Journal of Engineering, Emerging Technologies and Applied Sciences -– Volume 2 Issue 1, April 2024

Available at ***https://www.ndu.edu.ng/journalofengineering/***

RESEARCH ARTICLE OPEN ACCESS

SmartGate: A Biometric Access Control and Attendance System

Jenny E. Fawei, Oyindinipre Bioko, Gabriel Ebiowei Moses

Niger Delta University, Wilberforce island, Bayelsa.

Email: faweijenny@ndu.edu.ng)

----------**********----------

Abstract:

The importance of attendance in any organization cannot be overstated. Attendance in many organizations, college and schools are paper-based which makes taking attendance daily both exhausting and time-consuming. There are a couple of issues with security for such existing system as many security resource persons are required for an organization having a large number of employee and visitors. For offices with restricted access, most organizations use automatic doors with smart I.D. cards to grant access to authorized staff. However, there are problems associated with the use of I.D. cards some of which are: Staff can easily misplace I.D. card, I.D. cards can get bad and keep authorized personnel stranded, unauthorized persons can easily steal the card of an authorized staff to gain access and unnecessary cost of issuing new identity card after an expired duration. There are many technologies that provide support in solving this issue using either OR code, visual recognition technology, Computer Vision, Internet of Things (IOT) combine with Radio Frequency Identification (RFID) technology, and microcontrollers. This paper presents the design of an automatic access control and attendance system using biometric authentication (both fingerprint and facial recognition) system. This system verifies authorized staff, while access control at the gate (entrance) is established, the facial recognition system is used to detect if the person at the gate is a staff or not. After verification, the staff can then login (or logout) and open the gate using the fingerprint machine. The system also makes a report of attendance with date and time which is automatically updated in the database. The gate access control is achieved using Arduino microcontroller while the database is program in c and MySQL.

Keywords — **Biometric Technology, face recognition, microcontroller**.

----------**********----------

1. INTRODUCTION

With the advent of new technologies, many organizations are adopting smart solutions for personal identity (ID) verification in applications like verified entry at the gate, attendance monitoring of employees, and many other surveillance tasks. The most common methods used in today's scenario are; identification using Passwords, PIN (Personal Identification Number) and token systems such as RFID card reader, fingerprint and voice recognition. Since such systems suffer from the problem of falsification, robbery and passes in the user's memory, an impressive enthusiasm for biometric identification systems has arisen in recent years. Common forms of biometrics used for logical and physical access control include a fingerprint, face recognition, speaker (voice), hand geometry, keystroke and handwriting recognition, etc. (Patel *et al*, 2021). Out of these methods of identity verification, face recognition is considered more stable as the physiological features rarely changes except in case of severe injury (Jusoh*et al*, 2021). This paper presents an automatic security gate attendance system that uses face recognition system to

distinguish between staff and non-staff of an organization and utilities finger print technology to sigh in and out of the premises, attendance will be updated in the respective organizational database while security of restricted areas will be taken care of. This organizes the staff record and reduces the time of management and enhances the level of security. The remaining part of this paper discuss a brief literature review, review of related work and the methodology of our proposed system.

2. A BRIEF LITERATURE REVIEW

Facial recognition system is a branch of biometric authentication technology used to compare a human face from an image or video frame to a database of faces (Sundarvas*et al,* 2022).

2.1. Stages of Face Recognition System

I. Image acquisition: The first step for face recognition system is to acquire an image from a camera.
II. Detection: Detection is the process of finding a face from the acquired image.
III. Computer vision: Computer vision automates the extraction, analysis, classification, and interpretation of meaningful information from picture data using sophisticated artificial intelligence (AI) technologies. The image data can be in many formats, such as, single images, video sequences, multiple camera, views, and three-dimensional data.
IV. Analysis: The face image is then analyzed by the facial recognition system. It maps and reads face geometry and facial expressions and identifies facial landmarks that are key to distinguishing a face from other objects.
V. Recognition: By comparing the faces in two or more photographs and determining the chance that the faces match, facial recognition may identify a person. (Gürel*et al,* 2012).

2.2. Advantages of Face Recognition System

I. Efficient security: facial recognition is a quick and efficient verification system compared to entering passwords or PINs. For added security assurance, it offers multifactor authentication.
II. Greater accuracy: Using facial recognition to identify people is more accurate than relying solely on their IP address, mobile number, email address, or mailing address.
III. Easier integration: Face recognition technology is compatible and integrates easily with most security software and devices.

