SwiftVerify: A Multi-Modal Smart Attendance System

Major Project Report

submitted

in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

in

CSE (ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

by

BHUKYA VEERANNA	**20R11A6607**
MADANU SHALINI	**20R11A6631**
PELADOLU SAIKIRAN	**20R1 1A6643**

Under the esteemed guidance of

Dr. V. Madhusudhan Rao
Professor & Dean school of CS&I

DEPARTMENT OF CSE (ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

GEETHANJALI COLLEGE OF ENGINEERING AND TECHNOLOGY

(An Autonomous institution, NBA, NAAC Accredited and Affiliated to JNTUH, Hyderabad)

Cheeryala (V), Keesara (M),
Medchal (D), Telangana- 501 301

April - 2024

Geethanjali College of Engineering & Technology
(UGC Autonomous)
(Affiliated to JNTUH, Approved by AICTE, New Delhi)
Cheeryal (V), Keesara(M), Medchal Dist.-501 301.
Department of Computer Science and Engineering(AI&ML)

CERTIFICATE

This is to certify that the Major Project Report entitled **"SwiftVerify: A Multi-Modal Smart Attendance System"** is a bonafide work done and submitted by

BHUKYA VEERANNA	**20R11A6607**
MADANU SHALINI	**20R11A6631**
PELADOLU SAIKIRAN	**20R11A6643**

during the academic year 2023 - 2024, in partial fulfilment of requirement for the award of Bachelor of Technology degree in **CSE (Artificial Intelligence & Machine Learning)** from Jawaharlal Nehru Technological University Hyderabad, is a bonafide record of work carried out by them under my guidance and supervision.

Certified further that to my best of the knowledge, the work in this dissertation has not been submitted to any other institution for the award of any degree or diploma.

Project Guide
Dr. V. Madhusudhan Rao
Professor & Dean school of CS&I

Project Co-Ordinator
Mr. Shaik Akbar
Associate Professor CSE(AI&ML)

Head of the Department CSE(AI&ML)
Dr. L. Venkateswarlu

External Examiner

ACKNOWLEDGEMENT

The satisfaction of completing this project would be incomplete without mentioning our gratitude towards all the people who have supported us. Constant guidance and encouragement have been instrumental in the completion of this project.

First and foremost, we thank the Chairman, Principal, Vice Principal for availing infrastructural facilities to complete the major project in time.

We offer our sincere gratitude to our Project guide **Dr. V. Madhusudhan Rao**, Professor & Dean school of CS&I, Computer Science and Engineering (AI&ML) Department, Geethanjali College of Engineering & Technology for his immense support, timely co-operation and valuable advice throughout the course of our Major Project work.

We would like to thank the Project Co-Ordinator, **Mr. Shaik Akbar**, Associate Professor, Computer Science and Engineering (AI&ML) for his valuable suggestions in implementing the project.

We would like to thank **Dr. L. Venkateswarlu**, Head of the Department CSE(AI&ML), for his meticulous care and cooperation throughout the project work.

BHUKYA VEERANNA	**20R11A6607**
MADANU SHALINI	**20R11A6631**
PELADOLU SAIKIRAN	**20R11A6643**

ABSTRACT

Addressing the surging demand for advanced attendance systems, this major project introduces a revolutionary Multi-Factor Attendance System. Combining barcode scanning, facial recognition with anti-spoofing analysis, and voice matching, the system employs a multi-layered authentication process for comprehensive user verification. Beginning with swift barcode scans, each participant is assigned a unique identifier. The integration of advanced facial recognition technology, coupled with gesture analysis and voice matching, fortifies the authentication process, ensuring heightened security and resilience against unauthorized access. A centralized database efficiently manages user information, and upon successful verification, attendance is instantly updated to a backend Excel sheet in real-time. This not only streamlines attendance management but also minimizes manual data entry, reducing the likelihood of errors. The system's standout feature is offering valuable insights into attendance trends and patterns, thereby contributing significantly to the technological advancement of educational institutions.

Keywords: Multi-Factor Attendance System, Barcode scanning, Facial recognition, anti-spoofing, Voice matching, Authentication process, User verification, Centralized database, Real-time attendance tracking.

TABLE OF CONTENTS

11. CONCLUSION & FUTURE SCOPE

REFERENCES

APPENDIX

LIST OF FIGURES

Figure Title Page

LIST OF TABLES

Table Title Page

LIST OF ABBREVIATIONS

1.	MFAS	Multi-Factor Attendance System
2.	FR	Facial Recognition
3.	AS	Anti-Spoofing
4.	VM	Voice Matching
5.	GA	Gesture Analysis
6.	AM	Attendance Management
7.	DE	Data Entry
8.	AT	Attendance Trends
9.	PI	Patterns Insights
10.	TI	Technological Advancement

1. INTRODUCTION

The innovative Multi-Factor Attendance System that our project provides is a reaction to the growing need for sophisticated attendance systems. This system transforms traditional attendance tracking techniques by combining barcode scanning, facial recognition with anti-spoofing analysis, and voice matching technology. By combining these cutting-edge authentication procedures, we hope to improve the security, accuracy, and efficiency of attendance management. Our technology promises to simplify administrative work and provide useful insights into attendance trends and patterns by updating attendance records in real time and analysing data in depth. This introduction lays the groundwork for a thorough examination of our novel approach to modern attendance difficulties.

1.1 MOTIVATION

In today's fast-paced world, there is an increased demand for effective attendance systems. Traditional approaches frequently fall short of addressing the objectives of modern organisations, particularly educational institutions, which prioritise accuracy, security, and efficiency. Recognising this essential need, our project intends to develop a revolutionary Multi-Factor Attendance System that combines cutting-edge technology to deliver a complete solution.

1.2 PROBLEM STATEMENT

Traditional attendance systems have numerous flaws, including fraud risk, inefficient data administration, and a lack of real-time information. Manual attendance tracking is not only time-consuming, but also prone to errors, resulting in erroneous records and administrative complications. Advanced authentication mechanisms are required because the security of attendance systems is seriously threatened by the emergence of digital impersonation tactics.

- **Vulnerability to Fraud:** Manual attendance tracking methods, such as paper-based sign-in sheets or basic biometric scans, are susceptible to fraud and manipulation. Instances of proxy attendance, where one person marks

attendance on behalf of others, are common, leading to inaccurate records and undermining the integrity of attendance data.

- **Inefficiency in Data Management:** Traditional attendance systems rely on manual data entry, which is labour-intensive and prone to errors. Maintaining correct attendance records becomes more difficult as the number of participants expands, resulting in administrative responsibilities and delays in data processing.

- **Lack of Real-time Insights:** Traditional attendance systems frequently lack the capacity to deliver real-time attendance updates and insights. Administrators are unable to quickly monitor attendance patterns, which limits their capacity to spot trends, manage issues, and make educated decisions about resource allocation and student engagement initiatives.

- **Security Concerns:** As digital impersonation tactics, such as deepfake technology, progress, traditional authentication methods, such as facial recognition, become less secure. Without strong anti-spoofing safeguards, attendance systems are prone to unauthorised access and fraudulent activity, offering substantial security threats to organisations.

- **Limited Scalability:** Many present attendance systems struggle to scale successfully to meet the rising needs of organisations, especially those in big educational institutions or corporate environments. Scalability difficulties can cause performance bottlenecks, system downtime, and a poor user experience, reducing the effectiveness of the attendance management process.

- **Compliance Challenges:** Educational institutions and organisations are subject to a variety of regulatory regulations for attendance tracking and reporting. Conventional systems may lack the functionality required to assure compliance with regulatory norms, posing legal and regulatory concerns.

1.3 PROJECT OBJECTIVES

The primary goal of this project is to overcome the inadequacies of current attendance systems by proposing a Multi-Factor Attendance System with improved security, accuracy, and efficiency. Specifically, our aims are:

- **Implementing barcode scanning:** Barcode scanning is a rapid and effective approach to identify and record participants' attendance. The goal here is to seamlessly integrate barcode scanning technology into the system, ensuring speedy identification while maintaining accuracy.

- **Enhancing Authentication with Facial Recognition and Anti-Spoofing:** Facial recognition technology provides high-level security for authentication purposes. However, it is vulnerable to spoofing attacks, in which imposters try to trick the system by utilising photographs or videos. This goal entails combining advanced facial recognition algorithms with anti-spoofing analytical tools to improve the system's resilience against fraudulent attempts.

- **Incorporating voice matching:** Voice matching provides an additional layer of protection by authenticating the user's identification via voice. This goal requires developing voice recognition algorithms that can accurately match the user's voice to pre-recorded samples, hence improving the system's overall authentication capacity.

- **Developing a centralized database:** A centralised database is required for the secure storage and management of user information. This goal entails creating and implementing a solid database schema capable of efficiently storing attendance records, user profiles, and other pertinent information.

- **Enabling real-time update:** Attendance records are updated in real time, ensuring that administrators and stakeholders have the most up-to-date information. This goal focuses on creating a method that automatically updates attendance records to a backend Excel sheet in real time, allowing for easy access and analysis of attendance data.

1.4 PROJECT REPORT ORGANIZATION

The project report is divided into sections that detail the Multi-Factor Attendance System's development, implementation, and evaluation. The report is structured as follows:

- **Introduction:** Motivation, problem statement, project objectives, and overall organization of the report are to be explained in this document.
- **Literature Review:** Existing attendance systems and authentication technologies, along with relevant research studies, are to be explored.
- **System Design and Architecture:** This section will detail system components, technology choices, and overall architecture.
- **Implementation:** The development process, software, hardware components, and solutions to challenges will be described here.
- **Testing and Evaluation:** Methodologies for performance, accuracy, and security testing, along with results and analysis, are to be outlined.
- **Conclusion and Future Work:** Key findings, achievements, and recommendations for future enhancements will be summarized.
- **References:** All sources cited throughout the report will be listed.

2. LITERATURE SURVEY

Face recognition technology has evolved as a critical component in a variety of industries, providing exceptional ease and security. Its applications range from authentication and identity to attendance management systems, where efficient, automated solutions are critical. This introduction lays the ground for a thorough examination of three landmark publications on the use of face recognition technology into attendance management systems. These studies seek to improve attendance tracking systems in educational institutions and businesses by addressing the issues raised by existing manual techniques. This research extends attendance management systems by utilising novel methodologies such as facial recognition combined with audio output, gender classification, and speech recognition, promising increased accuracy, efficiency, and security.

2.1 EXISTING WORK

Face Recognition based Attendance Management System: This paper proposes a class attendance system leveraging face recognition technology to replace manual attendance processes prone to errors and proxy attendance issues. The system consists of four phases: database creation, face detection, recognition, and attendance updating.

- **Database Creation:** Initially, a database is created containing images of students enrolled in the class. Each image serves as a reference point for subsequent recognition tasks.

- **Face Detection:** The system employs Haar-Cascade classifier for face detection. This algorithm is capable of identifying faces within images or video streams, providing the necessary input for the recognition phase.

- **Face Recognition:** Utilizing the Local Binary Pattern Histogram algorithm, the system performs face recognition. This algorithm analyses facial features and patterns to match detected faces with those stored in the database, thereby identifying individual students accurately.

- **Attendance Updating:** Upon successful recognition, the attendance of recognized students is updated in real-time. This ensures accurate tracking of attendance without the need for manual intervention.

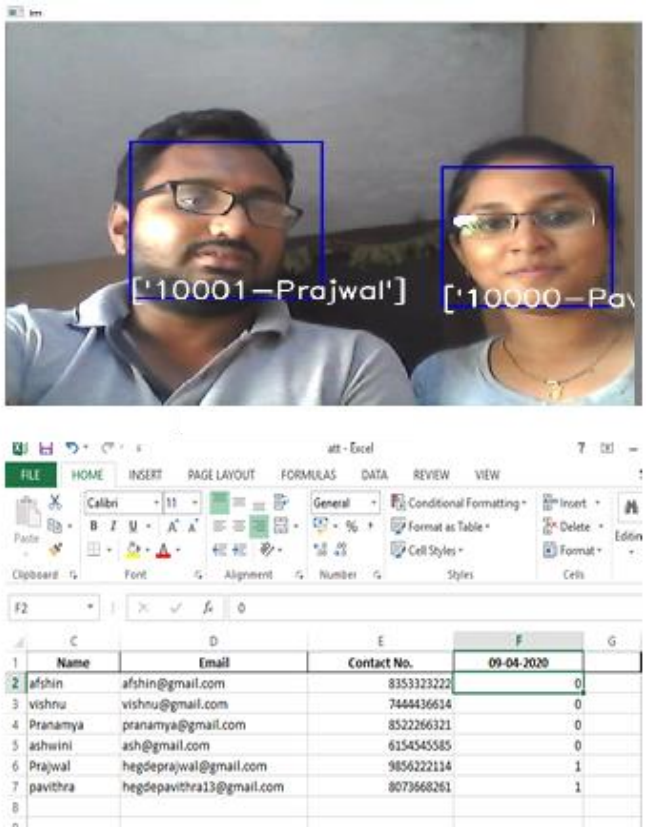


fig. 2.1.1 Sample output from paper

Attendance Monitoring System using Facial Recognition with Audio Output and Gender Classification: Introducing an innovative approach, this paper integrates facial recognition with audio output and gender classification for attendance monitoring. The system aims to enhance accessibility by providing auditory feedback and offers additional insights through gender classification, catering to diverse user needs.

- **Facial Recognition:** Similar to the previous paper, this system employs facial recognition for attendance monitoring. However, it extends the functionality by incorporating audio output for providing auditory feedback during the recognition process.

- **Gender Classification:** In addition to facial recognition, the system includes gender classification capabilities. By analysing facial features, the system can categorize individuals into different gender groups, offering additional demographic insights.

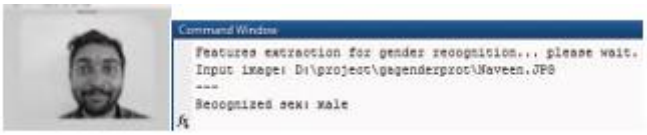


fig.2.1.2 Sample Gender classification output from paper

Smart Attendance System Using Speech Recognition: This paper presents a novel attendance management system utilizing speech recognition technology. By enabling attendance marking through voice commands, the system offers a hands-free, efficient alternative to traditional methods. This approach not only streamlines the attendance process but also addresses potential limitations associated with manual and biometric-based systems.

- **Speech Recognition:** The system utilizes speech recognition algorithms to interpret voice commands for attendance marking. Students can verbally confirm their presence, eliminating the need for manual attendance sheets or biometric scans.

- The integration of speech recognition technology simplifies the attendance process, particularly in environments where hands-free operation is desirable. However, challenges such as accent variability and background noise may impact the accuracy and reliability of speech recognition, necessitating robust algorithmic solutions.

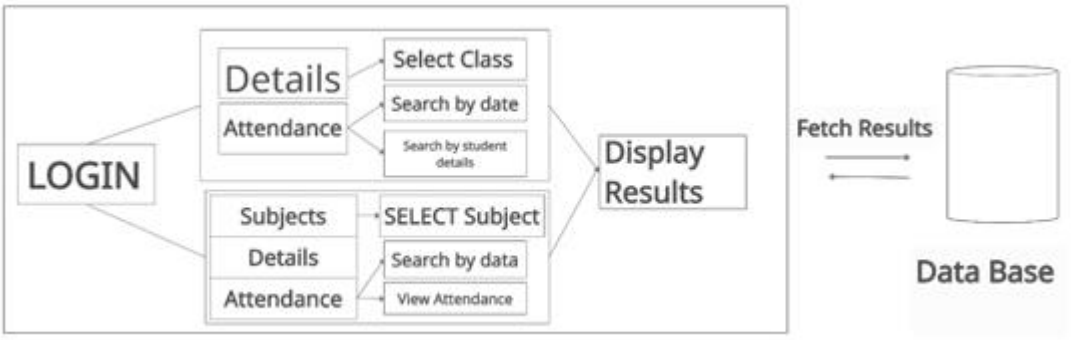


fig. 2.1.3 System architecture

While each paper presents innovative solutions to attendance management, they also highlight specific limitations and challenges associated with the implementation of advanced technologies in real-world scenarios. Addressing these limitations is crucial for the widespread adoption and effectiveness of such systems in educational institutions and workplaces.

