IMPACT: International Journal of Research in Business Management (IMPACT: IJRBM)
ISSN (E): 2321-886X; ISSN (P): 2347-4572
Vol. 4, Issue 2, Feb 2016, 65-78

TOWARDS AN EFFICIENT BIOMETRIC EMPLOYEE ATTENDANCE SYSTEM

AFOLALU, C.A., TOPE-OKE, A & ATSADU, S

Afe Babalola University, Department of Physical and Mathematical Sciences, Ado-Ekiti, Nigeria

ABSTRACT

Biometrics has grown and is widely applicable to various works of life. It serves as a means of identification, verification, access control, crime control, among others. The distinctive feature of certain physiological characteristics such as fingerprint, face, retinal pattern, hand geometry, iris pattern, has made it possible to apply biometrics in all works of life. Institutions and organizations all over the world are beginning to take advantage of this technological innovation. This technological innovation will be an established channel that will support the new initiative of the Federal government of Nigeria to ensure effectiveness and efficiency among her working force most especially in Nigeria University system which is important for the enhancement and ensuring dedication to work, aids unbiased promotion of dedicated employees, increase productivity and above all enhance quality learning outcome.Although there already exist biometric attendance system in some developed nations around the world, but the use is very limited across establishments and institutions in Nigeria as manual signing in of employee on attendance using hardcopy notebooks is much preferred. Therefore this workidentifiedsome of the challenges to the existing system of manual attendance system such as. Inaccuracy in time record and proposed a tested prototype design that will improve upon the existing attendance systemin order to foster quality productivity Using Afe Babalola University as a case study.

KEYWORDS: Biometric, Employee Attendance

INTRODUCTION

Humans still remain the greatest and most invaluable asset to any organization in information gathering and task execution. And as such employees' effectiveness and promptness to work becomes paramount to the advancement of any organization which cannot be overemphasized [5]. Attendance is among the 10 employee work ethics most valued by employers. Attendance can be quantified and verified, and employers keep employee attendance and leave records. When employers check references, they may ask about attendance. Poor attendance testifies that an employee might be insensitive to co-workers, unaccountable for responsibilities and uninterested in organization's success[4]. Over the years, manual method of taking attendance such as attendance register, hand ruled books and handwritten signatures have been the order of the day in collecting attendance in most establishments in Nigeria. This manual process is time consuming for large organizations like the university community and such system is manipulative in nature.

According to Thomas Y, et al [4], Biometric time and attendance system has brought more precise system to measure group or individual's activities and attendance as well. This done when biometric attendance machine captures a unique biological/physical feature such as hand or finger print, iris pattern and sometimes even voice as a record for identity verification and allows one to perform something that you are authorized to do. Biometric time attendance machines also count employees' work schedule, like which employee did what, and at what time did he do it, etc.

Biometric attendance system is a foolproof technology to ensure the accuracy of attendance and is useful to the ones who deal with large number of employees and further uses the biometric feature of finger print to authenticate the claim of any enrolled employee. It also provides an efficient way for administrators to manage employee attendance record.

Brief Overview of Biometrics

The word "Biometrics" comes from the Greek words bio (life) and Metrics (to measure). Biometrics is automated method of recognizing a person based on a physiological or behavioral characteristic [7]. Among the features measured are:

Facial Recognition: This technology uses a digital video camera image to analyze facial characteristics such as the distance between eyes, mouth or nose. These measurements are stored in a database and used to compare with a subject standing before a camera.

Fingerprints: Fingerprinting or finger-scanning technologies is the oldest of the biometricsciences and utilizes distinctive features of the fingerprint to identify or verify theidentity of individuals.

Hand Geometry: this is a form of biometric that uses the shape of hand for authentication and verification of a person. A hand geometry reader measures a user's hand along many dimensions and compere those measurements to measurements stored in a file.

Iris Recognition: this is a method of identifying people based on unique patterns within the ring shaped region surrounding the eye, the iris usually have different colors with complex patterns that are visible upon close inspection.

In iris recognition, the identification process is carried out by gathering one or more detailed image of the eye with a sophisticated digital camera and then compere the iris pattern with images stored in a database.it is mostly used in security related applications.