2.3. Applications of Face Recognition System

Face recognition systems have a multitude of use cases across various industries and sectors. Here are some prominent examples:

I. Security and Access Control: Face recognition is commonly used for authentication and access control in secure environments such as airports, government buildings, corporate offices, and residential complexes
II. Law Enforcement: Police and law enforcement agencies use face recognition to identify suspects in criminal investigations. It helps in matching faces captured in surveillance footage with known criminals in databases, aiding in the apprehension of suspects and solving crimes.
III. Attendance Tracking: Face recognition systems are used in schools, universities, and workplaces for automated attendance tracking
IV. Border Control and Immigration: Face recognition technology is employed at border crossings and immigration checkpoints to verify travelers' identities against their passport photos or biometric data stored in government databases,

enhancing border security and streamlining immigration processes.

V. Personal Devices and Authentication: Face recognition is integrated into smartphones, tablets, and laptops for user authentication and device unlocking.

VI. Healthcare: In healthcare settings, face recognition can be utilized for patient identification, ensuring accurate medical records and preventing identity theft or fraud. It can also assist in monitoring patients for signs of certain medical conditions, such as pain or discomfort.

VII. Smart Cities: Face recognition technology is employed in smart city initiatives for various purposes, including traffic management, public safety, and urban planning. For instance, it can be used to identify traffic violators, track the movement of individuals in crowded areas, or detect suspicious behavior in public spaces.

2.4. Process of Finger Print Recognition System

The stages of fingerprint recognition are illustrated in figure1. This is described in another work by Soukhya *et al* below.

I. Image Acquisition: The Image Acquisition stage is the process of obtaining images by different ways. For taking fingerprint images, there are both online and offline techniques. The optical fingerprint reader is used in online fingerprint identification to take a fingerprint image. The offline fingerprint identification is obtained by applying ink on the finger and then pasting the finger on a sheet of white paper and finally scans the paper to get a digital image

II. Pre-processing: Pre-processing involves taking out undesired information from the fingerprint image, such as noise, reflection, missing details, and blur to increase the clarity of the ridge structure.

III. Feature extraction: A fingerprint feature extraction process is to locate, measure and encode ridge endings and bifurcations in the fingerprint.

IV. Pattern Recognition (PR): PR is divided into two categories (a) Decision Theoretic: In this step, quantitative descriptors work with patterns such as texture, area, and length. (b) Structural: Relational descriptor described by qualitative descriptors that also focus on patterns

Matching stage: - The matching stage aimed at comparing the acquired feature with the template in the database. There are three methods: hierarchical approach, classification approach and Coding approaches (Soukhya *et al,* 2020).

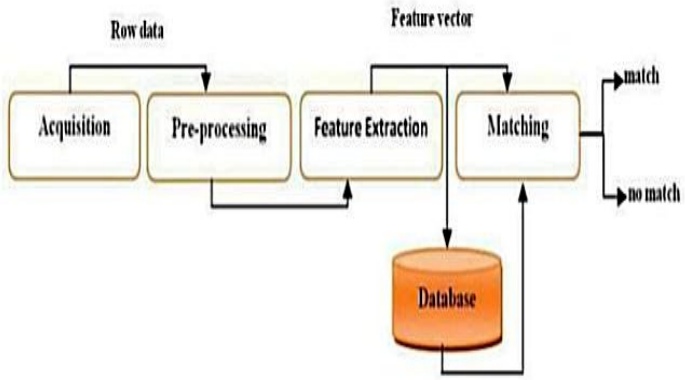

Figure 1: Process of Finger Print Recognition

Table 1: Comparison between fingerprint recognition and Face ID

Fingerprint	Face ID
It is safe as user need to just touch the device	It is completely contact-free; hence It is safer
Fingerprints are unique and do not duplicate, even among identical	Low uniqueness as people's facial traits can duplicate, for

twins	instance, in twins
Very accurate	Less accurate
Users can be identified only with a touch	Users can be recognized from a distance
Some individuals may not have fingers/fingerprint	Everyone has facial features
Specific device and software are essential	It can be software-based entirely

Fingerprint recognition, as a biometric authentication technique, offers several advantages:

I. Unique and Universal: Every person's fingerprint is unique, even among identical twins, making it an excellent method for individual identification. Additionally, fingerprints are universal, meaning nearly everyone has them, making fingerprint recognition widely applicable across diverse populations.

II. Highly Accurate: Fingerprint recognition systems boast high accuracy rates, especially when compared to traditional methods like passwords or PINs, which can be forgotten, stolen, or easily guessed.

III. Convenience and Speed: Fingerprint recognition offers a convenient and fast authentication process. Users can verify their identity simply by placing their finger on a scanner, eliminating the need to remember and enter complex passwords or carry physical tokens like ID cards or keys.

IV. Non-intrusive and Hygienic: fingerprint scanning is non-intrusive and does not require direct eye contact or capturing facial features. Additionally, it is considered more hygienic since users do not need to touch shared surfaces or devices with their faces or eyes.

