

Optimization Of An Identity Access control System Using Biometric Techniques

Olayiwola Abisola Ayomide¹, Olayiwola Dare S.², Mosud Y. Olumoye³, Ikedilo Obiora Emeka⁴, Famuyiwa Kolawole Samuel Abiodun⁵, Agboke Adeola J.⁶, Ugwu Nnaemeka Virginus⁷

¹Department Of Computer Science, Celeb University.

²Department Of Computer Engineering, Ladoke Akintola University Of Technology, Ogbomoso.

³Department Of Computer Science, Celeb University

⁴Department Of Computer Science, Akanu Ibaim Federal Polytechnic, Uwana.

⁵Department Of Computer Science, D.S Adegbenro Ict Polytechnic, Itori.

⁶Department Of Computer Science, Celeb University

⁷Department Of Computer Science, University Of Nigeria, Nsukka



Abstract – Access control systems are widely deployed on campuses as a means to provide security. This paper proposed a biometric access control system for restricted areas based on individual facial recognition. The verification system, identification system are implemented to aid the Registration system, during the registration process necessary data's are collected and updated to the database to help the administrator to update required information. Based on that processing, an integrated secure system for biometric access control is developed for restricted area with acceptable security level. This paper develop an access control system that is efficient, and can properly identify individuals and its cost- effective. A new authentication system has been created that can verify who and what enters through the pass gate, also the security operative of the school system can have a complete log record of who accessed the school premises/labs and at what time. There is concern that some campuses are not using such protective systems, hence this paper attempts to resolve this weaknesses in such institutions' by developing a system using Facial recognition and smart card technologies.

Keywords – *Biometric, Facial Recognition, Access Control System, Verification, And Identification System.*

I. INTRODUCTION

Access control strategies have always been a necessity in university campuses. There has always been a need to limit access to sensitive areas and protect resources and assets in various scenarios and locations, including classrooms and special laboratories. Not only that, unfortunate incidents such as thefts, vandalism of campus property, cars being broken into [1], and even fatal assault case [2] had happened in local universities. This paper introduces a multifunctional centralized access control and management system using Radio Frequency (RF) and contactless smart card technologies. Campus security is the prime candidate for such technologies as the nature of campuses are easy access by a relatively high number of people in a place. The pro-posed system will benefit universities with no access control in place or are deploying standalone system in various strategic areas on their grounds. Standalone systems have limitations in their features and one main weakness is their ineffective ability to trace back individuals who gained access into the rooms, thus making investigations on campus grounds difficult. A background study to explore the

various technologies such as barcodes, QR codes, Bluetooth, biometrics, RFID, contactless smart cards, and NFC, was carried out by reviewing relevant academic journals, papers and online technology articles. Research showed that the best possible technology to use for the implementation is the contactless smart card. The focus of this paper is to highlight the design and development of a Centralised Access Control (CAC) system for campus tasks such as lecture attendance automation, room booking and scheduling, and real time occupancy validation.

The need for the adoption of strategies in verifying the identities of people in our world today cannot be over-emphasized. We currently live in an era when everyone should be vigilant and conscious of the identity of persons in their environment. Recurring security challenges and menace of false identity claims in our schools and society calls for a holistic approach from stakeholders in overcoming the ugly trend. Identity theft and fraudulent document production are reaching alarming levels all over the world. Human identification is a delicate notion that requires optimum consideration at all levels of management. However, Identifying an individual started way back, whereby humans are identified by names, tribal marks, the manner in which they look, acted, sounded (low pitched grunts versus shrill ones), even by their smell [1]. We realize that numerous animals today, for example, Dogs, depend on their noses to translate their environment and this incorporates recognition of individuals and different creatures. Therefore, the need to develop a way to physically identify individual becomes important. Security provides a way of protecting life and properties, making sure people and their valuables are safe. Hence, enforcing security for the gate pass becomes very important to avoid problems in our environment. Unlike access into a computer system or web application (e.g. email), access to pass through a gate requires being authorized to enter into/leave a facility such as buildings, laboratory, storehouses, etc. Here access control is not only in charge of authenticating and granting access (which is its primary duty) it involves gathering information on who and what had access to the facility, when, for what reason (if possible) and when the individual left, etc. This work thus highlights and recommends the need to properly identify the user that is granted access to different facilities e.g. hospitals, conference room and restricted areas around the universities (example library, laboratories, offices, server room (ICT department)), etc.