2.2 LIMITATIONS OF EXISTING WORK

1) **Reliance on Single Modality:** All three papers primarily rely on a single modality for attendance tracking (facial recognition in the first two papers, speech recognition in the third paper). This reliance may limit the system's robustness in diverse environments or for users with specific needs.

2) **Accuracy Concerns:** The accuracy of the proposed systems, particularly in real-world scenarios with variations in environmental conditions or user characteristics, remains a significant concern. Issues such as variations in lighting conditions, occlusions, accent variability, and speech impediments may impact the accuracy of recognition.

3) **Dependency on Technology Infrastructure:** The effectiveness of these systems heavily depends on the availability and reliability of technology infrastructure, including hardware components (e.g., cameras, microphones) and software algorithms. Any disruptions or failures in these components could hinder the system's functionality.

4) **Accessibility and Inclusivity:** While efforts are made to enhance accessibility through features like audio output in the second paper and speech recognition in the third paper, there may still be accessibility barriers for users with disabilities, such as hearing impairments or speech disorders. Additionally, the reliance on facial recognition may not adequately address the needs of individuals with certain facial characteristics or conditions.

5) **Ethical and Privacy Considerations:** The use of biometric technologies, such as facial and speech recognition, raises ethical concerns related to privacy, consent, and potential biases. There is a need for careful consideration of ethical implications and the implementation of appropriate safeguards to protect users' privacy and rights.

6) **Scalability and Deployment Challenges:** Deploying these systems at scale, particularly in large educational institutions or workplaces, may pose challenges related to scalability, network bandwidth, and resource allocation. Additionally, integrating these systems with existing infrastructure and workflows could require significant time and effort.

3. PROPOSED WORK

The proposed work entails the development and implementation of a Multi-Factor Attendance System that addresses the surging demand for advanced attendance management solutions. The system integrates multiple authentication factors to ensure comprehensive user verification and enhance security measures.

- **Multi-Layered Authentication Process**

  The system employs a multi-layered authentication process comprising barcode scanning, facial recognition with anti-spoofing analysis, and voice matching. Each participant undergoes swift barcode scans to receive a unique identifier, followed by facial recognition and gesture analysis to fortify authentication. Voice matching further enhances security, ensuring resilience against unauthorized access attempts.

- **Centralized Database Management**

  A centralized database efficiently manages user information, storing biometric data, unique identifiers, and attendance records. This centralized approach facilitates seamless integration and access to user data across different modules of the system.

- **Real-Time Attendance Updates**

  Upon successful verification, attendance data is instantly updated to a backend Excel sheet in real-time. This eliminates the need for manual data entry, reducing the likelihood of errors and ensuring accurate and up-to-date attendance records.

- **Insights into Attendance Trends and Patterns**

  One of the standout features of the system is its ability to provide valuable insights into attendance trends and patterns. By analysing attendance data collected over time, the system offers valuable insights to educational institutions, enabling informed decision-making and contributing significantly to their technological advancement.

3.1 Comparison of Proposed Vs Existing work

Table 3.1.1 Comparison Table

Aspect	Proposed Multi-Factor Attendance System	Existing Works
Authentication Methods	Barcode scanning, facial recognition with anti-spoofing analysis, voice matching	Primarily facial recognition; some include additional features such as audio output, gender classification, and speech recognition
Multi-Factor Authentication	Yes	Only in few
Database Management	Centralized database management	No real time data update
Insights into Attendance Trends and Patterns	Yes	No Attendance analysis done
Accessibility and Inclusivity	Potential limitations depending on the implementation of voice matching	Efforts made to enhance accessibility through features like audio output and speech recognition
Complexity and Cost	May require higher development and maintenance costs due to multi-factor authentication	Complexity may vary depending on the integration of additional features; potential cost implications

3.2 ADVANTAGES OF PROPOSED WORK

The proposed Multi-Factor Attendance System offers several advantages over traditional and existing attendance management systems:

1) **Enhanced Security:** By employing multiple authentication factors such as barcode scanning, facial recognition with anti-spoofing analysis, and voice matching, the system ensures robust security measures, making it more difficult for unauthorized access or fraudulent attendance.

2) **Comprehensive User Verification:** The multi-layered authentication process provides comprehensive user verification, minimizing the likelihood of false positives or unauthorized access. This ensures that only authenticated users are granted access to attendance records and facilities.

3) **Real-Time Updates:** The system facilitates real-time attendance updates, eliminating the need for manual data entry and ensuring that attendance records are accurate and up-to-date. This feature enhances efficiency and reduces administrative overhead.

4) **Centralized Database Management:** With centralized database management, the system efficiently stores and manages user information, including biometric data and attendance records. This centralized approach streamlines data access and ensures data integrity.

5) **Insights into Attendance Trends and Patterns:** The system's ability to provide valuable insights into attendance trends and patterns enables educational institutions and organizations to make informed decisions regarding attendance management, resource allocation, and academic planning.

6) **Minimized Errors:** By automating the attendance tracking process and reducing manual intervention, the system minimizes the likelihood of errors and inaccuracies in attendance records. This enhances the reliability and integrity of attendance data.

4. SYSTEM REQUIREMENTS

4.1 FUNCTIONAL REQUIREMENTS

- **Faculty Registration and Authentication**

  Faculty should be able to create accounts and log in securely.

- **Student attendance management**
  - Ability to record student attendance for each class or session.
  - Implement appropriate security measures to protect student data and ensure only authorized personnel have access to attendance records.

- **Barcode recognition with Database**
  - The scanner reads the barcode and converts it into a digital format that the computer can understand. This usually involves decoding the barcode data into alphanumeric characters.
  - A database is setup to store information about Students and Faculty, including their barcode data and other relevant details such as name, ID, etc.

- **Face recognition or voice recognition**
  - Students and Faculty can mark their attendance simply by looking at the device or speaking, which can be particularly useful in scenarios where hands-free operation is important.
  - The face or voice recognition algorithms can achieve high accuracy rates.

- **Database management**
  - Managing attendance through a database system is a common and efficient way to keep track of attendance records.
  - Implement authentication mechanisms to ensure that only authorized users can access and modify attendance data.

- **User Friendly webpage**
    - Design an intuitive and user-friendly web application.
    - Ensure easy navigation, clear instructions, and user support features.

4.2 NON-FUNCTIONAL REQUIREMENTS

- **Performance**
    - The system should provide accurate record of tracking attendance for monitoring student engagement and participation.
    - It should handle concurrent user interactions efficiently.

- **Scalability**
    - Design the system to accommodate a growing user base and increasing data volume.
    - Ensure scalability to meet potential future demands.

- **Accuracy**
    - An accurate attendance system ensures fairness by accurately reflecting students' attendance records.
    - Minimize false positives and false negatives in Tracking.

- **Usability**
    - The user interface should be intuitive and accessible to a diverse user base.
    - Consider usability testing and user feedback for continuous improvement.

- **Reliability**
    - Ensure system uptime and consistency in recording student’s attendance.
    - Implement backup and recovery mechanisms to prevent data loss.

4.3 TECHNOLOGY DESCRIPTION

1. Python

fig. 4.3.1 Python logo

Python is a popular high-level programming language known for its simplicity, readability, and extensive standard library. With clean syntax and dynamic typing, it's widely used for web development, data analysis, and machine learning. Python's versatility, cross-platform support, and thriving community make it a top choice for developers.

2. MySQL

fig. 4.3.2 MySQL logo

MySQL is an open-source relational database management system (RDBMS) used across various applications including web development, e-commerce, and data analytics. It ensures data integrity, scalability, and performance optimization. Known for its speed, reliability, and compliance with ANSI SQL standards, MySQL offers high availability solutions like MySQL Router and Group Replication.

3. PyQt Designer

fig. 4.3.3 PyQt Designer logo

PyQt Designer is a visual tool for PyQt, simplifying UI design with a drag-and-drop interface. It generates XML-based UI files for PyQt applications, speeding up development by eliminating manual coding. PyQt Designer enhances productivity and accelerates the creation of PyQt-based GUI applications.

4. VScode

fig.4.3.4 VScode logo

Visual Studio Code (VSCode), developed by Microsoft, is a lightweight and versatile integrated development environment (IDE) popular among developers. It offers efficiency, extensibility, and customization through numerous extensions available in its marketplace. Key features include a powerful code editor, debugging support, and integrated version control.

5. Fundamental technologies for web development

fig. 4.3.5 Web technology fundamentals

HTML, CSS, and JavaScript are the cornerstone technologies of web development. HTML defines the structure and content of web pages, CSS controls their visual presentation and layout, while JavaScript adds interactivity and dynamic behaviour to enhance user experience.

6. Wamp Server

fig. 4.3.6 wamp server logo

WampServer is a Windows software stack for local web development, offering Apache, MySQL, and PHP. It includes tools like phpMyAdmin and OpenSSL, with a central control panel for managing services and configurations.

4.4 HARDWARE REQUIREMENTS

- **Processor:** The system should run on a processor with sufficient processing power, such as an Intel Core i5 or equivalent, to handle the computational requirements of biometric authentication and data processing.

- **RAM:** A minimum of 8GB of RAM is recommended to ensure smooth operation and efficient data processing within the system.

- **Storage:** The system should be installed on a Solid-State Drive (SSD) with a capacity of at least 256GB to accommodate the software components, attendance data, and system logs.

- **Webcam:** A high-quality webcam is essential for facial recognition processes. The webcam captures live video streams for facial detection and recognition algorithms to identify users accurately.

- **Microphone:** A microphone is required for voice verification processes. The system analyses vocal characteristics using the microphone to verify the identity of users during attendance marking.

- **Network Connectivity:** The system should support Ethernet or Wi-Fi connectivity for seamless data exchange between devices and the central database. Reliable network connectivity is essential for real-time updates and data synchronization.

4.5 TECH STACK

- Programming language →Python
- Development Framework →PyQt Designer
- Database → MySQL
- IDE →VScode
- Data visualization → matplotlib
- Operating System → Window 11
- Model Development → MobileFaceNet, MiniFASNetV

5. DESIGN

5.1 SYSTEM ARCHITECTURE

1) Components of the System Architecture

- **Facial Recognition:** Utilizes webcam for facial detection and identification.
- **Voice Matching:** Incorporates microphone for voice-based user verification.
- **Barcode Scanning:** Implements barcode scanning engines for quick data decoding.
- **Central Database:** Managed by a DBMS for storing attendance data and enabling real-time updates.
- **Web Server:** Hosts the system for user access and interaction with attendance management features.

2) Security Measures

- **Role-Based Access Control:** Regulates user permissions based on roles within the institution.
- **Encryption:** Protects data integrity and confidentiality through encryption techniques.

3) Scalability and Performance

- **Scalability Enhancements:** Designed to accommodate varying workloads and user demands.
- **Responsive Data Processing:** Prioritizes efficient data processing for real-time updates and user interactions.

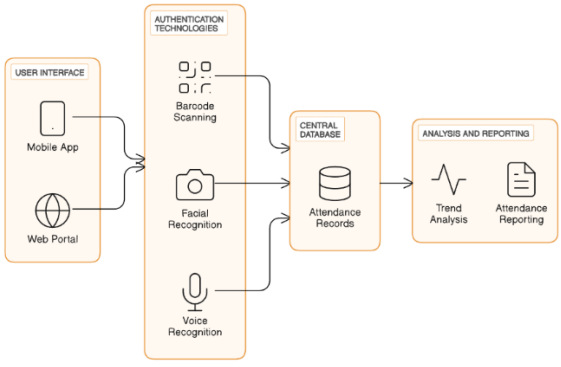


fig. 5.1 System Architecture

5.2 PROCESS DIAGRAM

The process diagram in the Multi-Factor Attendance System outlines the workflow of the system, detailing the steps from user interaction to data processing and storage.

1) **User Interaction**
   - Users, including faculty members and students, interact with the system through the user interface.
   - The user interface provides a platform for users to access attendance-related functionalities and features.

2) **Input Data Capture**
   - The system captures input data from users for authentication and attendance marking.
   - Input data may include biometric information such as facial features, voice patterns, or barcode scans.

3) **Biometric Engines**
   - The input data is processed by biometric recognition engines for authentication and verification.
   - Different biometric engines handle facial recognition, voice matching, and barcode scanning based on user preferences.

4) **Decision Making**
   - Based on the biometric data captured and processed, the system makes decisions regarding user authentication and attendance marking.
   - Decisions may include verifying user identity, marking attendance, or updating attendance records in the central database.

5) **Existing vs. New Users**
   - The system distinguishes between existing users (those with registered biometric data) and new users (those undergoing registration).
   - Existing users may proceed directly to authentication, while new users may need to register their biometric information first.

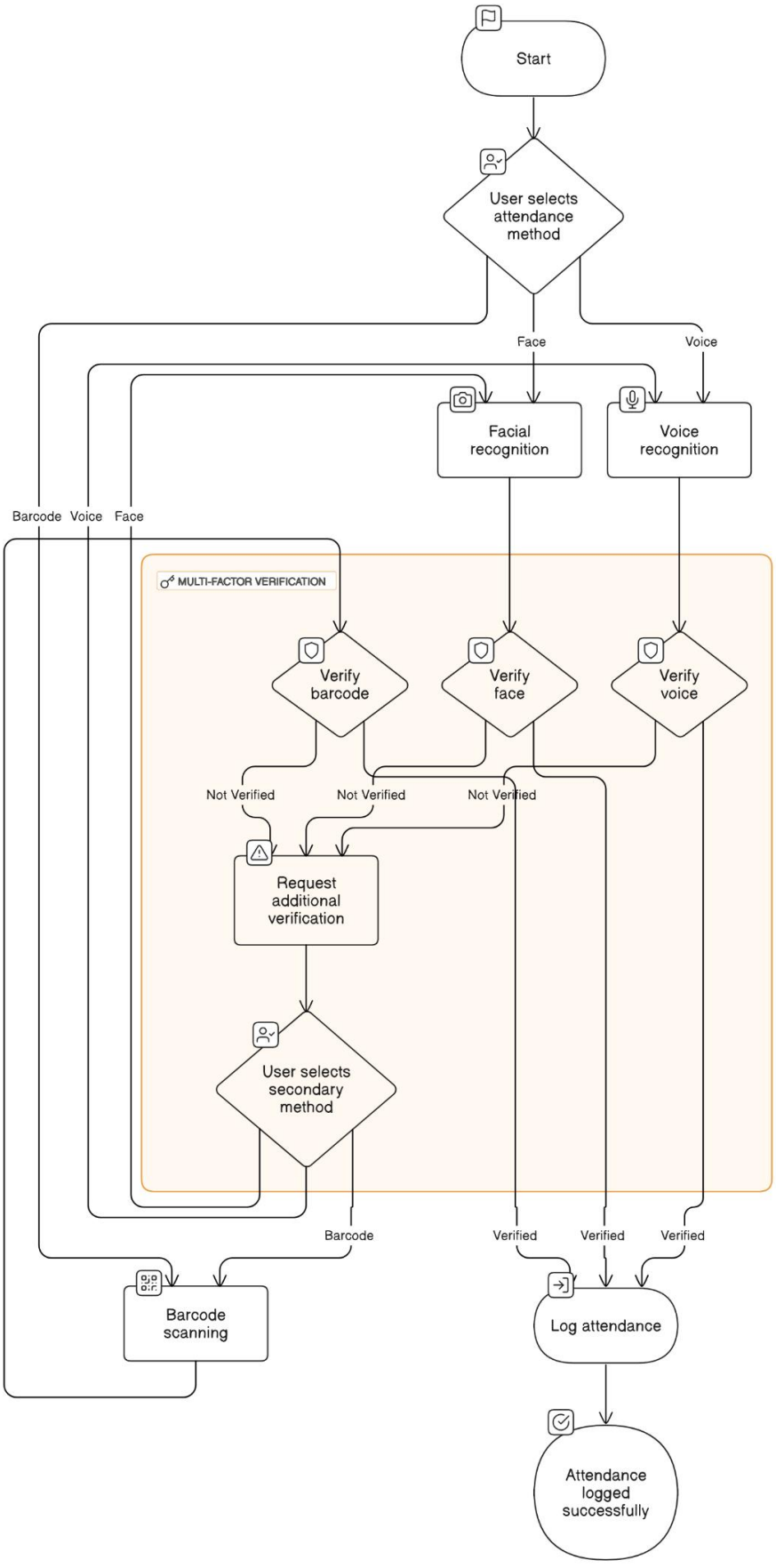


fig. 5.2 Process Diagram

6) **Authentication and Registration**

- Authentication involves verifying the identity of users based on their biometric data.
- Registration includes enrolling new users into the system by capturing and storing their biometric information.