V. Tamper-resistant: Fingerprint patterns are difficult to replicate or forge, providing a high level of security against fraudulent attempts to bypass authentication. Moreover, modern fingerprint recognition systems often incorporate anti-spoofing measures to detect and prevent spoof attacks using fake fingerprints or images.

VI. Scalability and Integration: Fingerprint recognition technology can be easily integrated into various devices and systems. This scalability allows for widespread adoption across different industries and applications.

VII. Cost-effective: With advancements in technology, fingerprint recognition systems have become more cost-effective to deploy and maintain, making them accessible to a wide range of organizations and businesses, regardless of size or budget constraints.

VIII. Privacy Protection: Unlike some other biometric modalities, such as facial recognition, fingerprint data can be stored and processed locally on the device without needing to be transmitted to external servers, thus providing greater privacy protection for users. (Wang *et al,* 2020).

3. REVIEW ON RELATED WORK

In recent times, different techniques, methods and algorithms have been employed in facial recognition and fingerprint techniques for attendance and security systems.

Sabeenian *et al,* develop a working model of a system that will promote attendance system in a classroom by recognize the frontal faces of students from a picture taken in a classroom (Sabeenian *et al,* 2020).

Chowdhury et al, work presents the development of a face recognition based automatic student attendance system by applying the Convolutional Neural Networks approach which requires data entry, dataset training, face recognition and attendance entry. The device can automatically record daily attendance and recognize numerous faces in a video stream. (Chowdhury *et al,* 2020)

In a work by Ghazal et al, an automatic multimodal biometric attendance checking system using Convolutional Neural Networks (CNN) was proposed. During the meeting attendance check, a computer equipped with a high-quality webcam is used. This system recognizes the attendee's face and voice and compares it with the known dataset; whenever a match occurs, the attendee's name is recorded in an excel file. (Ghazal *et al,* 2022).

In another work by Poojari et al, an automated system which monitors both attendance and activeness of each individual in its covered area and stores the data in a database for later use was implemented (Poojari *et al,* 2022).

Nuhi *et al,* proposed and implemented a smart attendance system with the aim to encourage the potential use of the Quick Response (QR) code as a future attendance management system, to track and record student attendance in lectures and exercises for all courses (Nuhi *et al,* 2020).

Patel et al, proposed a smart attendance system using QR code. The data-hiding algorithms inbuilt in the QR Code help to secure authentication. When a student scan QR code which was displayed by the teacher, attendance will be marked automatically according to the user id (Patel *et al,* 2019).

In another work, a system made of two applications was proposed, one for generating the QR Code by entering the student details and second application for taking the attendance and generating the attendance in CSV or XLS format (Wei *et al,* 2017).

Surekha et al, developed a smart attendance capturing and management system based on Viola–Jones algorithm and partial face recognition algorithms for controlled and uncontrolled environments. While the proposed system proved 100% accurate under controlled environment, the efficiency under uncontrolled environment is quite low (60%) (Surekha *et al,* 2017).

In a paper by Sawhney *et al,* a model was proposed for implementing an automated attendance management system for students of a class by making use of face recognition technique, by applying Eigen face values method, Principle Component Analysis (PCA) and Convolutional Neural Network (CNN) analysis. After these, the connection of recognized faces was conceivable by comparing with the database containing student's faces (Sawhney *et al,* 2019).

Wagh et al, Used Eigen face to detected and cropped face from image. After these, the comparison of detected faces can be done by crosschecking with the database of student's faces using PCA algorithms (Wagh *et al,* 2015).

Agrawal et al, proposed system aimed to create advancement in education systems by face detection and recognition-based attendance system, speech-to-text transcription for digital course material, and to save energy by automatically switching off the smart board when not in use (Agrawal *et al,* 2023).

A smart attendance system using body temperature measurement with the aid of contactless temperature sensors and Arduino UNO microcontroller was developed by utilizing a mobile and web application, to record and accesses the student's attendance details and body temperature measurement details (Zahira *et al,* 2021).

Dhawale developed a two-phase face mask detection and recognition for smart attendance system using face algorithm technique, python programming and to capture the images open cv and Tensor Flow is used (Dhawale, 2021).

Miao et al, implemented an innovative anti-cheating system for office attendance using Radio-Frequency Identification (RFID) system. Here, fingerprint recognition is achieved by using frequency distribution histogram extraction and the K-means clustering method is utilized for more refined recognition of targets with similar features (Miao *et al,* 2020).

Authors in Lee, D. 2020, established a Smart Attendance System using Bluetooth which consists of a student's smartphone app, a Raspberry Pi lecture room terminal and a management web page called RESTful.