Retina Pattern/ Scan: retina -scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier. Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina, Vein, and voice. Also the hand geometry and the voice recognition. Other biometric modalities include Gait, vascular and facial thermography

These above mentioned biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. It uniquely identify a person, replacing or supplementing traditional security methods by providing two major improvements: one is that personal biometrics cannot be easily stolen and two, an individual does not need to memorize passwords or codes. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information.

The Traditional systems to verify a person's identity are based on knowledge (secret code) orpossession (ID card). However, codes can be forgotten or overheard, and ID cards can belost or stolen, giving impostors the possibility to pass the identity test. The use of featuresinseparable from a person's body significantly decreases the possibility of fraud. Furthermorebiometry can offer user-convenience in many situationsas it replaces cards, keys, and codes. [12]. Any human

physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements; Universality; Distinctiveness; Permanence; Acceptability; Collectability; However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:Performance: This refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operationaland environmental factors that affect the accuracy and speed.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

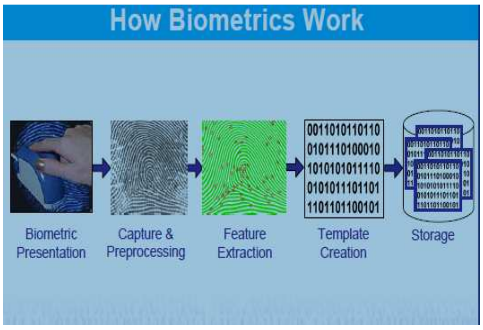

Figure 2: How Biometrics Work culled From: Www.Biometrics.Gov

The Fingerprint

In 1823, the Czech Jan Evangelista Purkinje was studying sweat glands in the hand and realized the grooves and depressions that these sweat glands opened up into seemed to be unique to each individual. In the late 19th century an extremely reliable method of categorizing and identifying marks in fingerprints was developed by Richard Edward. Henry of Scotland yard also made advancements on a fingerprinting method and that was first brought forward by Francis Galton in 1892, and conducted experimental tests in the 1890's. In the early 20th century, finger printing became the method of choice for police around the world. Today, fingerprinting is the biometric method most people associate when speaking ofbiometrics (www.biometrics.gov). Fingerprints are patterns created by the elevation of pores in lines, it is a pattern of ridges and furrows on the fingertip. Each individual has unique fingerprints. The uniqueness of each individual fingerprint is exclusively determined by the local ridge characteristics and relationships i.e. the ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprints, because of their uniqueness and other related characteristics, are the most widely used & highly accepted biometrics. The various parts of a fingerprint are shown below.[25]

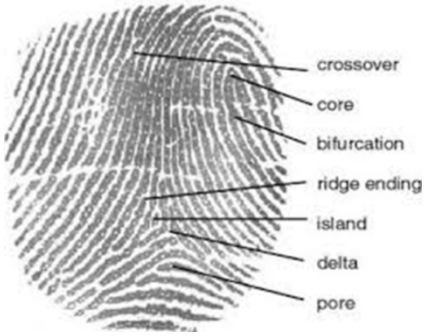

Figure 3: The Various Parts of a Fingerprint Culled from: www.biometrics.gov

Crossover or bridge – a short ridge that runs between two parallel ridges.

Core – a U-turn in the ridge pattern. Bifurcation – a single ridge that divides into two ridgesRidge ending – the abrupt end of a ridge. Island – a single small ridge inside a short ridge or ridge ending that is not connected to all other ridges. Delta – a Y-shaped ridge meeting.

There are several factors that can affect the quality of fingerprints images, these include; manual work, weather condition, contact of finger with sensor, greasy or dirty finger, cuts, wounds or bruises. All these have major or minor impact on the quality of fingerprint images. As such, the fingerprint algorithms procedure delivers the best match between the template fingerprint and query fingerprint for genuine verification and authentication of enrolled individuals. While fingerprint matching module computes a match score between two fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers.

Fingerprint scanning. According to Todd, (2002) Fingerprint scanning is the acquisition and recognition of a person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual.There are basically two different types of finger-scanning technology that make this possible.One is an optical method, which starts with a visual image of a finger and the other uses a semiconductor-generated electric field to image a finger. Both technologies will be employed in this research to get quality images. Fingerprint algorithms [9].An algorithm as a logical stepwise procedure for solving a mathematical problem in a finite number of steps often involving repetition of the same basic operation. The fingerprint algorithms are developed to arrive at a procedure that delivers the best match between the template fingerprint and query fingerprint for genuine verification and authentication of enrolled individuals. Fingerprint matching: [10], fingerprint matching module computes a match score between two fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers. Fingerprint matching is a difficult pattern-recognition problem due to large intraclass variations (variations in fingerprint images of the same finger) and large interclass similarity (similarity between fingerprint images from different fingers).