II. THEORETICAL BACKGROUND

Access control is a framework that empowers an expert to control access to zones and assets in a given physical facility or PC based data (logical). Access can be sub-divided into two types

1. Physical Access Control

2. Logical Access Control

1. Physical access control might be adequate in conditions where all users of a system require access to the majority of the data on it. In conditions where not all data assets on a system ought to be accessible equally to all clients, progressively exact control is essential.
2. Logical access control increases the security given by physical access control by acting as an additional guard against unapproved access to or utilization of the system's assets. It can likewise increase physical access control by giving included exactness since various clients can perform diverse functions.

2.1 Biometric Technology

Biometrics can be regarded as a science that is based on precise mathematics, by making use of strict measuring processes to detect an individual's identity; it is one access control system that is reliable. In contrast to measuring patterns in human's physical activity, biometrics discovers designs in different body features. Voice recognition and face recognition are becoming as popular as fingerprints [3]. When you say you implemented the means of biometrics for an individual to have access to your home, offices and company buildings, it means that you have implemented a reader that measure face distortions, it means that the reader's measure face distortions, finger curl or voice factors to let the access control tools know that the person demanding entrance is a person with sincere access and not an adversary.

Biometrics access control systems can solve the weak spots of using the former two factors (username and password) or just provide an extra level of security. Some commercial industries depend seriously on biometrics, including it as a part of the 2-factor authentication. Without reservation, I can say biometrics is a reliable and irreplaceable security mechanism for commercial and for residential application, particularly for developed communities and companies. Biometrics can be used in different ways to adjust the nature or needs of a company or firm. Palmtop recognition is another form of biometrics. In the light of this, [4] presented work

done on details based palmtop recognition framework for automatic door open and locking system. Biometric recognition is an upcoming and promising field with great commercial magnitude. It is an extremely reliable source identification system as it is based on what we are rather than what we possess. These characteristics are unique to individuals hence can be used to verify or identify a person. Biometrics can be sorted into two classes:

S/N	PHYSIOLOGICAL	BEHAVIORAL
1.	Face Recognition	signature
2.	Fingerprint	voice
3.	hand geometry	
4.	iris recognition	

2.2 Face Recognition And Voice Recognition In Biometrics

Face and voice recognition systems are one of the novel biometric measures, they are the safest authentication measures related to what the user is (the identity of the user). For comparing purposes, the usage of PINs and passwords are authentication credentials the user knows, and tokens are credentials the user owns. Each face has many unique landmarks and nodes that is the different points and height that make up facial structures. Some face qualities that are estimated by facial recognition software are the separation between the eyes, the width of the nose, profundity of the eye attachments, the shape of the cheekbones, and the length of the jawline. These nodes that are measured, are represented by codes known as face print in a database.

Facial recognition frameworks experience a few procedures to check the characteristics of an individual. The steps are:

1. Detection: Obtaining an image can be done by digitally scanning present passport or photograph or by using a digital camera to obtain a live photo of the individual.
2. Alignment: Once a facial recognition system (FRS) spots a face, it determines the position of the different facial attributes like the head, a distance of the eye from the nose, the size of the face, the pose, etc. the head must be turned at a certain degree towards the camera.
3. Representation: FRS convert the facial template into a unique code. This code assigns a set of numbers to reach template, to represent the characteristics of the individuals face.
4. Matching: facial matching is done using different imaging dimensions if the image uploaded to the FRS is in 3D and system database contain 3D images, then there will be no challenges in facial matching. But some problems facing the FRS database is 2D imaging. But recently researchers have profound a solution to that, by convert 3D images to 2D. that is when the 3D image is taken, the system identity different points, example the inner layer of the eye, the outside layer of the eye, the tip of the nose will be pulled and measure. If these measurements are taken, an algorithm will be applied to it to convert it to 2D format. Then the FRS can perform a facial matching action.