In a work by Kumar et al, the database creation, fingerprint reader access, authentication and recognition using python were entirely done on raspberry pi. Also updating the database obtained to the organization was achieved by creating an application through cloud (Kumar *et al,* 2017).

A system that uses RFID technology and verifies an employee's RFID as soon as they enter the organization's area by consulting the organizational database, if he/she is indeed an employee of the respective organization he/she will be allowed to enter into workspace and his attendance will be updated in the respective organizational database was discussed in Khan et al, 2020.

A smart attendance system was proposed by Basloom *et al.* that used Oracle database, NET C# Web service, fuzzy logic, and the ZKTeco U260-C fingerprint reader for verification and recording. The implemented system has been deployed in a real environment in an organization comprising over 18,000 employees and has been tested using real data containing 6.1 million records (Basloom *et al,* 2020).

A four-step smart attendance system based on face recognition was introduced by Kumar & Pandey. First, face detection is done based on Histogram of Orientation Gradient (HOG) algorithm. Second, face alignment is done based on face landmark estimation algorithm. Third, Face net algorithm-based approach is used for face encoding, Finally, SVM classifier is trained with each face captured. (Kumar &Pandey, 2018).

A smart Attendance Monitoring System with Computer Vision Using IOT was create. The system also has the feature to send emails to the administrator about the student‘s attendance status at the time of recognition itself (Raj *et al,* 2021).

In a recent work, the system was developed with an Arduino Uno microcontroller and RFID readers. A GSM Module is used to send messages to parent's mobile about the student's attendance status while a GPS module is used to detect the live location of the student (Bharathy *et al,* 2021).Shah *et al,* in their paper, propose a facial security system that can be installed at any door or gate which would operate using integrated face recognition. Then face features are extracted using the PCA algorithm and fed to the SVM classifier face vectors and recognizes the face. The algorithm is capable of recognizing multiple faces at a time (Shah *et al,* 2020).

Rodrigues et al, developed a smart gate pass that Used random key generator to gathering information about the visitor via web and android application and this information is recorded in the database that manages the data (Rodrigues *et al,* 2021).

Many authors have presented various methods on automatic attendance system using either fingerprint biometric model or face recognition method but did not take care of restriction. This means unauthorized persons can still gain access to the building or classes.

4. METHODOLOGY

In this work, the Biometric Authentication System (BAS) is developed by combining the two different approaches: facial recognition and fingerprint technologies. The following sections discuss the methods associated with each of the approaches.

4.1. Working Principle

Every staff of the organization will be registered with their fingerprints and face scanned and saved in the database. The face of everyone that gets to the gate will be scanned with the face scanner. If a face is associated with a face in the database, the person will be identified as a staff, a "PLEASE LOGIN" message will be displayed on the user interface requesting the staff to login. When a

person is not recognized, a message will be display stating "USE THE NEXT GATE" with an arrow pointing the direction of the next gate. Whenever a staff logs in, the date and login and logout times will be registered in the database. The block diagram of the system is presented below.

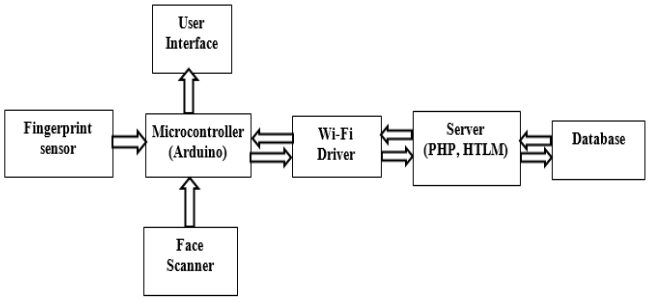

Figure 2: Block diagram of the system

4.2. Facial Recognition

We developed a very simple architecture for the system using facial recognition. First, all authorized staffs to the restricted area will be registered in the system in faces database. Then a high-definition camera is strategically placed at the gate to capture the face of an incoming staff. Once the image of the incoming staff is taken, the enhanced image will then be detected and compared against the images in the face database. If the staff is authorized, access is granted; and if not, access is denied.
The block diagram below shows this architecture.