Intraclass variations are caused by finger pressure and placement—rotation, translation, and contact area—with respect to the sensor and condition of the finger such as skin dryness and cuts. Meanwhile, interclass similarity can be large because there are only three types of major fingerprint patterns (arch, loop, and whorl). Most fingerprint-matching algorithms adopt one of four approaches: image correlation, phase matching, skeleton matching, and minutiae matching. Minutiae-based representation is commonly used; primarily Minutiae-based representation is commonly used, primarily

becauseForensic examiners have successfully relied on minutiae to match fingerprints for more than a century. Minutiae-based representation is storage efficient.The current trend in minutiae matching is to use local minutiae structures to quickly find a coarse alignment between two fingerprints and then consolidate the local matching results at a global level. This kind of matching algorithm typically consists of four steps. First, the algorithm computes pairwise similarity between minutiae of two fingerprints by comparing minutiae descriptors that are invariant to rotation and translation.

Next, it aligns two fingerprints according to the most similar minutiae pair. The algorithm then establishes minutiae correspondence—minutiae that are close enough both in location and direction are deemed to be corresponding (mated) minutiae.

Finally, the algorithm computes a similarity score to reflect the degree of match between two fingerprints based on factors such as the number of matching minutiae, the percentage of matching minutiae in the overlapping area of two fingerprints, and the consistency of ridge count between matching minutiae.

STATEMENT OF PROBLEMS

Although biometric attendance system is not a relatively new area, the usage of this system is limitedmost government and private establishment still rely on manual attendance register which can be fooled by a third party(impersonation). In other measure employees' promptness effectiveness and efficiency at work place, there is need to grow in technological innovations. With this at hand, the present attendance system has the following challenges: Manual login of employee on attendance using hardcopy notebooks, Inaccuracy in time record,Less efficient and effective way of accessing employee dedication towards attending work, Lack of specific verification and authentication technique, It is a time consuming process.

The proposed system is intended to automate the previous system, where the process of attendance will be done with minimal use of pen and paper. It will embed the biometric feature of the finger print for authentication and verification. In this process, the employees' bio data will be enrolled in a database using the MySQL server, the data will contain name, staff number, department etc. Each employee's finger print will be enrolled and mapped to the stored data. On resumption, rather than write names and sign, employees will simply thumbprint on the available scanner and their data will be verified with what s on the database. If it matches any of the data, then the employee will be marked present for work at that time for the day.The system will restrict who accesses the database, make alterations, exempt employees who have notified they won't be able to come to work and in cases where the data cannot be retrieved due to damage on the finger, the staff umber of the employee will be used to access the employee's data. By so doing, the proposed system will simplify the process of attendance taking in Nigeria Universities. It will standardize attendance taking system to the present day increase accuracy in attendance taking. And also will minimize the cases of proxy attendance since it has a biometric verification feature at its core.

Objective of the work: The aim of this work is to analyze the necessary requirements and design a biometric employee attendance system using the finger print model which will enable storage of employee's bio data and verified to generate periodic report when requested.

METHODOLOGY

The methodology used in this work involves the gathering of facts about the existing system. The purpose of this is to thoroughly analyse it in order to identify the inefficiencies associated with the existing system and determine the requirement analysis for the proposed system. The specific methods used in collecting data about requirements in the proposed system are more than one so as to ascertain accurate results and a comprehensive investigation. They include oral interview and Use of questionnaire. The oral interview isbasically to get the detail on the current system in use and how it can be improved upon, while the questionnaire is designed to collect the bio data of lecturers in department of physical and mathematical sciences, Afe Babalola University at random. The questionnaire required the employees to fill in bio-data about themselves and some information relating to the objective of this work.

The proposed system requirement specification: The basic requirements for the development of the proposed system include the software, hardware and accompanying tools. For Hardware Requirements are: U.ARE. U Biometric device with graphic LCD (Liquid Crystal Display), Finger print module, Memory and buttons, Uninterrupted Power Supplies (UPS) Switch Cables and Accessories / Battery etc.computer system with minimum of RAM: 512MBProcessor: Intel Pentium Hard disk: 20GB Software Requirements include: U.ARE.U 4500 series starter SDK (software development kit).The front-end interfaces will be developed using:Java for its object oriented nature and MySQL server for database creation at the back end.

