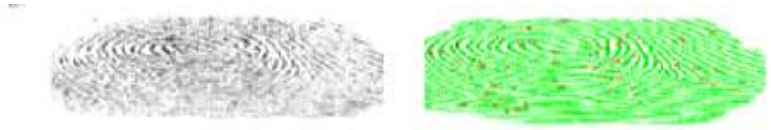

Figure 6: Fingerprint Matching, (Francis, 2009).

The use of fingerprint for human identification and verification has been in use for a long time, because of its unique features. Many scientists have researched and proved that each individual has his own unique fingerprint and therefore the best means of human identification and verification.

F. RELATED WORKS

A number of related works exist on the application of different methods and principles to effectively monitor the attendance of human.

Attendance Management has been carried out using attendance software that uses passwords for authentication. Cheng, Xiang, Hirota, and Ushijimaa (2005), designed and implemented a system that authenticates the user based on passwords, this type of system allows for impersonation since the password can be shared or tampered with. Passwords could also be forgotten at times thereby preventing the user from accessing the system.

Other attendance solutions are RFID-based student attendance system and GSM-GPRS based student attendance system. These are all device-based solutions. While GSM-GPRS based systems use position of class for attendance marking which is not dynamic and if schedule or location of the class changes, wrong attendance might be marked. Problem with RFID (Shoewu and Badejo, 2006) based systems is that students have to carry RFID cards and also the RFID detectors are needed to be installed (Pankanti *et al*., 2002).

The developed system, however, is a cost effective simplified system that uses fingerprints for identification. The fingerprint is unique to each individual and cannot be shared. It allows staffs to register for attendance with ease and

eliminate errors that are associated with attendance reports because the system generates reports at the end of the day, week, month, semester or session.

II. RESEARCH METHODOLOGY

This research work is based on the design and implementation of staff attendance system using fingerprint identification technique. The developed system can be used to monitor, identify and check the IN and OUT timings of non-academic staff in IBB University. The system requires that all non-academic staff enroll his/her fingerprint for the device to identify and verify if he is a valid staff and also to record daily resumption and closure timings for the staff for a whole month. The primary idea behind this is to avoid a situation where staff records fake timings in the manual register. This greatly affects output to input ratio of staffs and in earnest the institution as a whole. This design enhances compilation of each staff's attendance by remote workstations, which are then sent to the central database server. The result of each staff clocking in and out timing is captured via a fingerprint device at each terminal and stored in the central database server. Each Department remote terminal is interconnected to the central database server via a shared network.

III. ANALYSIS OF THE EXISTING SYSTEM

In Ibrahim Badamasi Babangida University Lapai, attendance management of staff is done manually through the use of sheet of papers and pen for registering (signing In/Out) at the registry unit of the admin. This method of attendance system is referred as the tradition method of attendance management, with various limitations and reduced the net productivity of the institution.

a. LIMITATION OF THE EXISTING SYSTEM

Using IBBU Lapai as case study, the traditional attendance system leads to improper management of staffs and has result to lower productivity in the institution. This method could easily allow for body clocking (impersonation) and the attendance sheet could be stolen or lost. Some of the limitations of the manual attendance system are:

- Improper use of staff by the institution
- Complexity and difficulty in report compilation: this system requires more computation in generating the report due to unordered listing of the staff's record.
- Work done manually: All computations in terms of report generating are done manually which may lead to greater error chances.
- Require much paper work: the existing system required a lot of paper work and also missing of a single register may lead to difficulty in compilation since all the papers are needed in compiling the report.
- Inefficiency: the existing system requires much time since the entire compilation of report is done manually which result to lateness in compilation of report in a month, semester or session.
- Space consuming: In terms of documentation the existing system requires large store for storage of the registers.
- Duplicate entry: Possibly due to lack of staff concentration, entering of data can be duplicated in the same page of the registry.

b. FUNCTIONAL MODEL OF STAFF BIOMETRIC ATTENDANCE SYSTEM

UML Use Case diagram for staff biometric attendance system is shown in figure 7; the various participants in the system are also detailed.

Actors: Database administrator, non-academic staffs

Non-academic staff: mark attendance, In-time, out-time.

Administrator: Keep track of attendance; generate monthly attendance summary, and reports to the Faculty or administrative unit.