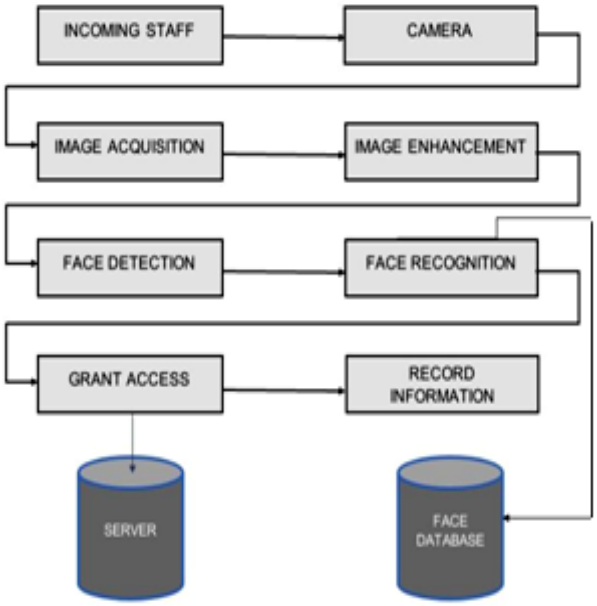

Figure 3: Face Recognition process for the system

4.3. Face Recognition Process

I. Registration of Authorized Staffs: all authorized staff will register with the system and have their information saved in the database that will be used for comparison. The images of the staff will be tied with their staff identity number. The reason for this is that the system has the additional capacity to record the "Access History" of the building. The Access History will show the staff I.D number, the date and time that staff accessed the building

II. Image Acquisition: a high-definition camera will be installed at the gate. It is well positioned to capture the face of any incoming person. This captured image is taken as an input to the system and passed on for processing.

III. Face Detection: after the enhancement of image, this module will detect the faces of an incoming staff from the image.

IV. Face Recognition: this is achieved by cropping the faces from the image and comparing them with the registered images in the authorized staff database.

V. Granting Access: after the verification of faces and successful recognition is done, the system grants access to the staff by sending a signal to the electronic door to open.

VI. Recording of Activity: the last stage here is the recording of the activity; that on day X, staff Y accessed the restricted area at time Z. this will be saved in the activity log.

4.4. Flow chart of activities for facial recognition

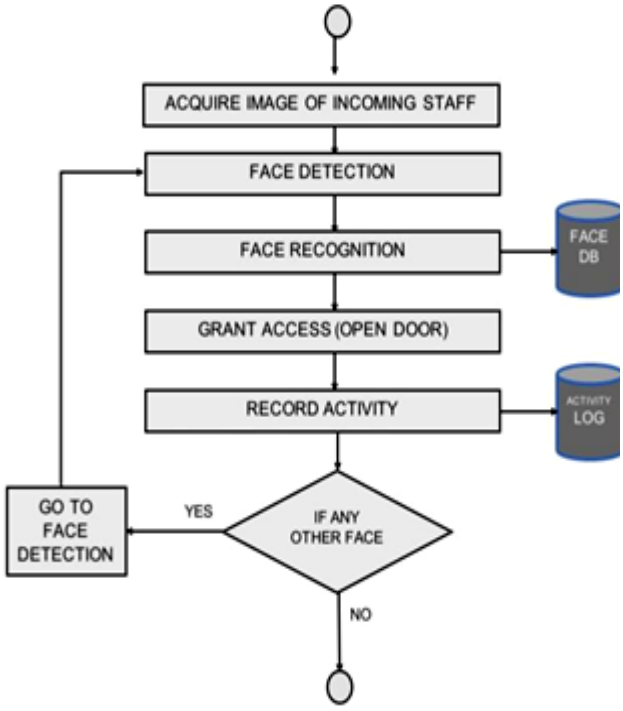

Figure 4: Face Recognition activity for the system

4.5. Fingerprint Architecture

A design that is very similar to that of facial recognition is used. First, all authorized staffs to the restricted area will be registered in the system and have their fingerprints stored in the fingerprints database (FPD) of authorized staffs. We then placed a Dermalog Fingerprint detection machine at the gate of the restricted area so that incoming staffs can place their fingers on the machine for authentication before access is granted. Once the fingerprint is captured, it is compared against the fingerprints in the FPD. If staff is authorized, access is granted; and if not, access is denied. The block diagram of the architecture is shown below.

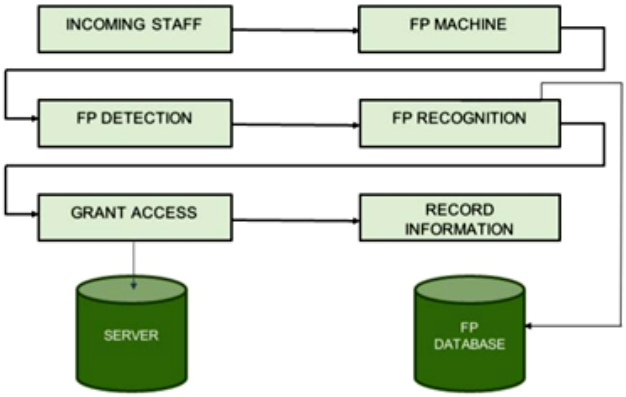

Figure 5: Fingerprint architecture for the system

4.6. Process of Fingerprint Access

I. Registration of Authorized Staffs: like the case of facial recognition, the fingerprint biometric system requires that all authorized staff will first register with the system and have their information saved in the fingerprint database (otherwise called FPD for short). It is the data in this FPD that will be used to compare against the fingerprint of an incoming staff requesting access to a restricted area. The fingerprint of staffs will be matched to their staff ID number so that the system can keep a log or "Access History" of the restricted area.