INPUT AND OUTPUT DESIGN OF THE SYSTEM

The parties involved in the implementation of the BEAS are basically the User (Administrator)and the Employee. The input and output of each are interrelated and interact at certain stages of the implementation, they are described as follows:The Administrator is responsible for setting the portal open for attendance taking. This is done by securely logging into the system using user name and password. The inputs are the user name and password that launches a user to other pages to administrate as an output.The admin is also involved in enrolling, the input here are the employee passport, the fingerprint and the employee data. The output for enrollment is the storage of all the data being confirmed with a message of “enrollment successful”.

The verification phase is basically the phase where the attendance is taken. The input for the verification is the employee fingerprint, and the output is the matching confirmation which include the employee detail and saved passport, alongside a flag for successful verification.In the report phase, the input is the employee Identity, with the start and end date for which report is required. The output is a statistical representation of;

- Number of days office opened
- Number of times present:
- Number of times absent:
- Percentages:
- Comment
-

DATA FLOW MODEL

The conceptual diagram represents the process as a set of activities, it shows the data transformation. It shows how the input to the process, such as how the Employee enrolment and finger matching details is stored into the database. The data flow diagram takes an input-process-output view of the system.The flowchart diagram is a series of shapes each representing process, data, input, output, decision and end/ start. This is a sequence or flow of data as represented in the software application.

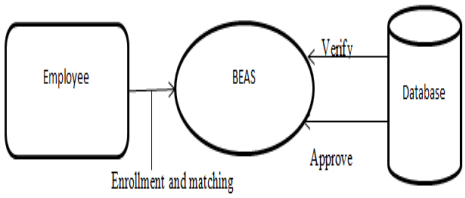

Figure 4: Conceptual Diagram for Biometric Employee Attendance System (BEAS)

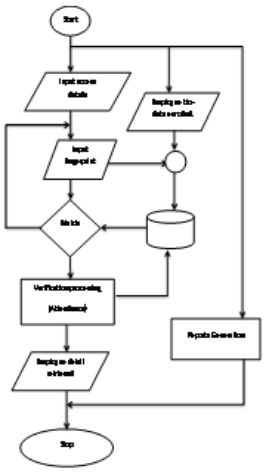

Figure 5: The Proposed System Data Flow Diagram

SOFTWARE STRUCTURE

The software has been divided into five parts for simplicity and understanding.Database: This section in the structure of com.bio.Database, this section deals with the collection, storage and retrieval of data. The database server structure which is in the table below:

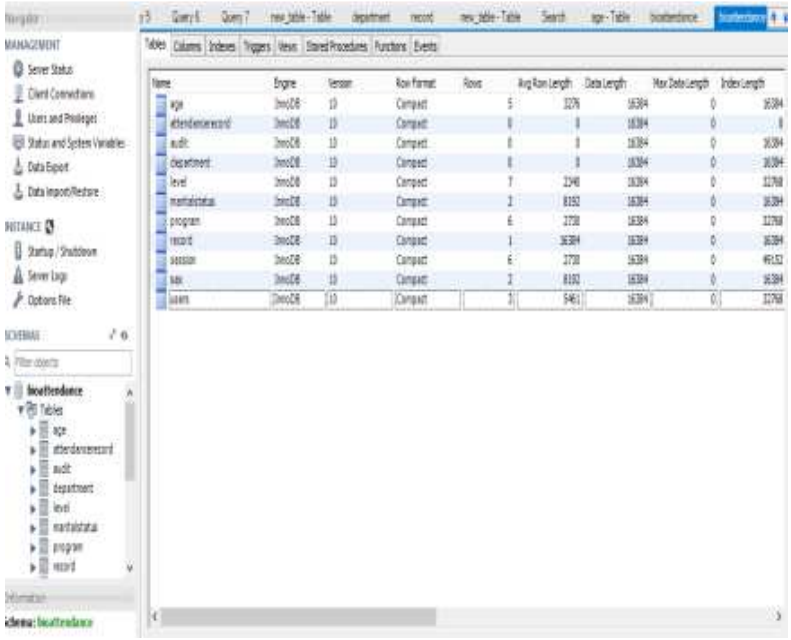

Table1: Structure of Database

The structure is composed of files that hold the data of each employee with the following tablesAge, Attendance Record,Audit,Department,Level,Marital Status,Program,Program,Session,SexUsers