DOI: 10.18535/ijecs/v6i5.43

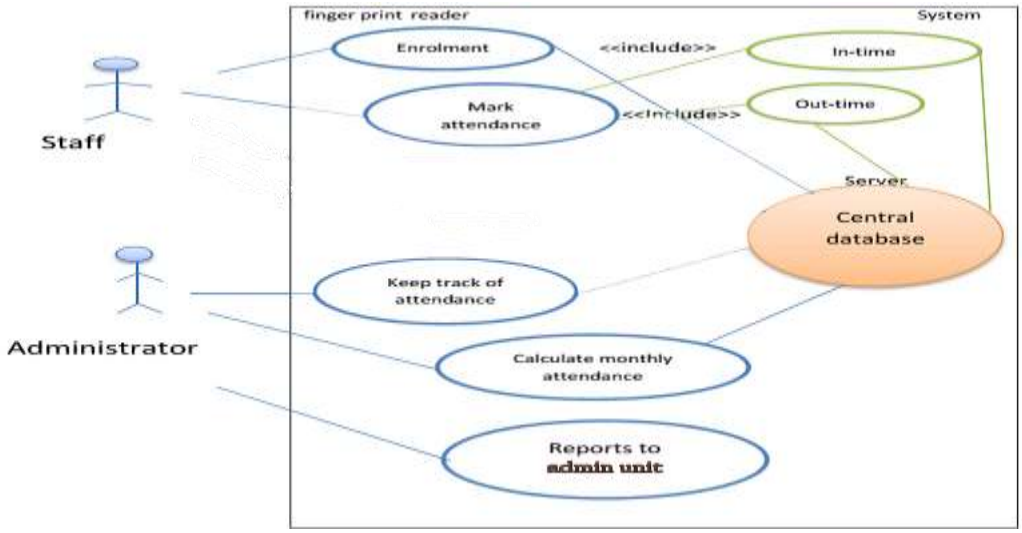

Figure 7: Use case diagrams for staff biometric attendance system

c. THE SYSTEM DESIGN OBJECT MODEL

In figure 8, the object model is represented using UML technique with class diagram; these describe the developed system (staff attendance system) structure in terms of objects, attribute, relations (associations), and methods (operations). The developed system (staff attendance system) class diagram describes the system in terms of classes, attributes, operations, and their associations as shown in figure 8. In UML, classes and objects are represented in three compartments, each in box format. The upper unit displays the name of the class or object. The center unit displays the attributes of the class or objects, and the bottom unit displays the operations of the class or objects, and the bottom unit displays the operations of the class or objects (Dan and Neil, 2005).

Figure 8: Class diagram for staff attendance system

IV. DISCUSSION OF RESULT

The developed system (staff attendance system) is an electronic attendance system. This system was implemented using Microsoft Visual Basic Dot Net programming language. It involves the interaction with the central database which contains all records of non-academic staff of the faculty or institution as well as records of monthly attendance taken. In implementing this system, certain criteria are considered. These criteria include: Only eligible non-academic staffs of the institution can enroll and take attendance. Similarly, no one can take attendance for another. The records of each attendance taken can be retrieved as well as the monthly summary attendance for all staff can be generated and viewed. Furthermore, there is a period of grace within which IN and OUT timings can be taken. The design requirements are met through the use of a fingerprint reader which captures the fingerprint of users and desirable results are achieved, some of which are discussed in this section.

DOI: 10.18535/ijecs/v6i5.43

V. PERFORMANCE EVALUATION

The management of staff attendance system (SAS) is done under the administrative unit, therefore to evaluate the performance of staff SAS the admin has to log in to the administrative unit for enrolment and registration operation. The staff fingerprint as well as bio data is stored into the database for the first time through the registration unit (add/manage staff). As all the necessary data and information required for proper attendance record are enrolled. The staff clicks on fingerprint scanner icon for attendance taking, then the staff places his/her fingerprint on the fingerprint scanner; the identification unit of the finger compares the features of the fingerprint with those stored in the database. The possible cases observed are:

Fingerprint Match: The fingerprint features captured are matched with the fingerprint templates stored in the database of the application (SAS). The student is automatically assessed for the day attendance. A notification box is trigger in a short time interval to show that the student has been recorded for the attendance. Figure 4.8 shows a snapshot of the program.

Figure 9: A snapshot of Fingerprint Match

Fingerprint non-match: the student fingerprint is not match with the stored fingerprint template a message is triggered on the screen showing that fingerprint is not found. The interface sample is shown in Figure 10.