II. Fingerprint Detection: this is achieved by placing a fingerprint detection machine at the gate of the building. The detected fingerprint is the input to the system and it's passed on for processing.

III. Fingerprint Recognition: the detected fingerprint is compared against data in the FPD. If the system finds a match to the detected one, access is granted; else access is denied.

IV. Granting Access: After successful recognition and verification of the staff is done, the system grants access to the staff by sending a signal to open the electronic door. However, the message "USE THE NEXT GATE" is displayed if the incoming staff is unauthorized.

V. Recording of Activity: the last stage is the recording of the activity. The system keeps record of the date, time, and staff member who accessed the building.

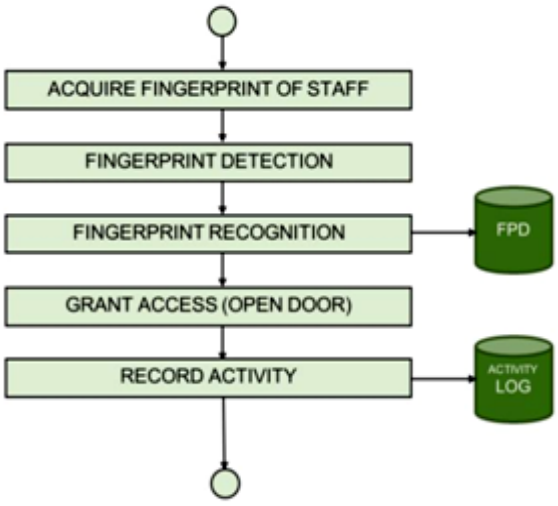

Figure 6: flow chart of fingerprint process

4.7. Hardware and software Requirements

- Arduino Uno, for the gate control
- Face++, for face detection, face comparison
- A Dermalog fingerprint detection machine, for fingerprint biometric
- Alarm, provide signal to indicate the presence of a visitor
- Language: Embedded C, MySQL
- Xampp PHP, for the database management system.

4.8. The Gate Access Control

A staff is identified with the aid of the facial recognition machine, then sign in using the right tomb print. At this point, the staff attendance is registered and stored at the database while the main gate is triggered opened which is controlled by the microcontroller. This will take the staff to the lodge. Every staff sign out from the lodge using the left tomb print. Every unauthorized person or visitors are directed to the next gate.

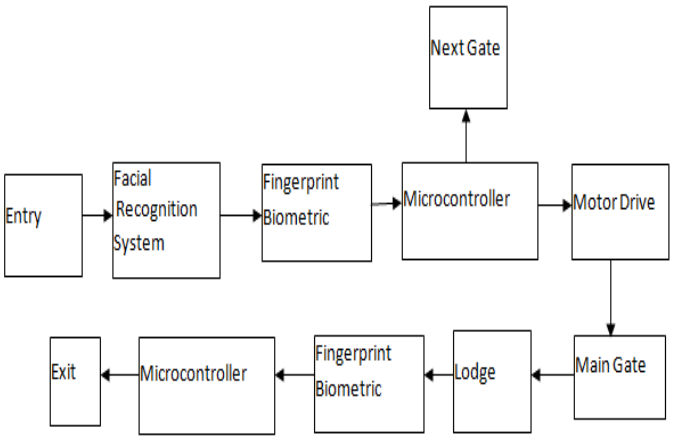

Figure 7: Block Diagram of the Gate Control System

The major advantage of this system of the system is that fingerprint of a person can be copied hence an unauthorized person can login with a copied fingerprint. But when the face of a person has been detected, he/she will not be able to login with a stolen fingerprint.