2.3 Review Of Related Literature.

Access in higher institutions (offices, libraries, laboratory, etc.) cannot be overemphasized in this work. A library, which is the core of any higher learning institution, is strategic to fulfill the learning, teaching and research goals of its clients. Below are review of existing approach:

[5] Propose a validation technique for physical access control by utilizing a cell phone and a QR code technique. However, solid technique to do verification, they built up a strategy dependent on matrix code and Rivest, Shamir, and Adelman (RSA) algorithm utilizing a one-time password. This system was subdivided into three sections; OTP RSA Server (ORS), OTP QR code Generator (OQG), OTP RSA Client (ORC). The ORS is utilized for enlisting the client's data, while the OQG is a mobile application used for receiving Multimedia Messaging Service (MMS) and generating authentication QR code image, and the ORC is a client portable computer with a camera, to scan the scene before it and process the captured picture. The figure below shows an overview of the system.

According to [6], proposed an Access Control Vehicle System based on camera installed at the parking entry. Firstly, the non-adaptive method is used to detect the moving object. An algorithm is used to detect, recognize and verify the face of the driver who want to enter to the parking. Viola-Jones method is used for face detection while LDA algorithm is used for face recognition.

In [7], implemented system comprises of digital door lock which is unlockable in real time to ensure secured access specifying activation, authentication and validation of users prior to bringing the RFID card close to the reader. The entire system is connected to central client-server sub-system that ensures and maintains the overall system.

According to [8], state a student authentication and verification systems is developed using Barcode Scanner. This system is aimed at reducing manual work and also eliminating the use of multiple cards. The student is allowed access to the college facilities such as library and central computer center more easily but also only by use of authorized ID cards.

In [9], a barcode recognition system is developed by using image processing. The barcode on the object to be identified is captured as an image instead of using a barcode scanner, this provides the convenience of observing data from the barcode with lower cost and can be done from anywhere any time. Barcoding systems are recommended as best practice for specimen labeling and point-of-care test barcoding because of the high overall strength of evidence of effectiveness.

According to [10], an RFID based access control system with GSM is installed at the entrance of a secured environment to prevent an unauthorized individual access. A security and access control based on RFID and biometrics is proposed for use in University Hostels to differentiate between valid and invalid users. This system accomplishes the security and access control task by processing information from sub-controllers which include entrance monitoring controller, exit this tag number in non-volatile RAM.

[11] Proposed a system that will encrypt student information into a quick response code (QR code). The QR code is then placed at the back of the understudy student ID card. This will recognize the student each time the QR code put on the back of the ID card is checked. Each dark and white box on the code, when examined, is translated to the student's information; which will enable the system to access the database and output the student data.

III. ACCESS CONTROL SCENARIO

A credential for access is presented to the reader, the reader then fetches the information from the credential and then sends it as input to the control unit which then compares it against a credential list stored in its database for a matching value. If a matching value is found the control unit then grants access by sending information to the lock unit to change its relay information from lock to open and vice-versa when credential does not match. The control unit then sends the transaction details in respective of access status to the database. This scenario might seem okay and secured but imagine a situation when an owner of the credential loses it into another person's hands, then a security breach occurs. So, it is important for the access control system to possess multiple access credentials that must all be satisfied before access is granted (which is a multiple-way authentication). Multiple-way authentication: this is the process of using two or more credential for authentication to enable access into a facility. The use of an ID card and password would be a two-way authentication credential criterion, the use of an ID card, password, and a signature would be a three-way authentication credential criterion, adding biometrics will make it a four-way authentication credential criteria. Credentials used to give access to users, can be anything either number or PIN, a thing you have on you (access badge), your biological attributes (biometric feature) or combination of different credentials. Why IAC Must Remain Distinctive, imagine a system with no passwords an individual can log on by inputting only his or her user ID. This would be ok if that system facility is only meant for one person. This system will only be secure if it is meant for one person. Someone else could simply enter your user ID and get access to your information, after all, it is public. Also, what happens if two people have the same name and want to use it as their User ID? Creating a matchless setting will be difficult.