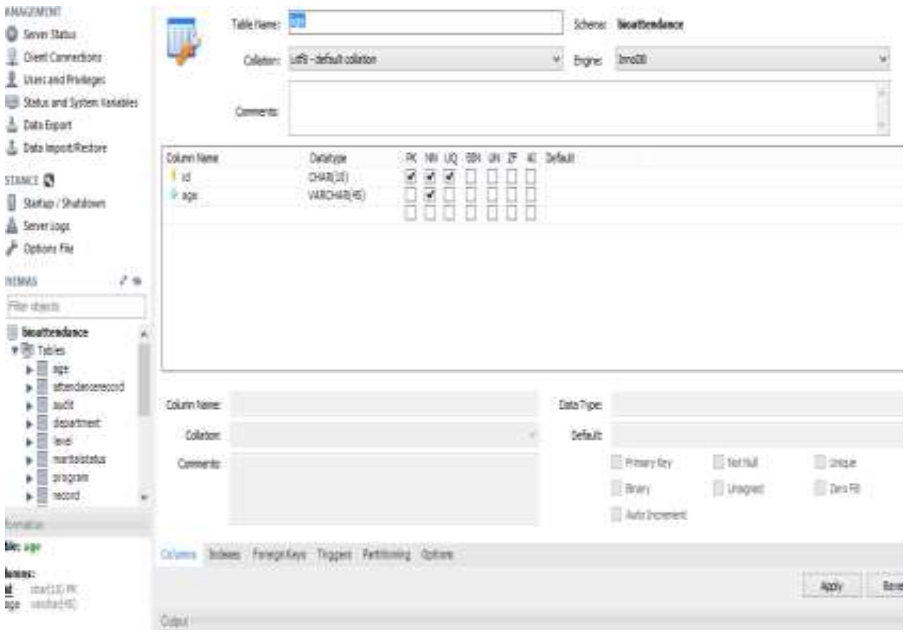

Table 2: Table Representing Age

Configuration: This section takes the form of com.bio.config. it is meant to basically read files and and hold the application root. The Core: this section is in the form of com.bio.core it interacts with all the classes including the main engine and co-ordinate between all other classesEntity: This section contains object oriented classes that will be used in configuration. It also contains records of employees. Report: This section is basically the report generation section, where

employees' attendance performance can be obtained. It's in the package com.bio.report

THE SOFTWARE INTERFACE

The software interface is designed to have six hyperlinks.

The hyperlinks are listed briefly below: Home: It is the log in page and also grants access to other links to an authorized user that has being registered and has the log in access which include the secure user name and password.

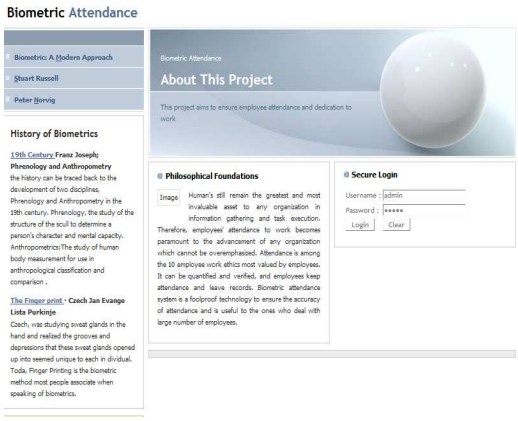

Figure 6: Home Page Screen Shot

Users: This is the link that an administrator gains access to once logged in. It is the link that has the form for adding new users, and setting a user active for the day to administer the function required for the day. A user cannot act as an administrator if he is not set as active.To add a user, simply log in and fill in the detail of the user as required in the form, then click on "create user". The fingerprint of an administrator is not required for registration. Once a user is registered, he can have a record in the database and a password can be set for the user to have access to log in, while the email address remains the user name.

Figure 7: User Creation and Activation Page

Enrollment link: the enroll link is the link that carries on with enrollment. Enrollment is the process of capturing a fingerprint image(s) for an individual, extracting fingerprint features, optionally checking for duplicates, and storing the fingerprint features.