7) **Data Processing**

- Processed biometric data is used for attendance marking and updating attendance records.
- The system ensures accuracy and consistency in processing data to maintain reliable attendance tracking.

8) **Storage and Retrieval**

- Attendance data, including timestamps, user identification, and metadata, is stored in the central database.
- The database facilitates efficient storage and retrieval of attendance-related information for analysis and reporting.

9) **Insightful Information**

- Real-time attendance updates and insightful information on attendance trends and patterns are provided by the central database.
- Educational institutions can leverage this information to enhance operational efficiency and optimize attendance management strategies.

10) **System Functionality**

- The process diagram highlights key system functionalities, including user authentication, attendance marking, data processing, and storage.
- It illustrates the flow of actions and interactions within the Multi-Factor Attendance System, guiding users through the attendance management process.

5.3 USER FLOW DIAGRAM

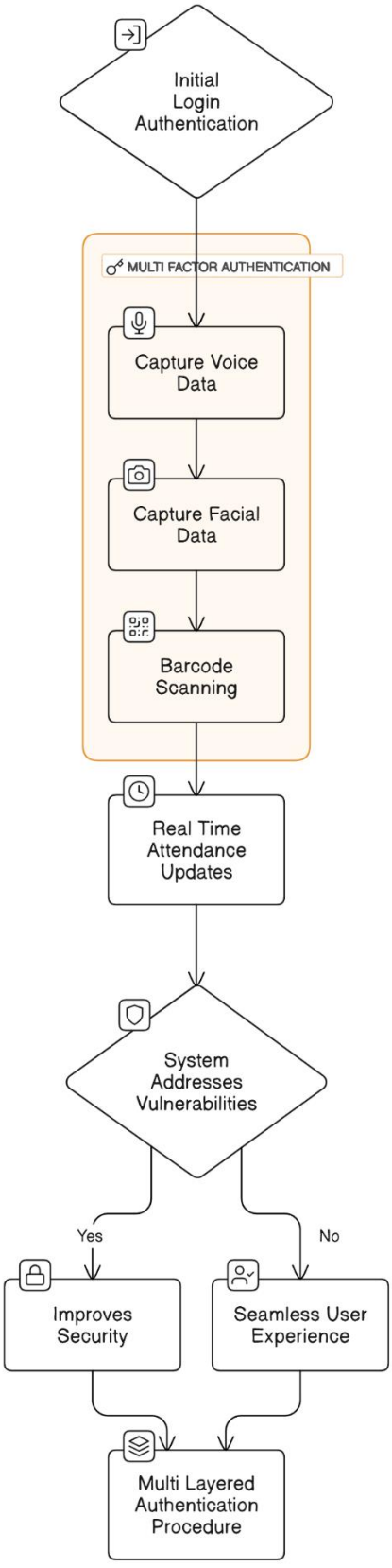


fig. 5.3 User Flow Diagram

1) **Access System**
   - Users access the attendance system through a designated platform, such as a mobile app or a web portal.
   - They may be required to enter their login credentials, such as username and password, to authenticate themselves.

2) **Scan Identifier**
   - Upon accessing the system, users are prompted to scan their unique identifier, typically in the form of a barcode or QR code.
   - They locate the designated scanner or area equipped with a barcode reader and present their identifier for scanning.

3) **Face Recognition**
   - After successful scanning, users' faces are captured by a camera integrated into the system.
   - The system performs facial recognition analysis to verify the user's identity based on pre-registered facial features.

4) **Voice Verification**
   - As an additional layer of security, users may be prompted to provide a voice sample or passphrase for verification.
   - Speech recognition technology analyses the user's voice and matches it against pre-registered voice patterns.

5) **Confirmation**
   - Upon successful authentication through all layers, users receive a confirmation message indicating that their attendance has been recorded.
   - The confirmation message may include details such as the time and location of the attendance mark.

6) **Real-Time Update**
   - Attendance data is instantly updated in the system's backend database, ensuring real-time accuracy of attendance records.

5.4 CLASS DIAGRAM

Class diagram illustrates the architecture of a revolutionary Multi-Factor Attendance System, designed to address the surging demand for advanced attendance tracking solutions. This system integrates barcode scanning, facial recognition with anti-spoofing analysis, and voice matching to provide comprehensive user verification. Through a multi-layered authentication process, it ensures heightened security and resilience against unauthorized access. The system efficiently manages user information in a centralized database and updates attendance in real-time to a backend Excel sheet, minimizing manual data entry and reducing errors. Additionally, it offers valuable insights into attendance trends and patterns, contributing significantly to the technological advancement of educational institutions.

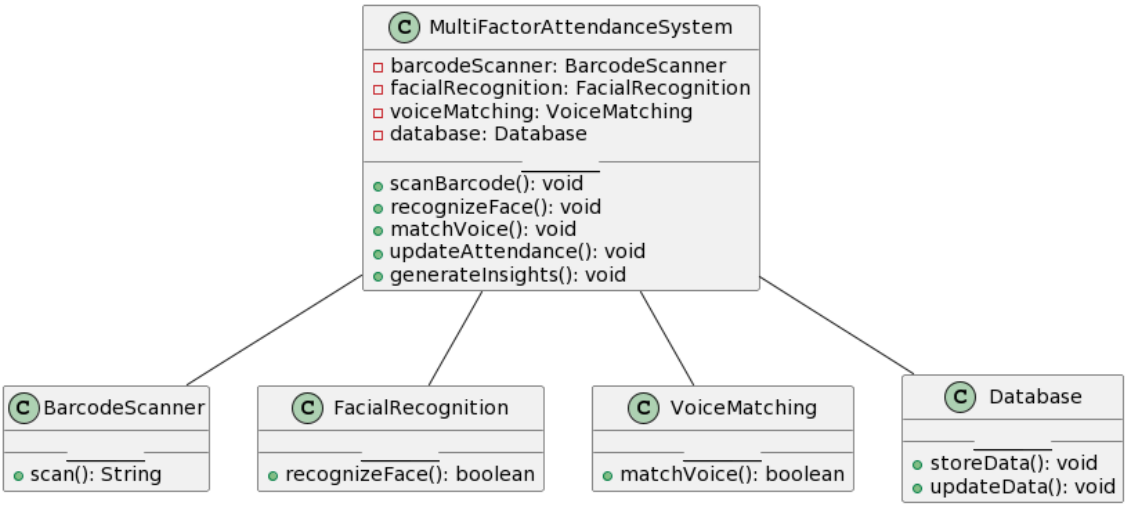


fig.5.4 Class Diagram

5.5 USE CASE DIAGRAM

The Use Case Diagram illustrates the interactions between users and the key functionalities of the Multi-Factor Attendance System. Users interact with the system through barcode scanning, facial recognition, anti-spoofing analysis, and voice matching modules. These modules authenticate user identities and update attendance data in real-time through centralized database management. Additionally, the system offers insights into attendance trends and patterns, aiding educational institutions in efficient attendance management and technological advancement.

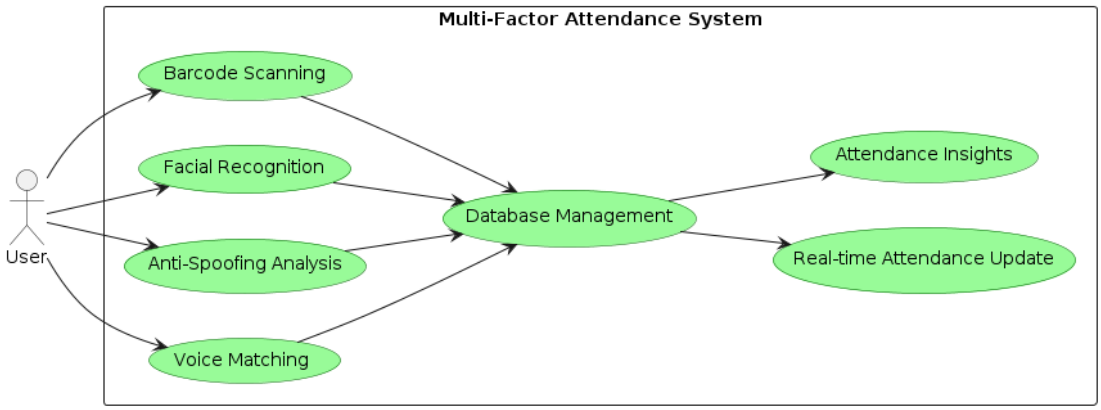


fig.5.5 Use case diagram

5.6 ACTIVITY DIAGRAM

Activity diagram illustrates the sequential steps involved in the authentication process of the Multi-Factor Attendance System. Each step contributes to the comprehensive verification of users, ensuring heightened security and resilience against unauthorized access.

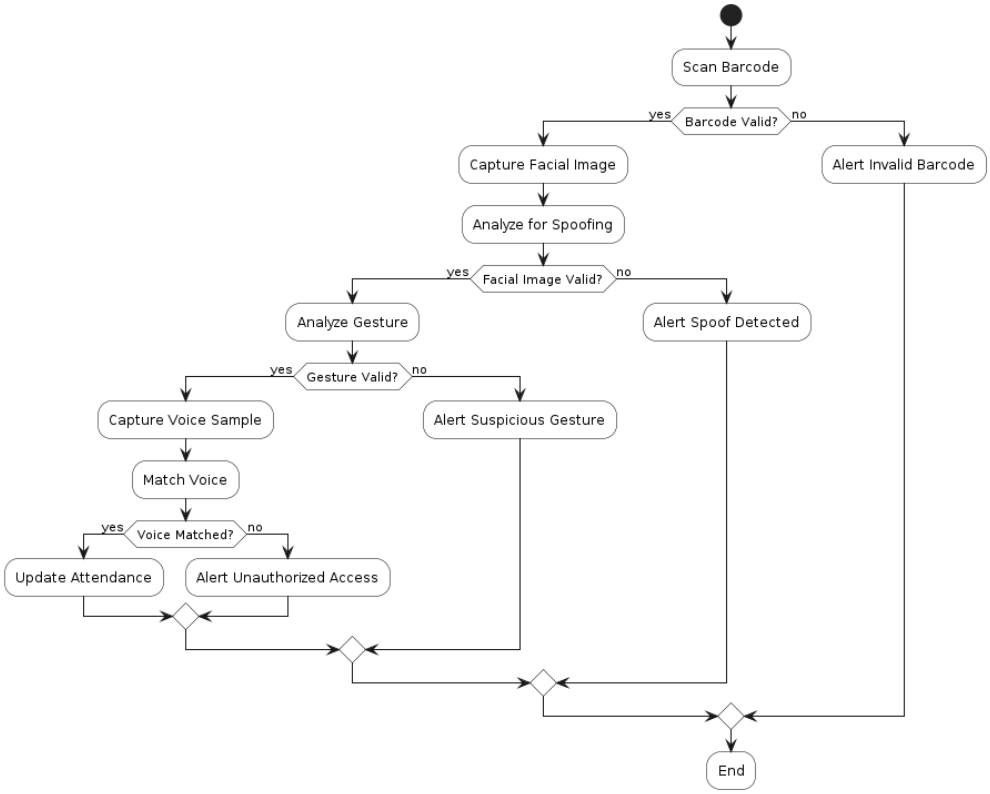


fig.5.6 Activity Diagram

5.7 SEQUENCE DIAGRAM

Sequence diagram depicts the interactions between the user and the Multi-Factor Attendance System during the authentication process. Each step, from barcode scanning to voice matching, contributes to ensuring comprehensive user verification and enhanced security within educational institutions.