Passwords are top-secret credentials and therefore should work, meaning an individual password now plays the role of identifying and authenticating, and here is where problems arise. Envisaging one wants to modify his/her password into something else and, unknown to him, an individual has already decided to use that password. You can't then use; it will alert you with an error message telling you "password is already in use. Please try another". You then have learned someone else's password and can access his or her account any time you wish. A system must uphold different mechanisms for identity and authentication. Identity must be something unique attribute and do not have to be private, however, passwords don't have to be unique, only secret. If an adversary

guesses or learns your password, you just change it. You do not need to go through the whole process of getting a brand new account. You can retract and re-assign passwords as often as you wish.

3.1 Analysis Of The Existing System

The existing system operates a manual authentication technique. In this system new students are given ID cards after their registration. This ID card contains their passport, their full name, their department, their signatures and the authorized signature of the chief security officer of the school. This ID card is being checked by the gate every time an individual comes into the library, offices, etc, records of their entry or exit and the time they stayed in school/labs of the school are documented but using a means of filling a notebook. In order to check the full information of a student, manual check through piles of files has to be made also no proper report is being made in case peculiar situations and replacing ID card takes a very long time before they are reissued.

3.2 Analysis Of The Proposed System

The proposed system consists of four main sections namely: registration, identification, verification, and access granted. The registration section can only be performed by either a student or staff. The system admin registers new user, generates QR code and trains the system by taking shots of the registered user. These shots will be taken using the system webcam which will enable the system to get the facial attributes of the user. The user takes a maximum of 5 shots to enable the system learn the facial features of the user. After the registration is complete the user is assigned a bar code. At the point of identifying the user scans the QR code placed at the back of his id card, this will serve as a means to identify him as a student or a staff in the institution. Furthermore, the verification stage involves the system taking snapshots of the user that has passed the first stage of identification. This stage, the system verify if the user is the rightful owner of that id card by verifying him/her using the facial recognition module. This is achieved by taking snap shot of the face of the user which is then analyzed and match with the once saved in the system database. Finally, if access is granted to the user, the user information is saved to the system in other to be able to generate a report at the end of the day so as to know who used a facility or entered into a premise. The timestamp is added to the record, at access entry and exit stages which are then stored in the database, where it is retrievable. Full student information can be checked at all times by just typing the user identity number (staff id). Daily, monthly, and yearly report can be generated by the system. The major aim of this proposed system is solving the limitations in the existing system by ensuring that both at entry and exit point the authentication criteria have to be issued. The figure below shows the architectural flow of the system .The figure below show the architectural flow of the proposed system.