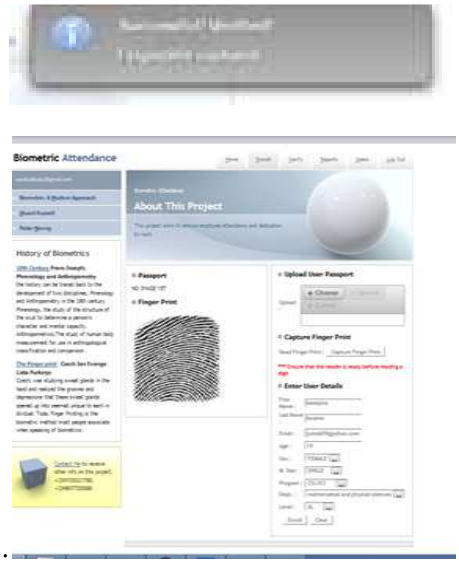

Figure 8: Enroll Page with an Employee's Scanned Fingerprint

Verify: (figure 8)This page is the page that can be termed the attendance taking page. it involves Comparing a fingerprint against a specific user's enrolled fingerprint(s) to verify a specific person's identity. Opening a session means the day has begun for employees and each employee can take attendance on resumption by verifying the record against the fingerprint.Attendance is taken by clicking on the button that reads "CAPTURE FINGER PRINT" at the left bottom of the window. If the finger print matches with the record in the database, the image and bio data of the employee is retrieved and shown on the provided field in the window. Then a message flags reading "verification successful". If the fingerprint does not match, the message will indicate "no record found". At the end of the attendance taking period for the day, the administrator closes the session by clicking on the button "Close Verification Session". This indicate that the attendance taking for the day has ended and every other employee verifying afterwards is not going to be in the record because attendance has closed.

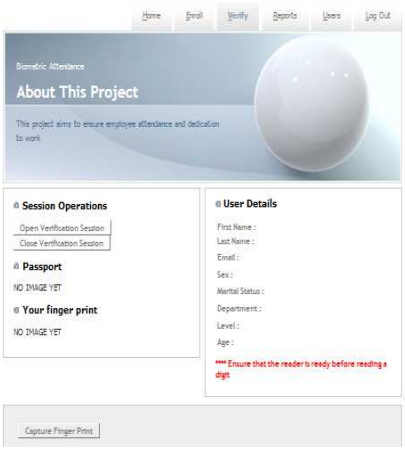

Figure 9: The Verification Window

Reports: The report page is reached by clicking the "Reports" link on the interphase.To generate a report for an employee, the employee user name (set as the e-mail) is filled os selected from the drop down given on the page, then the start date and end date for the report is selected by clicking "Start date" and "End date " respectively. Once the date required is filled, the next is to get report by clicking "show report".

The report for the user is automatically generated and the number of times present and absent is shown including the percentage and comment. The report can be optionally printed. The last link is the "Log Out" where ones the session is over or its not needed it can be ended. The last link is the "Log Out" where ones the session is over or its not needed it can be ended.

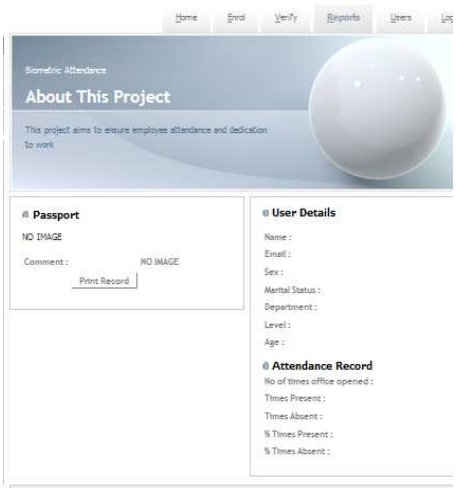

Figure 10: Reports Page for an Employee with Start and End Date

To ensure the confidentiality, integrity and availability among other objectives of information security, the home page puts a check on those who gain access to the system to administrate. This maintains the integrity of the system and data.