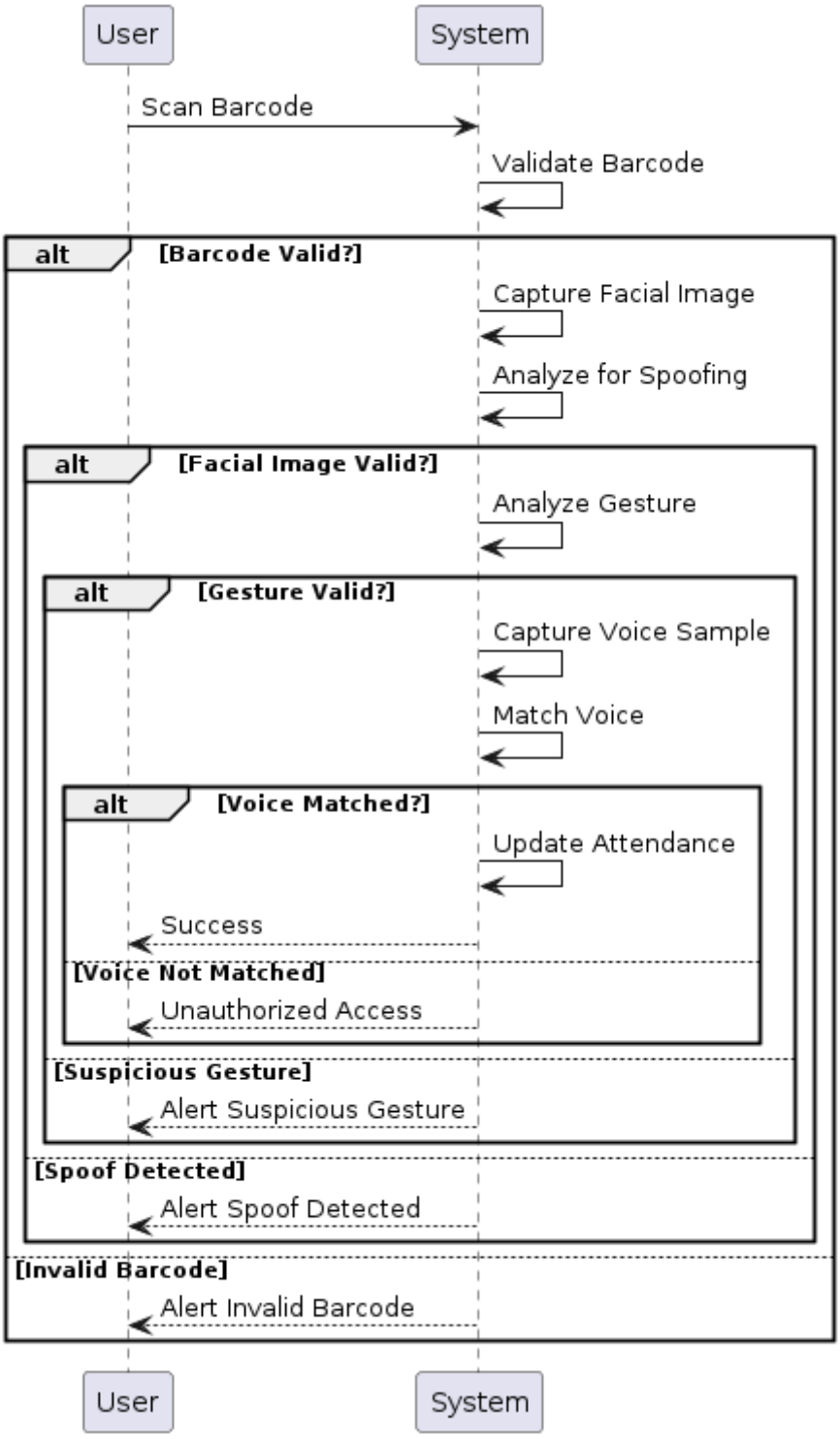


fig.5.7 Sequence Diagram

5.8 UML DIAGRAM

fig. 5.8 UML Diagram

5.9 ER SCHEMA DIAGRAM

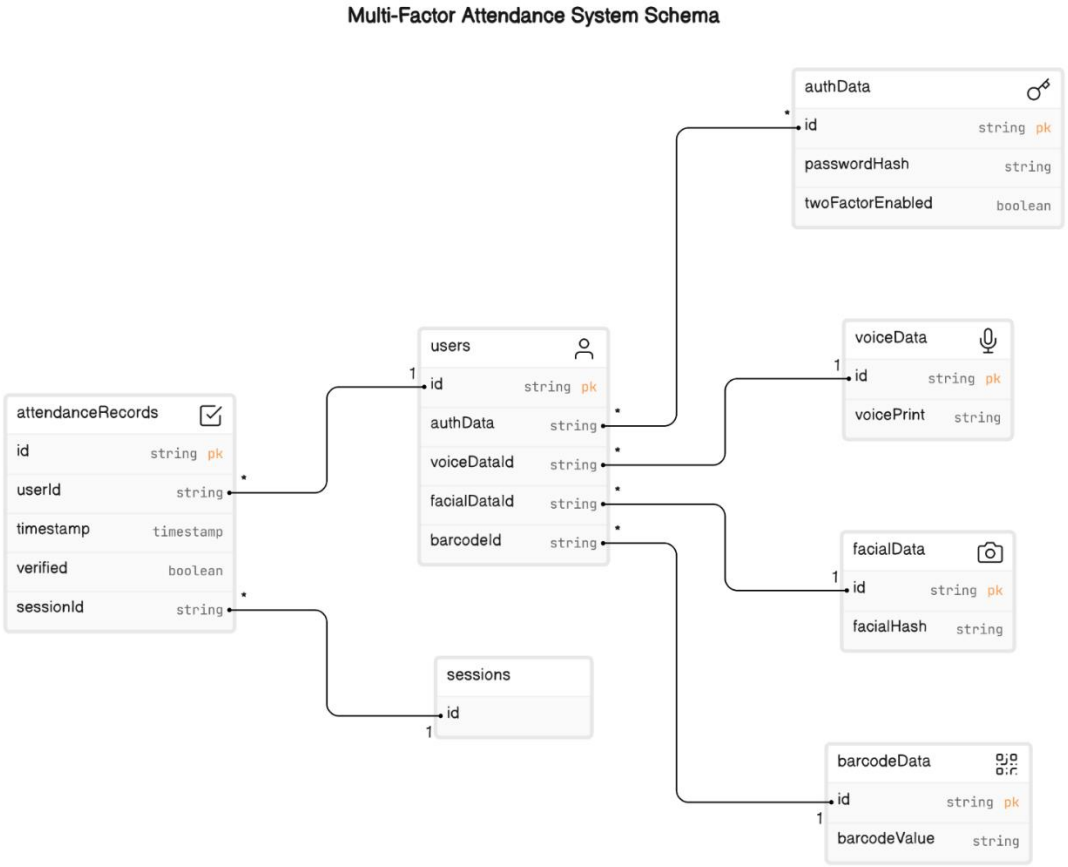


fig. 5.9 ER Schema Diagram

6. IMPLEMENTATION

6.1 BARCODE SCANNING

Barcode scanning is a technology that enables the automatic identification and capture of data encoded in barcode symbols. Barcodes are graphical representations of data, typically printed in the form of parallel lines or patterns that can be easily scanned and decoded by barcode readers or scanners. They are widely used across various industries for inventory management, product tracking, point-of-sale transactions, and more.

There are several types of barcodes symbologist, each with its own set of characteristics and applications. Some common barcode types include:

1) **UPC (Universal Product Code):** Used primarily in retail for product identification and inventory management.
2) **QR Code (Quick Response Code):** Known for its high data capacity and versatility, QR codes are used for various applications, including marketing, ticketing, and contactless payments.
3) **Code 128:** Widely used in logistics and shipping for encoding alphanumeric data, such as product codes and batch numbers.
4) **EAN (European Article Numbering):** Similar to UPC, EAN barcodes are used for product identification in retail and supply chain management.

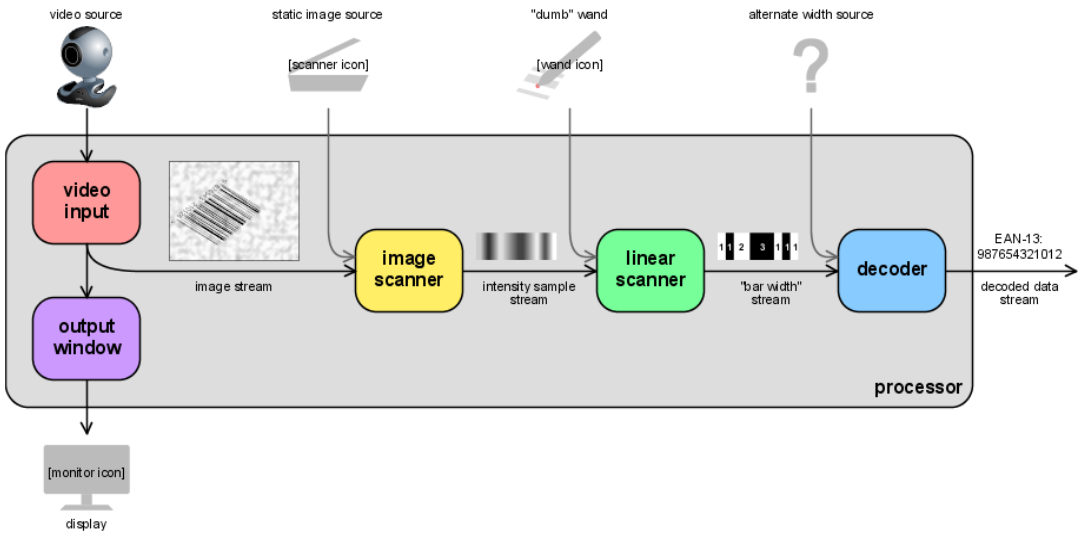


fig. 6.1.1 Internal Process of Barcode scanning

Process of barcode scanning using a camera

1) **Camera Initialization:** The camera is activated and configured to capture images or video streams suitable for barcode recognition.

2) **Barcode Detection:** Image processing algorithms analyse the camera feed to locate and identify potential barcode symbols within the captured images.

3) **Barcode Decoding:** Decoding algorithms interpret the pattern of lines and spaces within the barcode symbol to extract the encoded data.

4) **Data Extraction:** The decoded data is extracted from the barcode symbol and made available for further processing or display.

5) **Validation and Error Handling:** The extracted data may undergo validation checks to ensure its accuracy and integrity. Error handling mechanisms address issues such as unreadable or damaged barcodes.

6) **Integration with Application:** The extracted barcode data is integrated into the application or system where it is intended to be used, such as inventory management software or point-of-sale systems.

7) **Feedback and Confirmation:** Visual or auditory feedback confirms successful barcode scanning to the user, indicating that the encoded data has been successfully captured and processed.

8) **Optional: Advanced Features:** Additional features such as batch processing, multi-barcode recognition, or real-time tracking may be implemented depending on the requirements of the application.

9) **Optimization and Performance:** Continuous optimization efforts aim to improve the speed and accuracy of barcode scanning algorithms under various conditions, including different lighting and barcode sizes.

6.2 ANTI SPOOFING FACE RECOGNITION

Anti-spoofing face recognition is a crucial component of modern facial recognition systems designed to prevent unauthorized access and ensure the integrity of identity verification processes. The internal process of anti-spoofing face recognition involves several steps and techniques aimed at detecting and mitigating attempts to deceive the system using spoofing attacks.

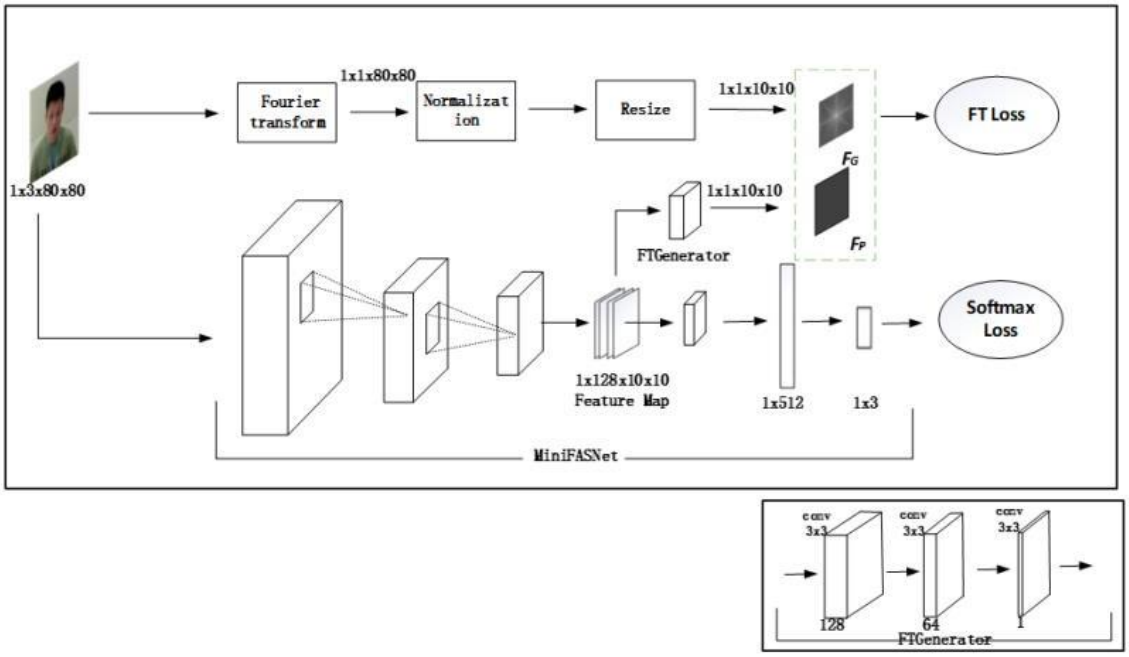


fig. 6.2.1 Anti Spoofing Face Recognition Architecture

1) Image Acquisition

- The process begins with the acquisition of facial images from the input source, such as a camera or image database.
- The images captured should have sufficient quality and resolution for effective facial feature extraction and analysis.

2) Pre-processing

- Pre-processing techniques are applied to the acquired facial images to enhance their quality and suitability for subsequent processing.

- Common pre-processing steps include noise reduction, image normalization, and alignment to ensure consistency in facial orientation and scale.

3) **Feature Extraction**
   - Feature extraction algorithms analyse the pre-processed facial images to identify distinctive features or landmarks that characterize the individual's face.
   - Various techniques, such as local binary patterns (LBP), histogram of oriented gradients (HOG), or deep learning-based approaches, may be employed for feature extraction.

4) **Spoof Detection**
   - Spoof detection algorithms assess the authenticity of the facial images to differentiate genuine faces from spoofed or fraudulent ones.
   - These algorithms analyse specific characteristics or artifacts associated with spoofing attacks, such as texture patterns, lack of 3D depth, or unnatural reflections.

Common spoof detection methods include

- **Texture Analysis:** Analysing texture patterns to distinguish real faces from printed images or masks.
- **Motion Analysis:** Detecting motion or changes in facial features to identify live faces.
- **Depth Analysis:** Assessing the depth information in facial images to detect flat surfaces or lack of 3D structure.
- **Reflection Analysis:** Analysing reflections or specular highlights to detect the presence of glass or glossy surfaces.

5) **Classification**
   - The extracted features are used to classify facial images as either genuine or spoofed based on predefined criteria or models.

- Machine learning algorithms, such as support vector machines (SVM), random forests, or convolutional neural networks (CNNs), are commonly used for classification tasks.

6) Decision Making

- Based on the classification results, a decision is made regarding the authenticity of the facial images.
- Genuine faces are accepted for further processing, while spoofed faces are rejected or flagged for further scrutiny.

7) Integration with Face Recognition System

- The output of the anti-spoofing process is integrated into the overall face recognition system to enhance its security and reliability.
- Genuine faces passing the anti-spoofing checks proceed to the face recognition stage for identity verification.

8) Feedback and Adaptation

- Feedback mechanisms monitor the performance of the anti-spoofing system and provide input for continuous improvement.
- Adaptive algorithms may be employed to update the spoof detection models based on new data or emerging spoofing techniques.

6.3 VOICE VERIFICATION

The internal process of voice verification using Google API involves several steps within the Google Cloud ecosystem, particularly leveraging services such as Google Cloud Speech-to-Text and Google Cloud Text-to-Speech.

The internal process of voice verification using Google API involves the following steps:

1) **Recording Voice Input**
   - Users provide their voice input by speaking into a microphone or audio recording device.
   - The voice input typically contains phrases, commands, or specific keywords required for verification.

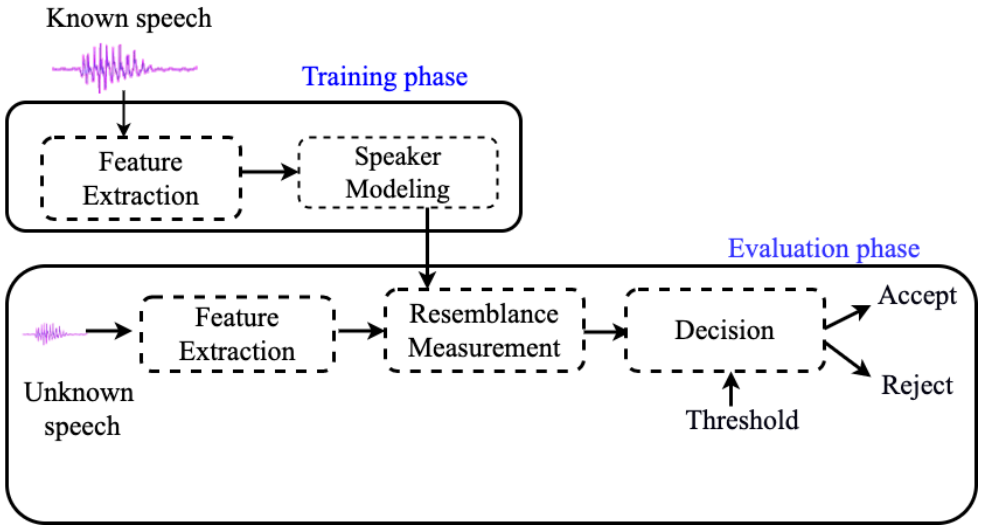


fig. 6.3.1 Internal process of Voice Verification

2) **Audio Encoding**
   - The raw audio data captured from the voice input is encoded into a digital format suitable for processing and transmission.
   - Common formats include WAV or FLAC.

3) **Google Cloud Speech-to-Text (STT)**
   - The encoded audio data is sent to the Google Cloud Speech-to-Text (STT) API for transcription into text.

- Machine learning models analyse the audio and convert spoken words into text.

4) Text Pre-processing

- The transcribed text may undergo pre-processing steps to enhance accuracy and suitability for verification.
- This may involve removing punctuation, normalizing case, or filtering out irrelevant words.

5) Voiceprint Comparison

- The pre-processed text is compared against pre-registered voiceprints or passphrase samples associated with the user's identity.
- Voiceprints are unique representations of vocal characteristics extracted from recorded voice samples.

6) Verification Decision

- Based on the comparison results, a decision is made regarding the authenticity of the user's voice.
- If the transcribed text matches the expected voiceprint or passphrase within an acceptable margin of error, verification is considered successful.

7) Response Generation

- A response indicating the outcome of the verification process is generated.
- Depending on the result, the response may include a confirmation message or prompt the user to retry or use alternative verification methods.

8) Google Cloud Text-to-Speech (TTS)

- Optionally, a synthesized speech response is generated using the Google Cloud Text-to-Speech (TTS) API.
- The response text is converted into natural-sounding speech audio, which can be played back to the user.

9) Feedback and Adaptation

- Feedback mechanisms monitor system performance and provide input for continuous improvement.
- Adaptive algorithms may update voiceprint models or refine verification criteria based on new data or user feedback.

10) Security Considerations

- Measures are implemented to protect voice data and ensure data security and privacy.
- Encryption, authentication, and access control mechanisms safeguard voice recordings and verification results within the Google Cloud environment.

6.4 DATABASE MANAGEMENT

The central database architecture process involves designing, implementing, and managing a centralized database system to efficiently store, organize, and manage data for an application or organization.