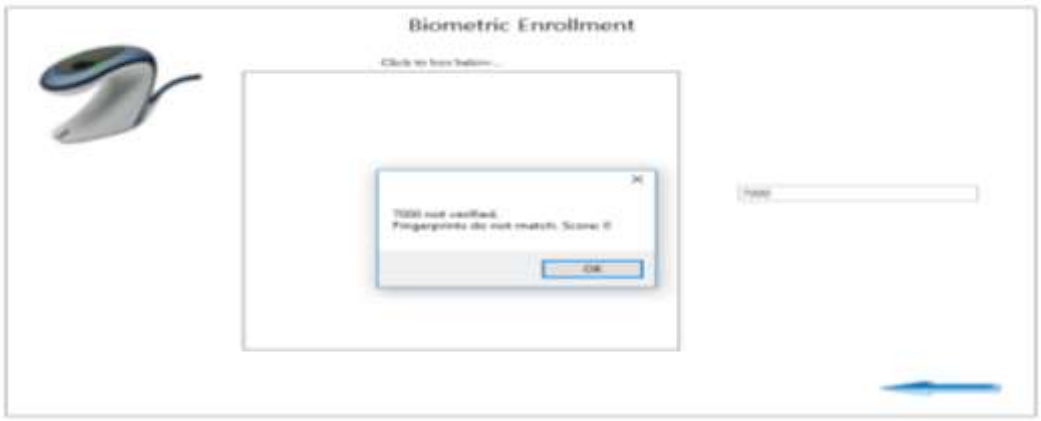

Figure 10: A snapshot of Fingerprint Non Match

Reports are generated for each staff and the total number of staff for each attendance is listed and their corresponding attendance record. The result of the test shows that the system is effective and efficient. There was no false identification of staff, limited number of false reject which was accepted later and only pre-registered staffs were authenticated. The matrix of the identified staffs was enrolled for attendance automatically.

The evaluation of the system was done using the student's bio-data and fingerprints received from eighty (80) industrial training students under department of Computer Engineering in Logic Gate Company Minna, Niger State. During the test there was no false acceptance, meaning a person that was not pre- registered was not falsely enrolled for attendance and also there were a few false rejections in which the system failed to recognize few pre- registered students. The result of false rejections could be due to improper placement of the finger on the scanner and possibly due to slight scar on the finger as a result of heal injury.

DOI: 10.18535/ijecs/v6i5.43

The 80 students are sub divided into 8 groups due to the limitation of the U are U SDK, 10 students in each group using different systems (PC). A success rate of over 94% was obtained from the tests carried out. The test results are shown in chart format in figure 11

Groups	1	2	3	4	5	6	7	8
Success (%)	100	90	100	100	80	100	90	100
Failure (%)	0	10	0	0	20	0	10	0

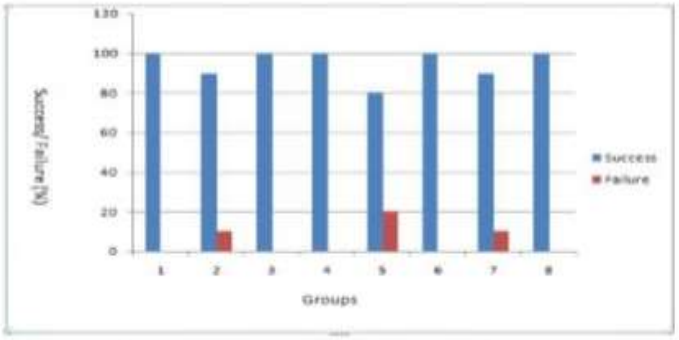

Figure 11: Comparison of success and failure rate chart.

VI. COMPARISON WITH MANUAL ATTENDANCE

The existing system of attendance estimated average execution time is approximately 17.83 seconds for eighty (80) students, as against 3.79 seconds for the new developed attendance system using fingerprint recognition. The new attendance system reports generation took approximately 30 seconds. Table 2 and figure 12 shows a table and graph sample of 25 students out of the 80 student tests conducted respectively. From the comparison, result is obvious that the developed attendance system using fingerprint authentication is more effective and efficient than the existing system which involves the use of sheets of paper.

STUDENT	MANUAL ATTENDANCE	ATTENDANCE SYSTEM
1	22.78	3.81
2	12.82	3.43
3	19.65	4.12
4	11.38	3.63
5	12.65	2.53
6	16.24	2..49
7	14.66	2.72
8	15.23	3.35
9	15.03	4.01
10	16.31	4.21
11	14.97	4.31
12	15.16	3.85
13	15.18	4.32
14	16.54	4.78
15	16.59	4.23
16	16.92	3.55
17	16.95	4.34
18	17.61	5.11
19	17.72	3.36
20	17.78	4.57
21	18.01	3.12
22	18.25	3.31
23	18.62	3.1
24	19.19	2.92
25	19.34	2.83

Table 2: Comparison of execution time of the existing system and the developed system.