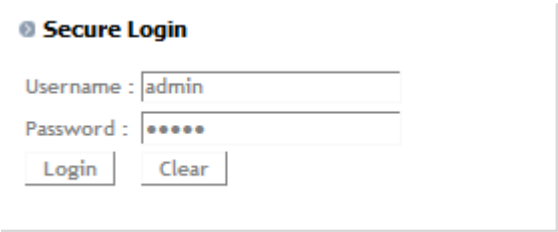

Figure 11: Secure Login

The password is not in plain text. It is hashed; the algorithm is SHA-256. The passwords cannot be stolen if a hacker breaks into the database. False request is also minimized by ensuring that a session can only be opened and closed once in a day, more so, a user log in detail expires when the system is left idle after every 15 minutes. Hence, login in will require access detail before actions can be taken.FAR (False Acceptance Rate) is greatly reduced by rejection of unknown finger record with a flag of information as shown:

Figure 12

CONCLUSIONS

The time attendance system has been one of the wide applications of the biometric technology. It has great advantages such as authenticity and accuracy, which is a major backbone in any field requiring identification. Fingerprint recognition, is also an established field of biometric. Therefore the use of biometric employee attendance system will support the new initiative of the Federal government of Nigeria to ensure promptness, effectiveness and efficiency among her working force which is important for the enhancement and ensuring dedication to work, aids unbiased promotion of dedicated employees, increase productivity and above all enhance quality learning outcome. It will be of immense importance and usefulness to the development of our society at large.

REFERENCES

1. Anil K. Jain, S. Prabhakar, and Sharath Pankanti. (2000) “Can identical twins beDiscriminated based on fingerprints?” Technical Report MSU-CSE-00-23,Department of Computer Science, Michigan State University, East Lansing, Michigan.
2. Antti S, Antti K, Teemupekka V, (2003) “Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner”, Telecommunication Software and Multimedia Laboratory Helsinki University of Technology, Australia.
3. Arun. S, Emmanuel. K, Diwakar. M & Rajeswari. R. (2008) “Automated attendance system using biometrics with embedded webserver“, Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology, Madurai, Tamil Nadu.
4. Thomas Y, Ing E Opoku-Mensah, Christopher A A,(2013) “Automatic Biometric Student Attendance System”: A Case Study Christian Service University College, Journal of Engineering, Computers & Applied Sciences (JEC&AS) Volume 2, No.6, June 2013, Ghana.
5. Namit S,(2013) “Bluetooth Attendance System” Department of Computer Science and Engineering, Dronacharya College of Engineering, Khentawas, Farukhnagar, Gurgaon, India, Academic Research Journals, Vol.1 No.1 January- June 2013, pp.8-11, India.
6. Norshidah K, Helmy A, and Jamal R (2010), “Development of Attendance System using Biometric Fingerprint Identification”, advanced Publishers, Kuching, Sarawak, Malaysia.
7. Eric P.K., Christine R.B., Shimon, K.M, and Tephen J.E.(2012) “Effect of Human Interaction on Fingerprint Matching performance, image quality and minutiae count” International conference on Information Technology and Applications, page 771-776

8. Prabhakar, S., Maltoni, D. Maio, D., & Jain, A.K. (2013) “Handbook of fingerprint recognition”, Springer-Verlag, New York.
9. Encarta dictionary (2008) edition
10. Byung-Gyu K, Han-Ju K and Dong-Jo P.(2001) “New Enhancement Algorithm for Fingerprint Images,” Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea.
11. Caesar, A.; Khan, S.A., (2006.)”Automation of Time and Attendanceuses RFID Systems”, IEEE-ICET 2006 2nd International Conference on Emerging Technologies, Peshawar.
12. Jain A., Hong L., Pankanti S., and Bolle R., (2008), “ An identify Authentication system using fingerprints” http://biometrics.cse.msu.edu/publications/fingerprint/JainEtAIIdentityAuthUsingFp_ProcIEEE97.pdf. Retrieved on : 12/07/2015
13. Connell J.H, Ratha N.K, and Bolle. R.M (2001) “An analysis of minutiae matchingStrength,” London.
14. Edmund Spinella, (2002) “Biometric Scanning Technologies: Finger, Facial and Retinal Scanning”, SANS institute, San Francisco.
15. Hoppner F, Klawonn R, Kruse R, and Runkler T, (1999) “Fuzzy ClusterAnalysis: Methods for Classification, Data Analysis and
16. Maltoni, D.(2010) “A tutorial on fingerprint Recognition”, Biometric Systems Laboratory -DEIS - University of Bologna.
17. Mohammad Z Bin Abdullah S,(2008) “attendance management system using fingerprint scanner”,Faculty of electronic and electrical engineering, Universiti Teknikal, Malaysia melaka.
18. www.biometrics.gov