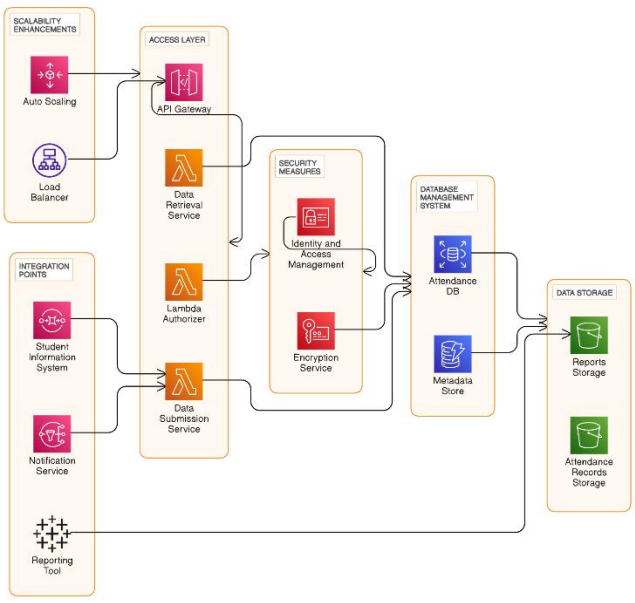


fig. 6.4.1 Database architecture

1) **Requirement Analysis and Schema Design**
    - This step involves understanding the data needs and requirements of the application or organization.
    - Data modelling techniques are used to design a database schema that defines the structure, relationships, and constraints of the data to be stored.

2) **Selection and Implementation of DBMS**
    - A suitable database management system (DBMS) is selected based on factors such as scalability, performance, and compatibility.
    - The designed database schema is implemented within the chosen DBMS environment, creating tables, defining data types, and establishing relationships.

3) **Data Population and Optimization**
    - Initial data is populated into the database from various sources, ensuring data consistency and integrity.
    - Performance optimization techniques such as indexing, query optimization, and data partitioning are applied to enhance database performance.

4) **Security and Access Control**
    - Security measures are implemented to protect data from unauthorized access, manipulation, or theft.
    - Access control mechanisms such as authentication and authorization are established to control who can access the database and what actions they can perform.

5) **Backup, Disaster Recovery, and Maintenance**
    - Backup and disaster recovery strategies are put in place to ensure data availability and business continuity in case of system failures or disasters.
    - Routine maintenance tasks such as data backups, software updates, and performance monitoring are performed to keep the database healthy and operational.

7. TESTING

7.1 UNIT TESTING

Unit testing for the Multi-Factor Attendance System would involve testing individual components or units of the system in isolation to ensure they function correctly.

1. **Barcode Scanning**
    - Test that the barcode scanning module correctly reads and validates barcodes.
    - Test various scenarios including valid barcodes, invalid barcodes, and edge cases.

2. **Facial Recognition**
    - Test that the facial recognition module accurately captures and analyses facial images.
    - Test for spoof detection to ensure it can detect attempts to spoof the system.
    - Test various lighting conditions, angles, and facial expressions.

3. **Gesture Analysis**
    - Test that the gesture analysis module correctly interprets user gestures.
    - Test for valid and invalid gestures, as well as edge cases.
    - Ensure that suspicious gestures are detected and handled appropriately.

4. **Voice Matching**
    - Test that the voice matching module accurately captures and matches voice samples.
    - Test for voice samples from authorized and unauthorized users.
    - Ensure that unauthorized users are detected and rejected.

7.2 INTEGRATION TESTING

Test the integration of all authentication modules to ensure seamless interaction. Test different combinations of valid and invalid inputs to simulate real-world scenarios.

1. **Data Management**
    - Test the functionality of the centralized database for managing user information.
    - Verify that user information is stored and retrieved correctly.
    - Test for data consistency and integrity.

2. **Attendance Update**
    - Test the functionality of updating attendance records in real-time.
    - Verify that attendance records are updated accurately upon successful verification.
    - Test for handling errors and exceptions during the update process.

3. **Insights Generation**
    - Test the generation of attendance trends and patterns.
    - Verify that insights are accurate and provide meaningful information.
    - Test for various data sets to ensure robustness.

4. **Error Handling**
    - Test the system's response to unexpected errors and edge cases.
    - Ensure that appropriate error messages are displayed or logged.
    - Test for resilience and graceful degradation under adverse conditions.

5. **Performance Testing**
    - Test the system's performance under various load conditions.
    - Measure response times for different operations and ensure they meet performance requirements.
    - Identify and optimize any bottlenecks in the system.

7.3 TEST CASE SCENARIOS

Table 7.3.1 Test Case Scenarios

Test Case	Input	Expected Output	Status
Valid Barcode	Valid barcode	Barcode recognized, proceed to next step	Passed
Invalid Barcode	Invalid barcode	Error message displayed	Passed
Valid Facial Image	Valid facial image	Facial image recognized, proceed to next step	Passed
Spoof Detection	Spoofed facial image	Spoof detected, alert displayed	Passed
Voice Matching Authorized User	Voice sample from authorized user	Voice matched, proceed to next step	Passed
Voice Matching Unauthorized User	Voice sample from unauthorized user	Voice not matched, unauthorized access alert	Passed
Data Management User Information Retrieval	Query for user information	User information retrieved correctly	Passed
Data Management User Information Update	Update user information	User information updated correctly	Passed
Error Handling Unexpected Error	Unexpected error during authentication process	Appropriate error message displayed	Passed

8. MODELS AND EVALUATION

8.1 BARCODE SCAN MODELS

Training a model for barcode scanning typically involves using existing libraries or frameworks such as ZBar, ZXing, or Dynamsoft Barcode Reader, which provide pre-trained models for barcode recognition. These libraries utilize machine learning algorithms and computer vision techniques to detect and decode barcodes from images or video streams.

1) **ZBar**
   - ZBar is an open-source software suite for reading barcodes from various sources such as image files, video streams, or webcam feeds.
   - Training a model with ZBar typically involves configuring the library to recognize specific barcode symbologies (e.g., UPC, QR code, Code 128) and optimizing parameters for barcode detection and decoding.
   - ZBar provides documentation and examples for customizing settings and fine-tuning the performance of the barcode scanning process.

2) **ZXing (Zebra Crossing)**
   - ZXing is an open-source library for barcode scanning and generation, originally developed by Google.
   - Training a model with ZXing involves configuring the library to recognize different barcode formats and optimizing parameters for accurate detection and decoding.
   - ZXing supports a wide range of barcode types, including UPC, EAN, QR code, Code 39, and more, making it suitable for various applications.
   - The library provides APIs for integrating barcode scanning functionality into Android, iOS, and Java-based applications.

3) **Dynamsoft Barcode Reader**
   - Dynamsoft Barcode Reader is a commercial barcode scanning SDK that offers high-performance barcode recognition capabilities for web, desktop, and mobile applications.

- Training a model with Dynamsoft Barcode Reader involves configuring the SDK to recognize specific barcode symbologies and optimizing settings for performance and accuracy.
- The SDK provides comprehensive documentation, tutorials, and support resources to assist developers in integrating barcode scanning functionality into their applications.

8.2 FACE RECOGNITION MODELS

8.2.1 MobileFaceNet

MobileFaceNet is a lightweight deep learning model designed specifically for face recognition tasks on mobile devices with limited computational resources. It aims to achieve high accuracy in face recognition while maintaining low latency and memory footprint, making it suitable for real-time applications on mobile platforms.

1) **Architecture**
   - MobileFaceNet is based on the MobileNetV2 architecture, which is a convolutional neural network (CNN) designed for mobile and embedded vision applications.
   - It utilizes depth wise separable convolutions and efficient building blocks to reduce the computational cost and model size while preserving high accuracy.
   - MobileFaceNet consists of multiple convolutional layers followed by global average pooling and fully connected layers for feature extraction and classification.

2) **Feature Extraction**
   - MobileFaceNet is trained to extract discriminative features from facial images that are robust to variations in pose, illumination, and expression.
   - The network learns hierarchical representations of facial features by processing input images through multiple convolutional layers.
   - The final feature embeddings produced by MobileFaceNet are compact yet descriptive representations of facial identity, suitable for face recognition tasks.

3) Model Size and Efficiency

- One of the key advantages of MobileFaceNet is its compact model size and computational efficiency, which are crucial for deployment on resource-constrained mobile devices.
- The model is designed to minimize memory footprint and inference latency, allowing for real-time face recognition performance on smartphones and tablets.
- Despite its small size, MobileFaceNet achieves competitive accuracy compared to larger and more computationally intensive face recognition models.

4) Training and Optimization

- MobileFaceNet is trained using large-scale face recognition datasets such as VGGFace2 or MS-Celeb-1M to learn discriminative facial representations.
- During training, techniques such as data augmentation, regularization, and learning rate scheduling may be employed to improve generalization and convergence.
- The model is optimized for deployment on mobile platforms using techniques such as quantization, pruning, and model compression to further reduce the computational cost and memory requirements.

8.2.2 MiniFASNet

MiniFASNet, short for Mini Face Anti-Spoofing Network, is a compact deep learning model designed for detecting facial spoof attacks in face recognition systems. It focuses on efficiently detecting fake faces created by printed photos, digital screens, or masks to enhance the security of face recognition systems.

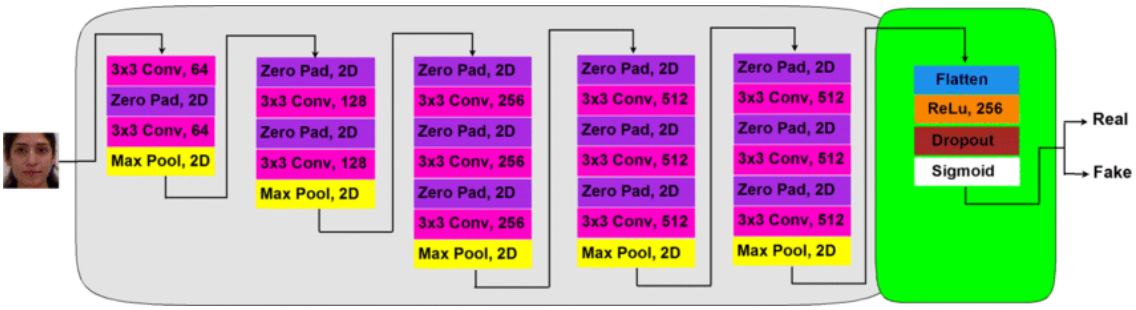


fig. 8.2.2 MiniFASNet Architecture

1) **Architecture**
   - MiniFASNet typically employs a lightweight convolutional neural network (CNN) architecture, optimized for real-time processing and low computational resource consumption.
   - The architecture is designed to extract discriminative features from facial images and classify them as genuine or spoofed.

2) **Feature Extraction**
   - MiniFASNet utilizes convolutional layers to extract features from input facial images that are indicative of spoof attacks.
   - These features may include texture patterns, color variations, and geometric distortions that differentiate real faces from spoofed ones.

3) **Spoof Detection**
   - MiniFASNet is trained to classify facial images into genuine and spoofed categories based on the extracted features.
   - It learns to distinguish between genuine facial features and artifacts characteristic of spoof attacks, such as lack of depth or unnatural textures.

4) Efficiency and Speed

- One of the primary advantages of MiniFASNet is its efficiency and speed, allowing for real-time detection of spoof attacks on low-powered devices.
- The model is optimized to minimize inference latency and memory footprint, making it suitable for deployment on mobile devices and edge computing platforms.

5) Training and Optimization

- MiniFASNet is trained using large-scale datasets of genuine and spoofed facial images to learn discriminative features for spoof detection.
- During training, techniques such as data augmentation, regularization, and model distillation may be employed to improve generalization and robustness.
- The model is optimized for deployment on resource-constrained devices using techniques such as quantization, pruning, and model compression.