DOI: 10.18535/ijecs/v6i5.43

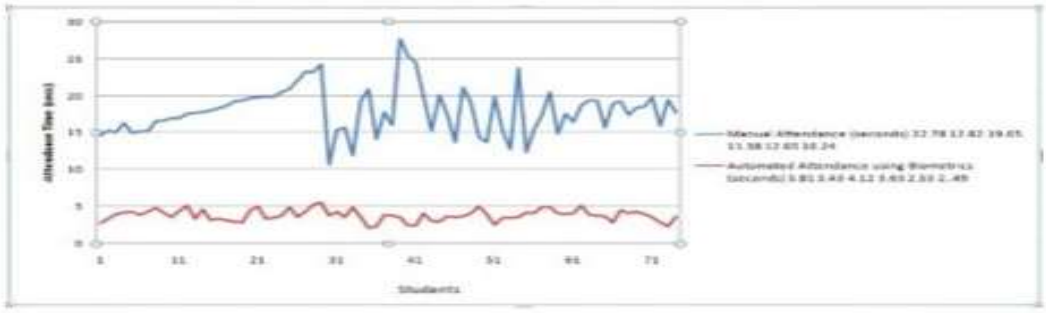

Figure 12: Comparison of execution time of the existing system and the developed system in graph format.

VII. CONCLUSION

Ultimately, since the inception of IBB University Lapai staff attendance has been taking manually, this involves lots of paper usage and pen for registering. The implementation of an electronic biometric-based method of attendance management system for non-academic staffs in IBBU Lapai will greatly assist IBB University Lapai in improving the net productivity of the institution and there by prevents time-consuming processes in attendance registering. The staff attendance system will ease the activity of the registry unit of the institution in providing easy access to non-academic staff attendance information as well as easy monitoring of weekly, monthly, and semester or session attendance report.

The developed system has some important features such as reliability, efficiency, security, and is capable of substituting the traditional manual method (unreliable method) of attendance management in IBB University Lapai. This system ensures security of non-academic staff's records, eliminate impersonation and body clocking, provide efficient time utilization as well as mitigate the administrator effort in gathering staffs attendance records. The developed system can be improved through the integration of multimodal biometric technologies to provide more security for the staff attendance management system.

REFERENCES

ALLAN, A. (2002). Biometric Authentication. Perspective. Gartner Research, ID Number: DPRO-95808: p. 1-31.

Ashbourn, J. (2000). Biometrics: Advanced Identity Verification: The Complete Guide. Springer-Verlag, London: Springer. 201.

Bowman, E. (2000). Biometric technologies: "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

Cheng, K., L. Xiang, T. Hirota, and K. Ushijimaa (2005). "Effective Teaching for Large Classes with Rental PCs by Web System WTS". *Pro. Data Engineering Workshop* (DEWS2005), 1D – d3 (in Japanese).

Dan, P. and Neil, P. (2005). *UML 2.0 in a Nutshell*. O'Reilly publication. ISBN: 0-596-00795-7.

Ericson, M. (2001). "Fingerprint verification systems ". farahanum bt masruni (2004219959).

Francis, G (2009). Fingerprint recognition McGraw-Hill Books. Inc: USA.

Pankanti, S., S. Prabhakar, and A.K. Jain (2002). "On the Individuality of Fingerprints". *IEEE Transaction on Pattern Analysis and Machine Intelligence*. 24(8).

Prabhakar, S., S. Pankanti, and A.K. Jain (2003), Biometrics Recognition: Security and Privacy Concerns. IEEE Security & Privacy 1(2): p. 33-42.

Shoewu, O. and O. Badejo (2006). "Radio Frequency Identification Technology: Development, Application and Security Issues". *Pacific Journal of Science and Technology*. 7 (2):144-152.

Tiwana, A. (1999). Web Security. Digital Press An imprint of Butterworth-Heinemann.

Wayman, J.L. and L. Alyea (2000). Picking the Best Biometric for Your Applications, in National Biometric Test Center Collected Works. National Biometric Test Center: San Jose. p. 269-275.

Zhang, D. (2000). Automated Biometrics: Technologies and Systems, Norwell, MA: Kluwer Academic Publishers. 331.