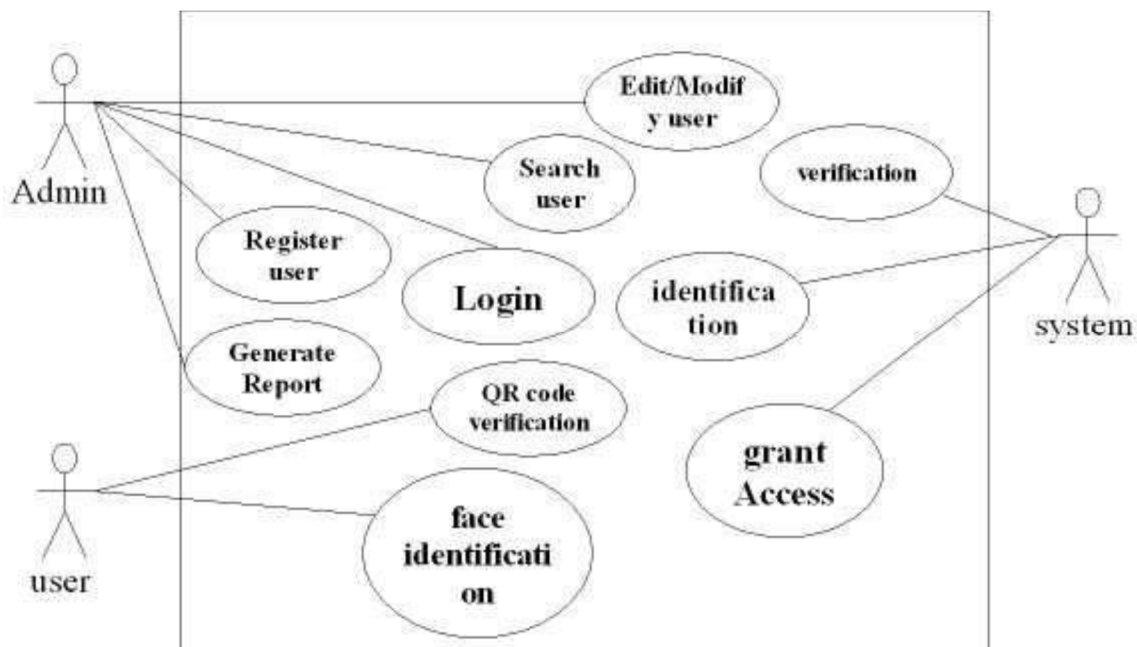


Fig 3.3 Use case diagram.

IV. SYSTEM ARCHITECTURE

The access control system is deployed on a dependent client-server based architecture. Stakeholders and users send a request to the server by scanning the QR code generated during registration and performing facial scanning operators using the system camera. The server verifies the QR code and facial features (basically checking if it matches the ID of any of the records in the database). If successful, it returns details of the requested person or error message when no result is found.

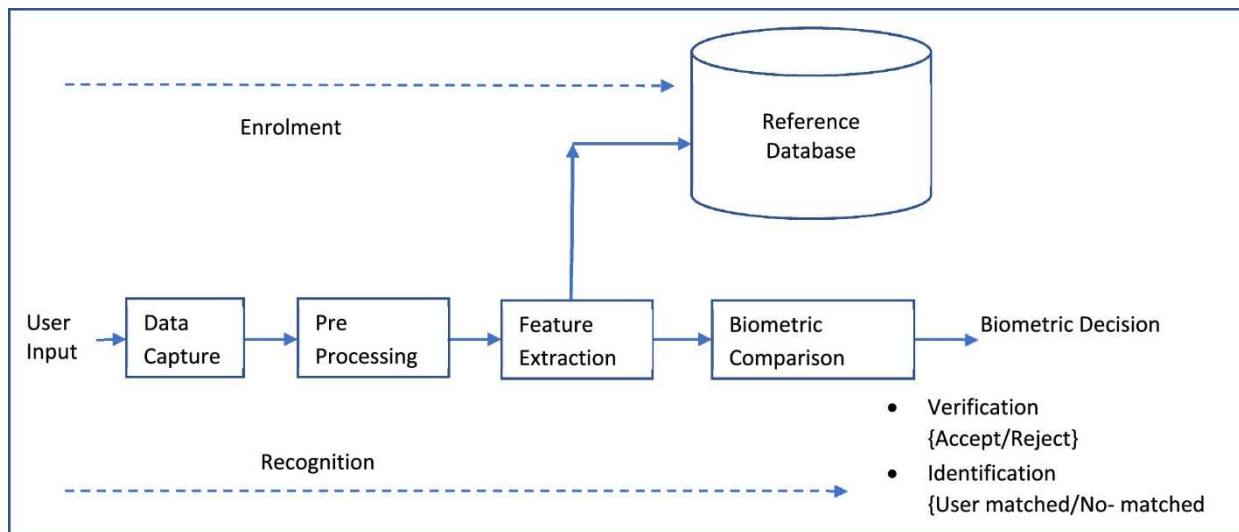


Fig. 4.0 Proposed System Architectural Flow

V. RESULT AND DISCUSSION

Security which has been an important aspect of an organization has to be taken seriously. The paper develop an access control system that is efficient, and can properly identify individuals, cost-

Effective. A new authentication system has been created that can verify who and what enters through the pass gate, also the security operative of the school system can have a complete log record of who accessed the school premises/labs and at what time. The result gathered the system will be more accurate if more face features are saved for a particular individual. Images was recorded in different positions, with each person having a 5 images. The maximum of accuracy of the system is reached when all parameters are controlled and the number of photos is at least 5. This result shows that high accuracy of the system is reached if the environment is controlled both on registration and at the point of verification, and if a large number of facial features are saved on the system.