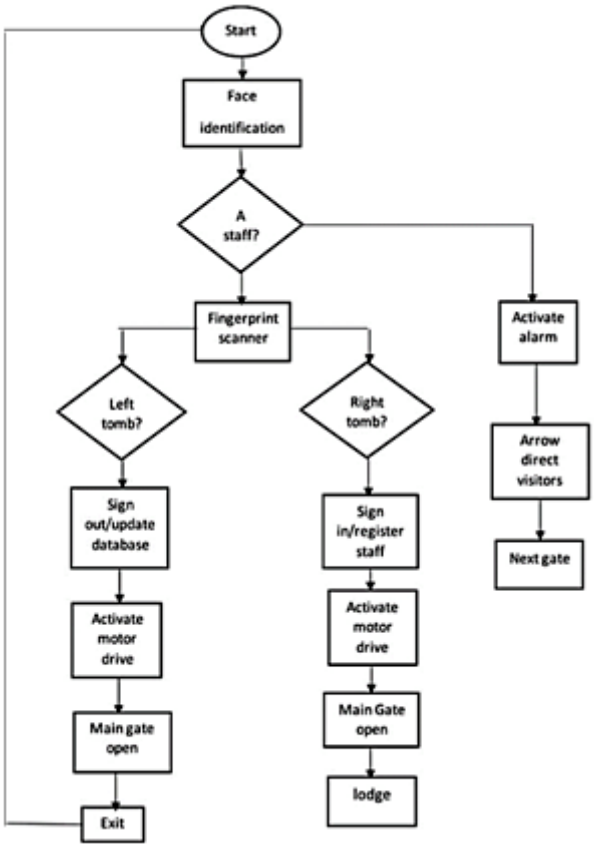

Figure 8: Flow chart for the gate control system

Whenever a visitor or an unauthorized person gets to the gate, an alarm will be activated. This will signal the security personnel that there is a visitor.

4. CONCLUSION

This paper on smart gate: Access control and security system using biometric authentication (both face recognition and fingerprint technology) features one of the best ways of securing a restricted area and taking record of everybody that enters the company. It is a dual system that prevents an intruder from entering the building, and gives automatic attendance of all the staff daily. this is a time-saving, and efficient system which can be implemented using microcontroller (Arduino Uno), a fingerprint scanner, face ++, webcam, and MySQL database on xampp server. The purpose of our proposed system is to provide security and reduce errors and human effort in traditional attendance taking via biometric authentication system.

5. REFERENCES

Patel A. K., Patel U. P., Suthar F. A. (2021). Fingerprint recognition in biometric security. Journal of information, knowledge and research in computer science and applications Volume – 01, Issue - 02 Page 44 DOI:10.13140/RG.2.2.11683.17441

Jusoh F.A., Zakaria M., Sabapathy A., Ibrahim T., Rahim M., Azizan H., Zakaria M., Nasir M., Albreem N., Ahmad M. (2021). Smart Gateless System using RFID Technology in Universiti Malaysia Perlis. In Journal of Physics: Conference Series (Vol. 1878). IOP Publishing Ltd. https://doi.org/10.1088/1742-6596/1878/1/012066

Sundarvas T.S., Goutham T., Senthil M.K. (2022). Face Recognition based Smart Attendance System Using IoT" (PDF). International Research Journal of Engineering and Technology. 9 (3): 5. Pp 182-186

Gürel C., Erden A.(2012). Design of a face recognition system. The 15th International Conference on Machine Design and Production. Pamukkale, Denizli, Turkey

Soukhya S M, SonuG , L Karthik Narayan, Dr.Manju VC. (2020). Fingerprint Recognition and its Advanced Features. International Journal of Engineering Research & Technology (IJERT) Vol. 9 Issue 04, Access at: http://www.ijert.org ISSN: 2278-01

Wang, C., Yu, L., Chang, H., Shen, S., Hou, F., & Li, Y. (2020). Application research of file fingerprint identification detection based on a network security protection system. Wireless Communications and Mobile Computing, 2020. https://doi.org/10.1155/2020/8841417

Sabeenian, R. S., Aravind, S., Arunkumar, P., Harrish Joshua, P., &Eswarraj, G. (2020). Smart attendance system using face recognition. Journal of Advanced Research in Dynamical and Control Systems, 12(5 Special Issue), 1079–1084. https://doi.org/10.5373/JARDCS/V12SP5/20201860

Chowdhury, S., Nath, S., Dey, A., & Das, A. (2020). Development of an Automatic Class Attendance System using CNN-based Face Recognition. In ETCCE 2020 - International Conference on Emerging Technology in Computing, Communication and Electronics. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ETCCE51779.2020.9350904

Ghazal, M., Albasrawi, R., Waisi, N., & Al Hammoshi, M. (2022). Smart Meeting Attendance Checking Based on A multi-biometric Recognition System. PrzegladElektrotechniczny, 98(3), 93–96. https://doi.org/10.15199/48.2022.03.21

Poojari, N. N., Sangeetha, J., Shreenivasa, G., & Prajwal. (2022). Automatic Student Attendance and Activeness Monitoring System. In Smart Innovation, Systems and Technologies (Vol. 289, pp. 405–415). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-19-0011-2_36

Nuhi, A., Memeti, A., Imeri, F., &Cico, B. (2020). Smart Attendance System using QR Code. In 2020 9th Mediterranean Conference on Embedded Computing, MECO 2020. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MECO49872.2020.9134225