8.3 RESULTS

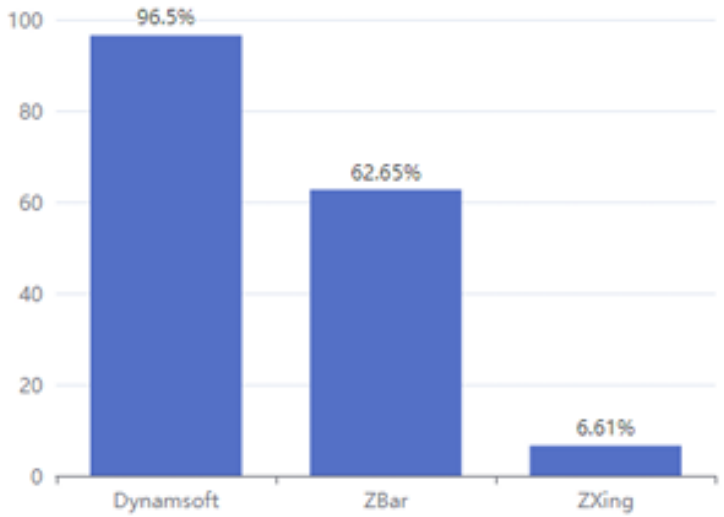


Fig. 8.3.1 Reading results of barcode scanning

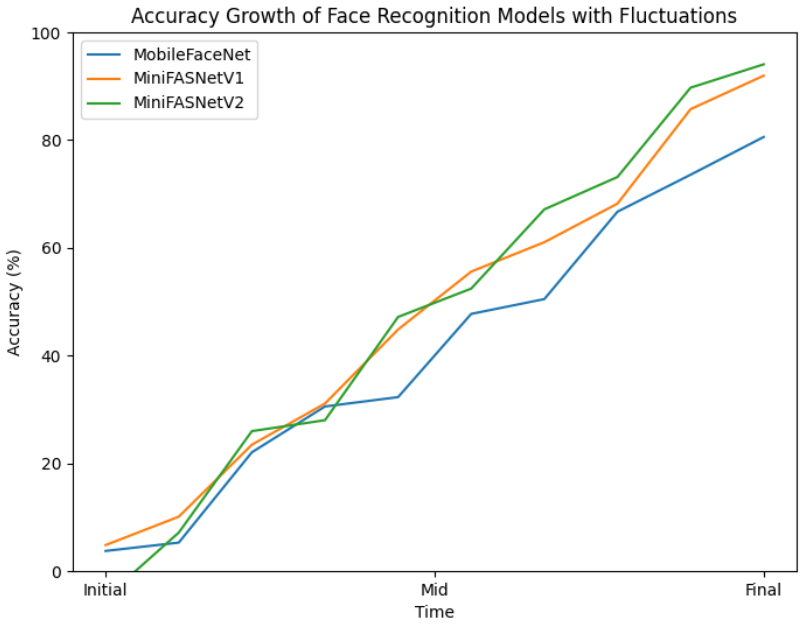


fig. 8.3.2 Accuracy of models used in Face Recognition

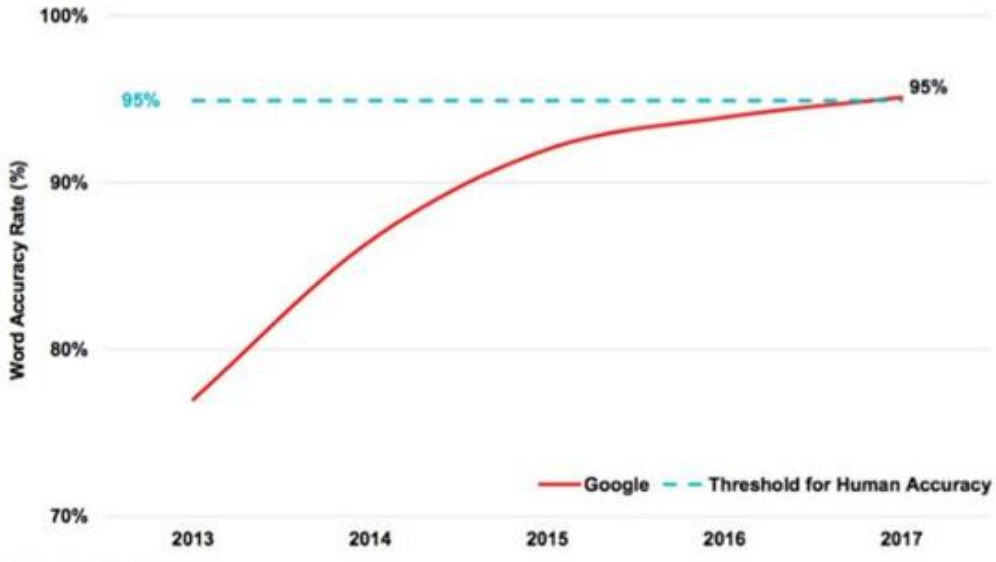


fig. 8.3.3 Voice verification Accuracy

9. SAMPLE CODE

9.1 barcode_scan.py

```
import numpy as np
import cv2
import winsound
from pyzbar.pyzbar import decode

def decode_image(im):
    decoded_objects = decode(im)

    return decoded_objects

def detect_glare(image):
    if image is None or image.size == 0:
        return 0.0  # Return 0 glare percentage for empty or invalid images

    # Convert the image to grayscale
    gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)

    # Calculate mean pixel intensity as a measure of glare
    mean_intensity = np.mean(gray)

    # Normalize mean intensity to the range [0, 1]
    glare_percentage = (mean_intensity / 255.0)

    return glare_percentage

def display(im, decoded_objects):
    scanned_data = set()  # To store scanned data and ensure it's printed only once

    for decoded_object in decoded_objects:
        x, y, w, h = decoded_object.rect

        # Ensure that the bounding box falls within the image bounds
        if x < 0 or y < 0 or x + w > im.shape[1] or y + h > im.shape[0]:
            continue  # Skip processing if the bounding box is out of bounds

        # Extract the region of interest (ROI) from the image
        roi = im[y:y+h, x:x+w]
        glare_percentage = detect_glare(roi)

        if glare_percentage > 0.5:  # Adjust the threshold as needed
```

```
            # Display warning in red for barcodes scanned from electronic devices
            cv2.rectangle(im, (x, y), (x + w, y + h), (0, 0, 255), 3)
            cv2.putText(im, "Not accepted from Electronic Devices", (x, y - 10),
cv2.FONT_HERSHEY_SIMPLEX, 0.5, (0, 0, 255), 2)
        else:
            # Display bounding box for accepted barcodes
            cv2.rectangle(im, (x, y), (x + w, y + h), (0, 255, 0), 3)
            cv2.putText(im, str(decoded_object.data), (x, y - 10),
cv2.FONT_HERSHEY_SIMPLEX, 0.5, (255, 255, 255), 2)
            winsound.Beep(1000, 200)  # Play beep sound once barcode is scanned

            # Add scanned data to the set
            scanned_data.add(decoded_object.data.decode('utf-8'))

    cv2.imshow("Barcode Scan", im)
    cv2.waitKey(1)  # Adjust the waitKey delay to control the frame rate

    return scanned_data

if __name__ == '__main__':
    # Open the default camera (index 0)
    cap = cv2.VideoCapture(0)

    scanned_data = set()  # To store scanned data and ensure it's printed only once

    while True:
        # Capture frame-by-frame
        ret, frame = cap.read()
        if not ret:
            print("Error: Unable to capture video.")
            break
        # Decode the frame to detect barcodes
        decoded_objects = decode_image(frame)

        # Display the frame with bounding boxes around detected barcodes
        scanned_data.update(display(frame, decoded_objects))

        # Break the loop if 'q' is pressed
        if cv2.waitKey(1) & 0xFF == ord('q'):
            break

    # Release the capture when finished
    cap.release()
    cv2.destroyAllWindows()
```

9.2 anti_spoof_predict.py

```
import os
import cv2
import math
import torch
import numpy as np
import torch.nn.functional as F


from src.model_lib.MiniFASNet import MiniFASNetV1,
MiniFASNetV2,MiniFASNetV1SE,MiniFASNetV2SE
from src.data_io import transform as trans
from src.utility import get_kernel, parse_model_name

MODEL_MAPPING = {
   'MiniFASNetV1': MiniFASNetV1,
   'MiniFASNetV2': MiniFASNetV2,
   'MiniFASNetV1SE':MiniFASNetV1SE,
   'MiniFASNetV2SE':MiniFASNetV2SE
}


class Detection:
   def __init__(self):
      caffemodel = "D:/Face_Detection_Real_Fake/Silent-Face-Anti-Spoofing-
master/resources/detection_model/Widerface-RetinaFace.caffemodel"
      deploy = "D:/Face_Detection_Real_Fake/Silent-Face-Anti-Spoofing-
master/resources/detection_model/deploy.prototxt"
      self.detector = cv2.dnn.readNetFromCaffe(deploy, caffemodel)
      self.detector_confidence = 0.6
   def get_bbox(self, img):
      height, width = img.shape[0], img.shape[1]
      aspect_ratio = width / height
      if img.shape[1] * img.shape[0] >= 192 * 192:
         img = cv2.resize(img,
                          (int(192 * math.sqrt(aspect_ratio)),
                           int(192 / math.sqrt(aspect_ratio))),
interpolation=cv2.INTER_LINEAR)
      blob = cv2.dnn.blobFromImage(img, 1, mean=(104, 117, 123))
      self.detector.setInput(blob, 'data')
      out = self.detector.forward('detection_out').squeeze()
      max_conf_index = np.argmax(out[:, 2])
```

```
        left, top, right, bottom = out[max_conf_index, 3]*width, out[max_conf_index,
4]*height, \
                                   out[max_conf_index, 5]*width, out[max_conf_index, 6]*height
        bbox = [int(left), int(top), int(right-left+1), int(bottom-top+1)]
        return bbox


class AntiSpoofPredict(Detection):
    def __init__(self, device_id):
        super(AntiSpoofPredict, self).__init__()
        self.device = torch.device("cuda:{}".format(device_id)
                                   if torch.cuda.is_available() else "cpu")
    def _load_model(self, model_path):
        # define model
        model_name = os.path.basename(model_path)
        h_input, w_input, model_type, _ = parse_model_name(model_name)
        self.kernel_size = get_kernel(h_input, w_input,)
        self.model =
MODEL_MAPPING[model_type](conv6_kernel=self.kernel_size).to(self.device)
        # load model weight
        state_dict = torch.load(model_path, map_location=self.device)
        keys = iter(state_dict)
        first_layer_name = keys.__next__()
        if first_layer_name.find('module.') >= 0:
            from collections import OrderedDict
            new_state_dict = OrderedDict()
            for key, value in state_dict.items():
                name_key = key[7:]
                new_state_dict[name_key] = value
            self.model.load_state_dict(new_state_dict)
        else:
            self.model.load_state_dict(state_dict)
        return None
    def predict(self, img, model_path):
        test_transform = trans.Compose([
            trans.ToTensor(),])
        img = test_transform(img)
        img = img.unsqueeze(0).to(self.device)
        self._load_model(model_path)
        self.model.eval()
        with torch.no_grad():
            result = self.model.forward(img)
            result = F.softmax(result).cpu().numpy()
        return result
```

9.3 Voice_verification.py

```
import wave, os, speech_recognition as sr, librosa, numpy as np, soundfile as sf
from sklearn.metrics.pairwise import cosine_similarity

def record_audio():
    recognizer = sr.Recognizer()
    with sr.Microphone() as source:
        audio = recognizer.listen(source)
    return audio

def speech_to_text(audio):
    recognizer = sr.Recognizer()
    try:
        text = recognizer.recognize_google(audio)
        return text
    except sr.UnknownValueError:
        return None

def save_voice_sample(audio, filename):
    with wave.open(filename, "wb") as wf:
        wf.setnchannels(audio.channel_count)
        wf.setsampwidth(audio.sample_width)
        wf.setframerate(audio.sample_rate)
        wf.writeframes(audio.get_wav_data())

def train_voice_model(name):
    enrollment_audio = record_audio()
    sr = 16000
    enrollment_audio_np = np.frombuffer(enrollment_audio.frame_data,
dtype=np.int16)
    save_voice_sample(enrollment_audio_np, f"{name}_voice.wav", sr)

def load_voice_model(name):
    filename = f"{name}_voice.wav"
    if os.path.exists(filename):
        voice, sr = librosa.load(filename)
        return voice, sr
    else:
        return None, None

def compare_voices(recorded_voice, reference_voice):
    similarity = cosine_similarity([recorded_voice], [reference_voice])
    return similarity[0][0]
```

```
def main():
    name = input("Enter your name or ID: ")
    filename = f"{name}_voice.wav"
    reference_voice, sr = load_voice_model(name)

    if reference_voice is None:
        train_voice_model(name)
        reference_voice, sr = load_voice_model(name)

    recorded_audio = record_audio()
    save_voice_sample(recorded_audio.get_raw_data(), "recorded_audio.wav",
recorded_audio.sample_rate)
    recorded_voice, sr_recorded = librosa.load("recorded_audio.wav", sr=None)
    text = speech_to_text(recorded_audio)

    if text is not None:
        recorded_mfcc = librosa.feature.mfcc(y=recorded_voice, sr=sr_recorded)
        reference_mfcc = librosa.feature.mfcc(y=reference_voice, sr=sr)
        similarity = cosine_similarity(np.transpose(recorded_mfcc),
np.transpose(reference_mfcc))

        if np.max(similarity) > 0.5:
            print("Welcome back.")
        else:
            print("Voice did not match.")
    else:
        print("Failed to convert speech to text.")

    os.remove("recorded_audio.wav")

if __name__ == "__main__":
    main()
```