VI. CONCLUSION

Access control system can bring in numerous benefits to many organizations, including making the campus a smarter and more secure space. This paper discussed on how to maximize the utilization of the data gathered by Access control system to integrate several useful features and services quite efficiently in terms of its stored data. The fact that the management system is web-based makes it very flexible as additional functions can be incorporated into the system with ease. Selecting smart cards and the use of facial recognition as user credentials is not only a security strategy to reduce tailgating, but also to allow for future applications that require secure transactions. A multifunctional smart card would surely relief the burden of students and staff having to carry several different cards at the same time. The system, however, is still quite simple and therefore prone to trickeries such as proxy attendance and tailgating issues. The system could be bolstered with facial recognition and biometrics to address such weaknesses. The goal of the paper is to provide a secure access control means for organization, and I believe that if the system is managed and used effectively, life, properties, and school facilities will be more secured.

REFERENCE

- [1] Ismail, H. Handbag reported stolen from UBD student's car. *Borneo Bulletin*. [Online] 8th March. [Accessed: 10th July 2015]. Available from: <http://www.brusearch.com/news/107443>.

- [2] Hamit R. "Students want UBD to strengthen security". *The Brunei Times*. [Online] 23rd December. [Accessed: 10th July 2015]. Available from: <http://bt.com.bn/frontpage-news-national/2014/12/23/students-want-ubd-strengthen-security>.
- [3] Tiwalade O. Majekodunmi, Francis E. Idachaba. "A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies". *Proceedings of the World Congress on Engineering 2011 Vol II WCE 2011*, July 6 - 8, 2011, London, U.K.
- [4] Seng Chun Hoo¹ and **Haidi Ibrahim**. "Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements". *Journal of sensor*. Volume 2019 |Article ID 7410478 | <https://doi.org/10.1155/2019/7410478>
- [5] Kuna-chieh liao et al. "A One-Time Password Scheme with QR-Code Based on Mobile Phone". *International Conference on Networked Computing and Advanced Information Management*. January 2009. DOI:[10.1109/NCM.2009.324](https://doi.org/10.1109/NCM.2009.324)
- [6] Taleb, M. E. Amine Ouis and M. O. Mammar, "Access control using automated face recognition: Based on the PCA & LDA algorithms," 2014 4th International Symposium ISKO-Maghreb: Concepts and Tools for knowledge Management (ISKO-Maghreb), Algiers, 2014, pp. 1-5.
- [7] M. Kishwar Shafin et al., "Development of an RFID based access control system in the context of Bangladesh,," *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, vol. , pp. pp. 1-5., 2015.
- [8] Akshatha M. et al, ""Student Authentication and Verification System using Barcode Scanner", " *International Journal of Internet of Things*, vol. 6(2):, pp. 71-74, 2017, .
- [9] N. M. Z. Hashim et al, "Barcode Recognition System", " *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Vols. Volume 2, , no. Issue 4, , July 2013.
- [10] S. Snyder, Peter Adole, et al "RFID Based Security Access Control System with GSM Technology". *Journal of Engineering Research (AJER)*, vol. 5, no. 7., pp. pp 236-242, pp. 2012.
- [11] Reshma Siyal¹, Mubina Pathan², et al. "Secure Students Identification by Using of Quick Response Code for Generating ID card for Library". *Journal of Applied Environmental and Biological Sciences. J. Appl. Environ. Biol. Sci.*, 7(7)74-79, 2017.