Patel, A., Joseph, A., Survase, S., & Nair, R. (2019). Smart Student Attendance System Using QR Code. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3370769

Wei X., Manori A., Devnath N., Pasi N., Kumar V. (2017). QR Code Based Smart Attendance System. International Journal of Smart Business and Technology, 5(1), 1–10. https://doi.org/10.21742/ijsbt.2017.5.1.01

Surekha, B., Nazare, K. J., Viswanadha Raju, S., & Dey, N. (2017). Attendance recording system using partial face recognition algorithm. Studies in Computational Intelligence, 660, 293–319. https://doi.org/10.1007/978-3-319-44790-2_14

Sawhney, S., Kacker, K., Jain, S., Singh, S. N., & Garg, R. (2019). Real-time smart attendance system using face recognition techniques. In Proceedings of the 9th International Conference On Cloud Computing, Data Science and Engineering, Confluence 2019 (pp. 522–525). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CONFLUENCE.2019.8776934

Wagh P., Thakare R., Chaudhari J., and Patil S. (2015). Attendance system based on face recognition using eigen face and PCA algorithms. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India. pp. 303-308, doi: 10.1109/ICGCIoT.2015.7380478.

Agrawal, S., Chandhok, A., Maheswari, S., & Sasikumar, P. (2023). Smart Classroom: A Step Toward Digitization. In Lecture Notes in Networks and Systems (Vol. 400, pp. 781–789). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-19-0095-2_74

Zahira, M. N., Mca, J., Phil, M., & Prakash, M. (2021). Iot Based Smart Attendance System With Body Temperature Measurement. International Journal of Computer Techniques, 8(2). Retrieved from http://www.ijctjournal.org

Dhawale, S. P. (2021). Face with Mask Detection and Recognition for Smart Attendance System. International Journal for Research in Applied Science and Engineering Technology, 9(VII), 1586–1591. https://doi.org/10.22214/ijraset.2021.36615

Miao, Q., Xiao, F., Huang, H., Sun, L., & Wang, R. (2020). Smart attendance system based on frequency distribution algorithm with passive RFID tags. Tsinghua Science and Technology, 25(2), 217–226. https://doi.org/10.26599/TST.2018.9010141

Lee, D. (2020). Bluetooth-Based Smart Attendance System. International Journal of Engineering and Advanced Technology, 9(3), 3851–3854. https://doi.org/10.35940/ijeat.c6280.029320

Kumar P. M. S., Dr. Suresh K., Indumati T & Kumar K. (2017). Smart Attendance System using Raspberry Pi. International Journal of Trend in Scientific Research and Development, Volume-1(Issue-5), 514–518. https://doi.org/10.31142/ijtsrd2306

Khan, A., Jhanjhi, N. Z., & Humayun, M. (2020). Secure Smart and Remote Multipurpose Attendance Monitoring System. EAI Endorsed Transactions on Energy Web, 7(30), 1–10. https://doi.org/10.4108/eai.13-7-2018.164583

Basloom, H., Bosaeed, S., & Mehmood, R. (2020). Hudhour: A Fuzzy Logic based Smart Fingerprint Attendance System. In 2020 5th International Conference on Fog and Mobile Edge Computing, FMEC 2020 (pp. 331–336). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/FMEC49853.2020.9144948

Kumar Chauhan, R., & Pandey, V. (2018). Smart Attendance System Using CNN. International Journal of Pure and Applied Mathematics, 119(15), 675–680. Retrieved from http://www.acadpubl.eu/hub/

Raj, A., Raj, A., & Ahmad, I. (2021). Smart Attendance Monitoring System with Computer Vision Using IOT. Journal of Mobile Multimedia, 17(1–3), 115–125. https://doi.org/10.13052/jmm1550-4646.17135

Bharathy, M. G. T., Bhavanisankari, M. S., &Tamilselvi, T. (2021). Smart Attendance Monitoring System using IoT and RFID. International Journal of Advances in Engineering and Management (IJAEM), 3(6), 1307. Retrieved from https://www.researchgate.net/publication/352508504

Shah M., Shukla, D., & Pandya, D. (2020). Smart Gate: Intelligent Security System Based on Face Recognition. International Journal of Innovative

Technology and Exploring Engineering, 9(3), 601–608. https://doi.org/10.35940/ijitee.k2234.019320

Rodrigues, R., Pavate, A., Sawant, R., & Lopes, N. (2021). SMART GATE PASS SECURITY MANAGEMENT SYSTEM USING RANDOM KEY GENERATION. International Journal of Innovative Research in Computer Science & Technology, 9(3). https://doi.org/10.21276/ijircst.2021.9.3.10