10. OUTPUT SCREENS

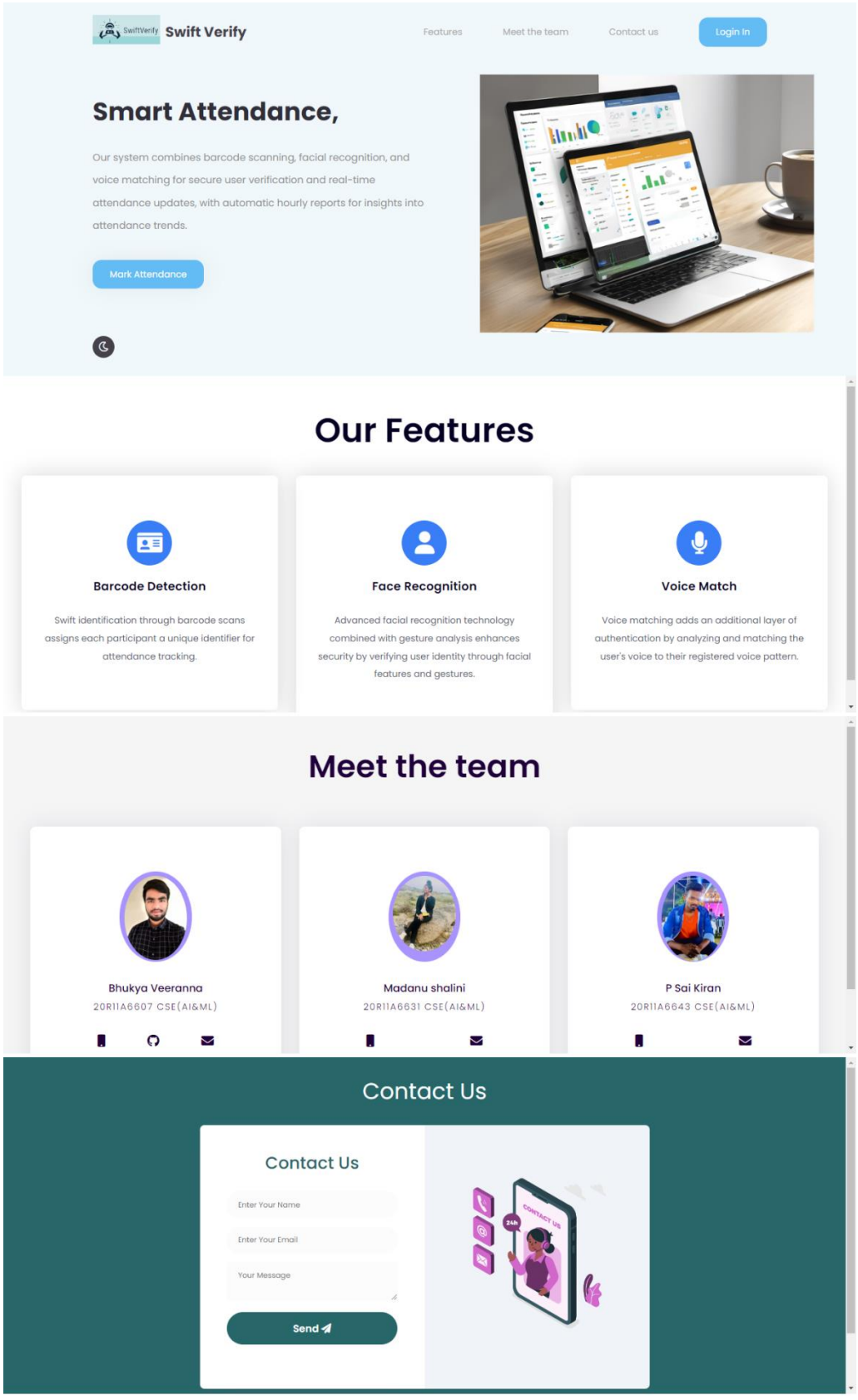


fig. 10.1 Website Home page

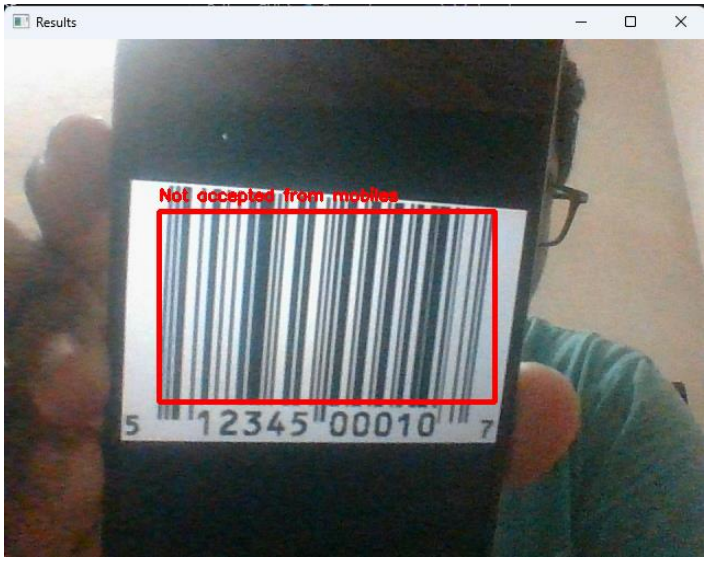


fig. 10.2 Barcode Scan Rejected from mobile screen

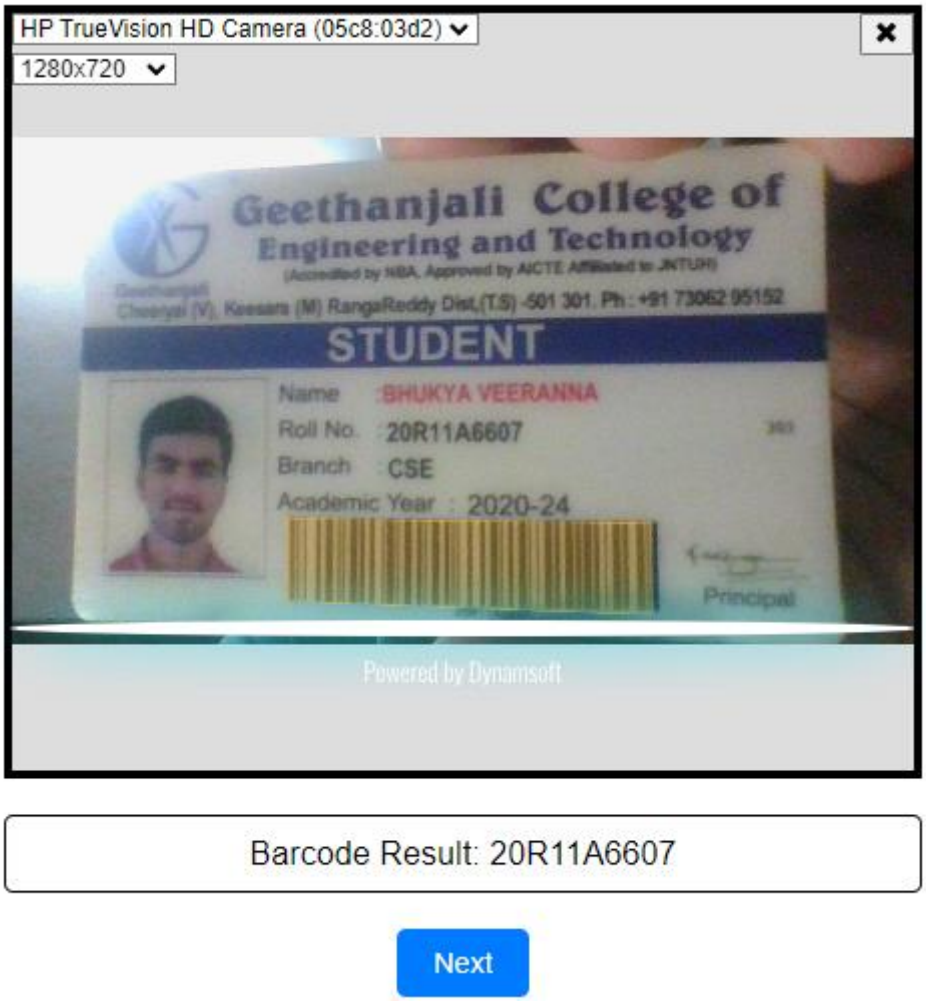


fig. 10.3 Barcode accepted

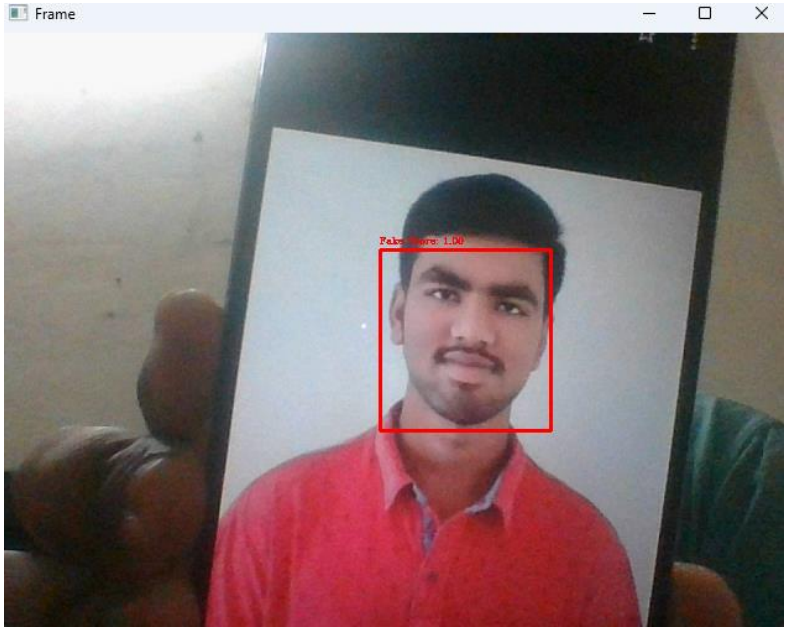


fig. 10.4 Fake face detection

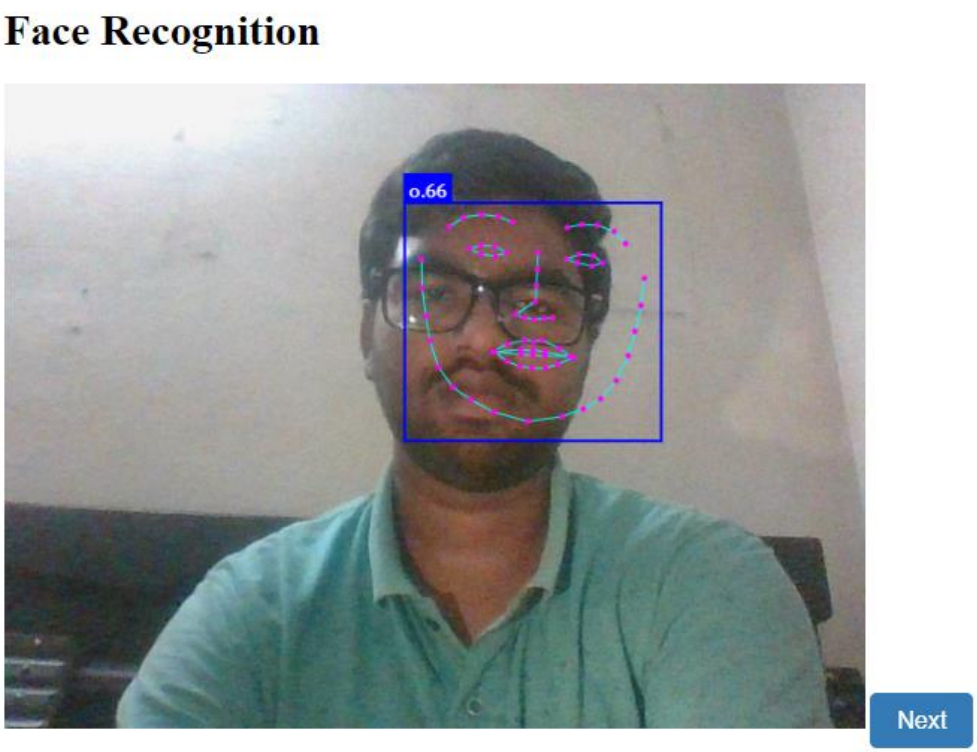


fig. 10.5 Real Face Detection

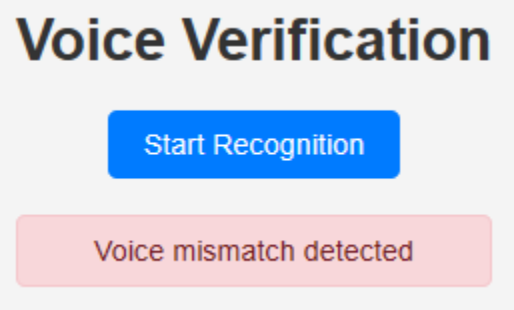


fig. 10.6 Voice Mismatch

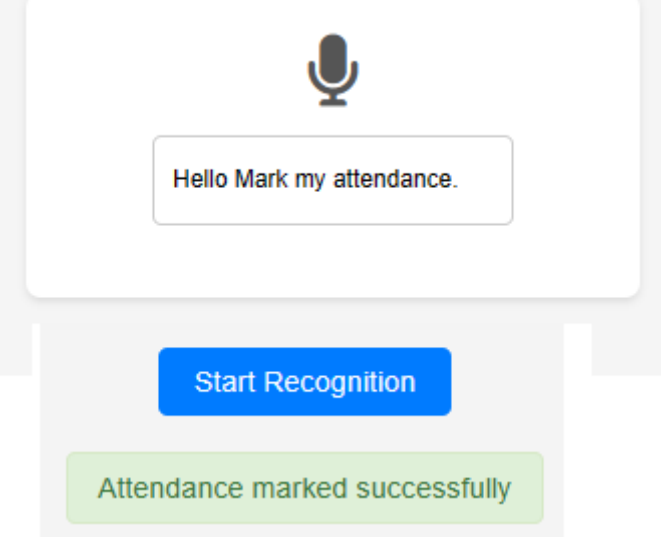


fig. 10.7 Voice matched and attendance marked successfully

Name	RollNumber	Time
Veeranna	20R11A6607	17:26:33
Sai Kiran	20R11A6643	17:26:46

fig. 10.8 Sample Attendance result

11. CONCLUSION & FUTURE SCOPE

The proposed Multi-Factor Attendance System represents a significant advancement in attendance management for educational institutions. By integrating voice matching, facial recognition, and barcode scanning technologies, the system addresses vulnerabilities present in traditional approaches, such as inaccuracies in data entry and susceptibility to unauthorized access. The multi-layered authentication procedure enhances security while reducing human data entry errors, resulting in more reliable attendance records. Additionally, real-time updates provided by the centralized database offer valuable insights into attendance trends and patterns, empowering administrators to make informed decisions. Overall, this innovative approach has the potential to greatly improve attendance management and contribute to the technological advancement of educational institutions.

Looking forward, the Multi-Factor Attendance System presents several avenues for future improvement in educational settings. This includes exploring additional authentication methods like fingerprint or iris scanning for enhanced security. Continuous optimization efforts are crucial to refining algorithms for better speed and adaptability. Integration with existing student information systems and predictive analytics can streamline administrative tasks and forecast attendance trends. Developing user-friendly mobile applications and collaborating with industry partners can further enhance the system's effectiveness and user experience. By pursuing these avenues, educational institutions can continue to advance their attendance management processes and foster a more technologically driven learning environment.

REFERENCES

1. Prerak Moolchandani, Shreya Hegde, Muskan Hassanandani, Garv Jhangiani, Gresha Bhatia, Abha Tewari, Shashikant Dugad, "Pehchaan: A Touchless Attendance System", 2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1), pp.1-5, 2023.
2. Ss, Poornima & Sripriya, N & Vijayalakshmi, B & Vishnupriya, P. (2017). Attendance monitoring system using facial recognition with audio output and gender classification. 1-5. 10.1109/ICCCSP.2017.7944103.
3. Smitha, & Hegde, Pavithra & Afshin,. (2020). Face Recognition based Attendance Management System. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS050861.
4. Soewito, Benfano & Lumban Gaol, Ford & Simanjuntak, Echo & Gunawan, Fergyanto. (2016). Smart mobile attendance system using voice recognition and fingerprint on smartphone. 175-180. 10.1109/ISITIA.2016.7828654.
5. Ajinkya Patil, Mrudang Shukla(2014) "Implementation of classroom attendance system based on face recognition in class", International Journal of Advances in Engineering & Technology, Vol. 7 Issue 3, pp976-978.
6. https://www.dynamsoft.com/codepool/barcode-scanning-accuracy-benchmark-and-comparison.html
7. https://paperswithcode.com/task/face-anti-spoofing
8. https://www.pingidentity.com/en/resources/blog/post/introducing-voice-verification.html
9. https://www.idrnd.ai/voice-biometrics
10. https://speechprocessingbook.aalto.fi/Recognition/Speaker_Recognition_and_Verification.html
11. https://domino.ai/blog/building-a-speaker-recognition-model

RESEARCH PAPER

SwiftVerify: A Multi-Modal Smart Attendance System

[1] **Bhukya Veeranna**
CSE(AI&ML)
GCET
Hyderabad, India
20r11a6607@gcet.edu.in

[2] **Madanu Shalini**
CSE(AI&ML)
GCET
Hyderabad, India
20r11a6631@gcet.edu.in

[3] **Peladolu Sai Kiran**
CSE(AI&ML)
GCET
Hyderabad, India
20r11a6643@gcet.edu.in

[4] **V. Madhusudhan Rao**
Professor & Dean school of CS&I
GCET
Hyderabad, India
madhuveldanda.cse@gcet.edu.in

***Abstract* - In response to the growing demand for enhanced attendance systems in educational institutions, this paper proposes a ground breaking Multi-Factor Attendance System. Vulnerabilities in traditional approaches include inaccuracies in human data entry and vulnerability to unauthorised access. Our technology offers a multi-layered authentication procedure by combining voice matching, facial recognition, and barcode scanning technologies to overcome these issues. By doing this, security is improved and human data entry errors are reduced. In addition, our system's centralised database allows for real-time attendance updates, providing relevant information on attendance trends and patterns. We hope to enhance attendance management and make a major technological contribution to the development of educational institutions with this creative approach.**

Keywords- Multi-Factor Attendance System, Educational Institutions, Vulnerabilities, Security, Real-time Attendance Updates, Centralized Database, Attendance Trends, Attendance Management

I. INTRODUCTION

Traditionally, maintaining student involvement and operational efficiency in the context of educational institutions has depended heavily on the regulation of attendance. Historically, manual techniques like paper-based registers or crude electronic systems have been used for attendance tracking. These methods, however, are time-consuming, prone to error, and devoid of the strong security features required to protect confidential attendance information. The demand for more advanced attendance systems has arisen due to the rapid growth of technology. These systems must be able to reliably record attendance, ensure strict authentication, and provide meaningful data for decision-making processes.

To overcome these issues, this study presents a ground breaking Multi-Factor Attendance System. Our solution combines voice matching, facial recognition, and barcode scanning technologies, drawing on the development of attendance management systems and biometric technology improvements. Our system's cornerstone, multi-factor authentication, requires numerous kinds of authentication to ensure thorough user verification. This strategy reduces the drawbacks connected to single-factor authentication techniques while also improving security. By using a range of biometric modalities, our system provides a strong and dependable authentication method, reducing the possibility of identity theft and unwanted access.

By offering a complete and safe solution that expedites procedures and improves data accuracy, our research aims to completely transform attendance management in educational institutions. In addition to providing increased security, our system makes use of cutting-edge technology like voice-recognition and facial identification to deliver insightful data about attendance patterns and trends. With the ability to make decisions and allocate resources more efficiently based on real-time attendance data, educational institutions will be better equipped as a result. Ultimately, our Multi-Factor Attendance System contributes to increased effectiveness, security, and transparency in learning environments by marking a substantial technological development in attendance management systems.

II. RELATED WORK

[1] Despite technological developments, the outdated practice of human attendance logging has continued, leading to errors and inefficiencies. Using speech recognition technology presents a viable way to solve this problem and provide accurate, automatic attendance tracking. Utilising Google's speech recognition module is proposed system, which is incorporated into an easy-to-use Kivy application that runs in a Python environment. This technology guarantees precision and dependability in attendance recording while also doing away with the need for personal intervention. Furthermore, stakeholders in corporate offices and educational institutions can easily access thorough attendance status thanks to the integration of a sophisticated user interface.

Through the implementation of this novel strategy, this successfully address the persistent issue of imprecise attendance recording, opening the door to more efficient and streamlined operations. Approach, which is based on speech - recognition technology, reduces errors and improves accessibility for both staff members and students. Moreover, the accuracy rate of 95% indicated in “Mary Meeker's annual Internet Trends Report highlights” how well answer meets the exacting requirements of attendance tracking.

[2] The manual method of keeping track of student attendance in classes is prone to manipulation and is therefore often unsuccessful. In an attempt to automate the process of tracking attendance, the Automated Attendance System (AUDACE) was created in response to this problem. AUDACE uses face recognition technology to identify pupils in the classroom automatically and in real time. The technology precisely tracks attendance by taking pictures in real time and comparing them to reference faces stored in the dataset.

This eliminates the need for human entry and lowers the possibility of mistakes or record manipulation. A speech conversion system that audibly announces the list of absentees is another feature of AUDACE that offers a dependable confirmation method for attendance tracking.

The inherent problems of manual attendance logging in educational settings are successfully alleviated by using AUDACE. The precise and automatic attendance tracking features of the system address students' propensity for proxy attendance or absenteeism. With the use of speech converter technology and facial recognition, AUDACE guarantees the accuracy and dependability of attendance records while simultaneously improving tracking efficiency. The system's capacity to classify the gender of the pupils present in the class enables more detailed attendance management methods within educational institutions. This capability adds another layer of information to attendance demographics, allowing for a deeper understanding of the composition of the class and potentially influencing various educational strategies and interventions.

[3] Face recognition technology is a valuable biometric solution for security, authentication, and identity in today's digital world. It is applicable to many different industries. Face recognition is more generally applicable due to its non-invasive and contactless nature, even though its accuracy is lower than that of other biometric techniques like iris or fingerprint recognition. The inefficiencies and vulnerability to proxy attendance inherent in manual attendance systems have led to an increased adoption of facial recognition systems for attendance marking in offices, educational institutions, and other settings.

An innovative face-recognition-based class attendance system is suggested as a solution to these problems. Using four main automated processes—database construction, face detection, face recognition, and updating—this system simplifies the process of tracking attendance. Utilising cutting-edge methods like the Local Binary Pattern Histogram algorithm and the Haar-Cascade classifier, the system reliably and efficiently manages attendance by correctly identifying people from live streaming video in the classroom. The adoption of this automated system ultimately provides an easy and transparent method of tracking attendance, which helps to increase responsibility and productivity in organisational and educational contexts.

[4] Many years have passed since the manual attendance systems gave way to biometric-based ones. But current methods frequently have flaws, especially when it comes to overseeing those who work off-site. In this study, a novel attendance system designed specifically to efficiently record off-site employees' attendance. This technology allows the accounting department to easily compute and report salaries, including overtime expenditures, because it integrates seamlessly with the payroll system. Solution provides fingerprint and voice recognition identification using smartphones for verification. Investigation revealed that voice recognition has a false negative rate of 5.88% and fingerprint verification produces a false positive rate of 95%. These results highlight the dependability and usefulness of our suggested attendance method for managing remote workers.

[5] Particularly since the development of image processing methods, facial features have become an important identifier for identification. Conventional attendance practices, such summoning students verbally, take up valuable class time. We suggest an automatic attendance system based on facial detection and identification to overcome this. The system uses a camera-equipped Raspberry Pi module to record the entire classroom, and student databases with names, photos, and roll numbers allow for precise attendance monitoring. This method allows attendance to be taken at any time during class, saving time and providing convenience. Face detection guarantees accurate identification, and recognition effectively logs student attendance. Our technology ensures the best possible use of instructional time by automating this procedure, which simplifies attendance management in educational environments.

Here are some drawbacks in present system:

1. Traditional attendance systems are prone to inaccuracies due to human data entry errors and susceptibility to manipulation, such as proxy attendance.

2. Manual attendance methods are inefficient and time-consuming, leading to wasted instructional time, with attendance recording taking up to 10 minutes per lecture.

3. Existing systems lack robust security measures, making them vulnerable to unauthorized access and compromising the integrity of attendance records.

4. Current systems rely heavily on human intervention for data entry and verification, increasing the likelihood of errors and inefficiencies.

5. Many systems lack real-time updates, making it challenging for administrators to track attendance trends and patterns effectively, hindering decision-making and proactive intervention.

6. Traditional systems often rely on single-factor authentication, such as manual sign-ins or ID card scanning, which may not adequately verify the identity of individuals.

7. Existing systems may operate in silos, making it difficult to integrate attendance data with other administrative or educational platforms, hindering data analysis and decision-making.

8. Some attendance systems struggle to scale effectively, particularly in large organizations or classrooms, leading to inefficiencies and delays in attendance tracking.

9. Maintaining traditional attendance systems, such as manual logbooks or card readers, can be labour-intensive and costly, requiring frequent upkeep and repairs.

III. PROPOSED WORK

In response to the growing demand for enhanced attendance systems in educational institutions, this paper proposes a ground breaking Multi-Factor Attendance System. Vulnerabilities in traditional approaches include inaccuracies in human data entry and vulnerability to unauthorised access. Our technology offers a multi-layered authentication procedure by combining barcode scanning, facial recognition, and voice matching technologies to overcome these issues. By doing this, security is improved and human data entry errors are reduced. Furthermore, the centralised database of our system enables real-time attendance updates, providing insightful information on attendance trends and patterns.

A. Barcode Scanning

Barcode scanning is a vital first step in many automated systems, providing quick decoding of barcoded data for activities like identification and inventory control.

Two crucial steps are involved in this process:

1. **Detection:** where the system locates possible barcode candidates in a picture
2. **Decoding:** where the encoded data is taken out of these areas

Measuring precision and reading rate—which indicate the system's capacity to provide accurate results among all returned results and barcodes present, respectively—are two ways to evaluate the accuracy of barcode scanning.

[6] Multiple barcode scanning engines—both open-source and commercial—are thoroughly analysed and contrasted according to reading rate and precision criteria. Zbar and ZXing are two well-known open-source solutions that are compared to other commercial SDKs while evaluating Dynamsoft's barcode SDK. Performance tests are carried out on datasets that include barcode images captured in various settings. Test results include metrics for each engine, including precision, reading rates, misreads, and correctly recognised barcodes.

Figure 1 is the flow diagram of the barcode scanning system with internal processing and evaluation.

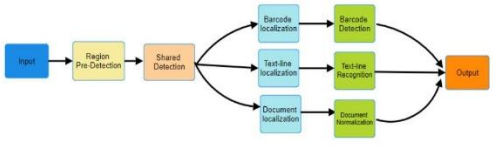


Fig.1 Flow Diagram of Barcode Scanning System

B. Face Recognition

Liveness detection technology plays a crucial role in discerning between real and fake faces presented to a system. This involves determining if the face in front of the device is genuine or an imitation, such as a printed photo or a mask. Mainstream liveness solutions encompass coordinated and non-cooperative methods. Coordinated detection prompts users to perform specific actions for verification, while silent detection conducts verification without user involvement.

Fig 2 is the overall architecture of silent face anti spoofing where the model detects whether the provided input is real or fake based on the Fourier transform and Normalization.

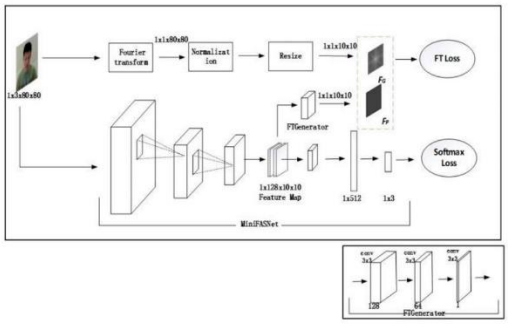


Fig.2 Silent Face Anti Spoofing Architecture

Using supervision aided by Fourier spectrogram, the suggested face recognition model uses a quiet liveness detection technique. Using Fourier spectrograms, this method identifies frequency domain differences between real and fake faces. The model architecture consists of a supervised branch aided by a Fourier spectrogram and a primary branch for classification. To maximise efficiency, the model also includes a self-developed pruning technique. For example, MobileFaceNet's Flops were lowered from 0.224G to 0.081G using this method, improving performance with little loss of accuracy.

The evaluation method involves displaying information such as speed (in milliseconds), confidence level (ranging from 0 to 1), and the outcome of liveness detection (real or fake face). This comprehensive approach ensures efficient and accurate assessment of the face recognition model's performance.

[7] The comparison of facial recognition models demonstrates the efficiency gains made possible by an in-house pruning technique. The computational complexity of MobileFaceNet decreased from 0.224G to 0.081G, while the computational needs of MiniFASNetV1 and MiniFASNetV2 also significantly decreased. These improvements preserve accuracy levels and improve the liveness detection efficiency of the models.

C. Voice Verification

Voice verification, also referred to as voice authentication, relies on distinctive vocal characteristics to identify individuals, offering a seamless and passive authentication approach. Through the analysis of voice features like pitch and tone, it ensures robust security while eliminating user friction. [8] The authentication process involves enrolling voice samples, either through self-service methods or passive collection during interactions with Interactive Voice Response (IVR) systems or call centre agents. Verification is executed through text-dependent or text-independent methods, or via web/mobile applications, where the system assesses confidence scores to validate identity.

Voice verification finds widespread applications in call centres and phone banking, revolutionizing user authentication over the phone and enhancing operational efficiency compared to traditional methods.

Fig.3 outlines the sequential steps involved in voice verification, including sample capture, template creation, and comparison for authentication.

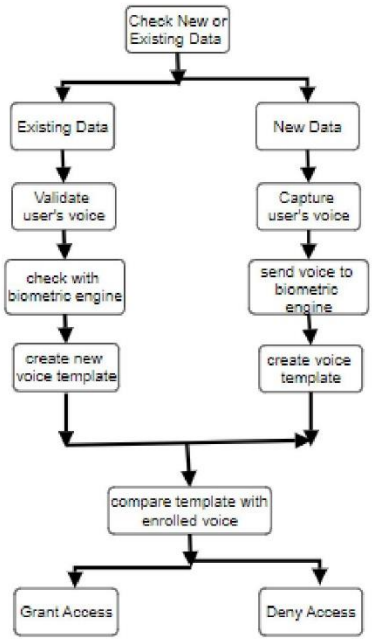


Fig.3 Flow Diagram of Voice Verification

[9]-[11] Voice verification technology employs advanced algorithms, including biometric voice recognition and liveness detection, to analyse vocal characteristics for authentication. These algorithms leverage machine learning and signal processing techniques to create unique voiceprints and ensure data security. Integration with IVR systems and mobile/web applications enhances user experience and operational efficiency. Through these technologies, voice verification provides reliable authentication while meeting stringent security requirements.

D. Central Database

The centralised database that houses all of the attendance-related data is the fundamental component of the Multi-Factor Attendance System. Time stamps for attendance entries, user identifying data, and extra metadata related to every attendance record are all stored in this database. The solution guarantees accuracy and consistency in tracking attendance across several locations and user interactions by centralising the data. Additionally, real-time attendance updates are facilitated by the central database, which also provides insightful information about attendance patterns and trends. The information contained in the central database can be utilised by educational institutions to improve overall operational efficiency and optimise attendance management tactics by employing advanced data analysis techniques.

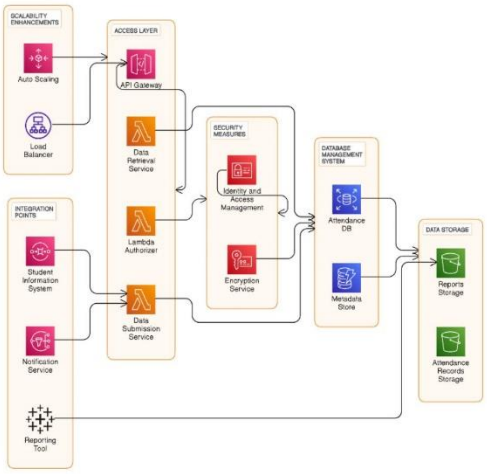


Fig.4 Central Database Architecture for Multi-Factor Attendance System

The central database in the Multi-Factor Attendance System serves as the backbone for storing, managing, and retrieving attendance-related data. It operates by utilizing a Database Management System (DBMS) to organize attendance records into structured tables within the database. These tables typically include user information, attendance logs, timestamps, and metadata.

Data access layers facilitate interactions with the central database, handling tasks such as querying, inserting, updating, and ensuring data integrity. Robust security measures, such as role-based access control and encryption, safeguard the database against unauthorized access and ensure data integrity.

Managed by database administrators, the central database undergoes regular maintenance, including backups, optimization, and monitoring for performance and security. It integrates with other system components, such as user interfaces and reporting tools, enabling seamless data exchange and real-time updates.

E. System Architecture & Process

The system architecture of our Multi-Factor Attendance System is a sophisticated framework integrating facial recognition, voice matching, and barcode scanning technologies. It revolves around a robust central database managed by DBMS, ensuring efficient storage and retrieval of attendance data. Security measures such as role-based access control and encryption protect data integrity, while scalability enhancements ensure responsiveness under varying workloads. Integration points with other system components enable seamless data exchange, supporting real-time updates and analysis. This architecture represents a forward-thinking solution to enhance attendance management in educational institutions.

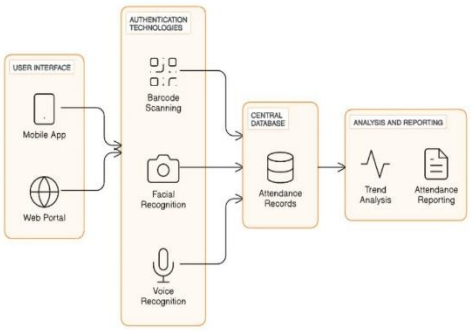


Fig.5 System Architecture

The process diagram outlines the workflow of the Multi-Factor Attendance System, illustrating steps from user interaction to data processing and storage. It delineates actions such as capturing input data, processing it through biometric engines, and making decisions based on user status. The diagram distinguishes between existing and new users, guiding them through authentication or registration processes accordingly. Emphasizing key decision points and system interactions, it provides a concise overview of the system's functionality.

Multi-factor authentication (MFA) is a pivotal security measure that bolsters access control by necessitating users to provide multiple forms of identification. MFA typically incorporates a combination of factors: knowledge (such as passwords or PINs), possession (like smartphones or tokens), inherence (biometric data like fingerprints or facial recognition). By requiring verification across multiple factors, MFA significantly heightens security, even in the event of a compromised factor.

IV. RESULTS AND DISCUSSIONS

The results and discussion section provides an in-depth analysis and interpretation of the findings obtained from the study. This section synthesizes the outcomes of research and engages in a critical examination of their implications, significance, and potential applications.

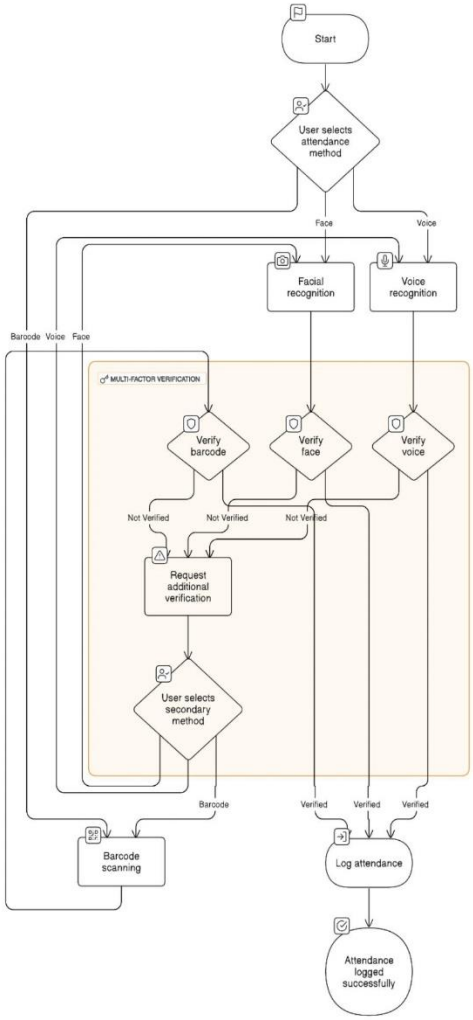


Fig.6 System Model

A. User Interface

The user interface (UI) features a homepage with project details and a contact form for inquiries. Faculty members access a dashboard to view attendance records and utilize biometric authentication methods for marking attendance.

Ease, clarity, and productivity are highlighted in a user-friendly user interface. Clear navigation menus, instantly recognisable buttons and icons, an intuitive layout and style, adaptable and adaptive device display, succinct and informative error messages, contextual assistance choices, and customisable preferences are just a few of its characteristics.

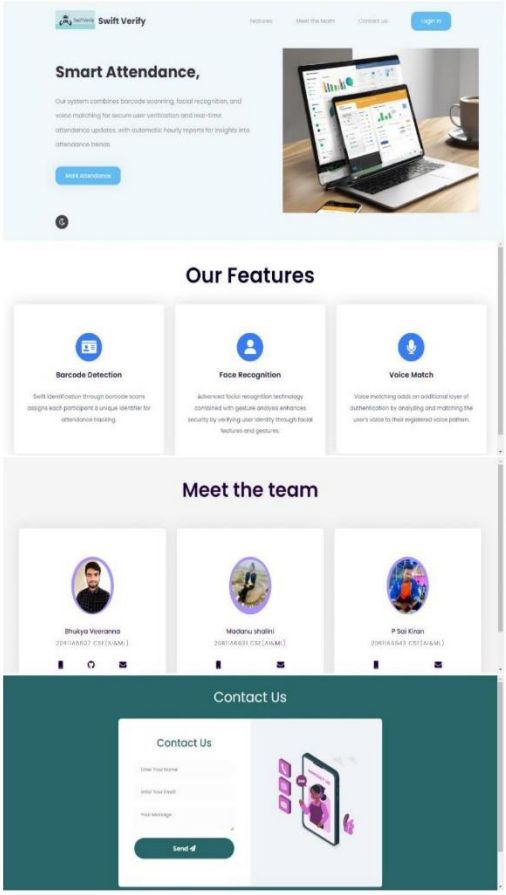


Fig.7 Home Page

B. *Barcode Results*

The evaluation's findings show that the Dynamsoft Barcode Reader outperformed competing barcode scanning engines, achieving an impressive reading rate of 96.5%. Its superior capacity to identify and recognise different barcode types makes it a very good choice for attendance systems, even though it may take a little longer to process data.

Fig.8 Reading results of barcode scanning

Evaluation Metrics

Reading rate: $\frac{\text{correctly detected barcodes}}{\text{Total barcodes}}$

Average time: $\frac{\text{Total time elapsed}}{\text{Total files}}$

Distinguishing between real and fake barcodes to enhance security. By analysing various factors such as movement, texture, and depth, liveness detection technology ensures that only authentic barcodes are recognized, thereby mitigating the risk of fraudulent activities. This feature adds an additional layer of verification, safeguarding the integrity of attendance records and enhancing the overall reliability of the system.

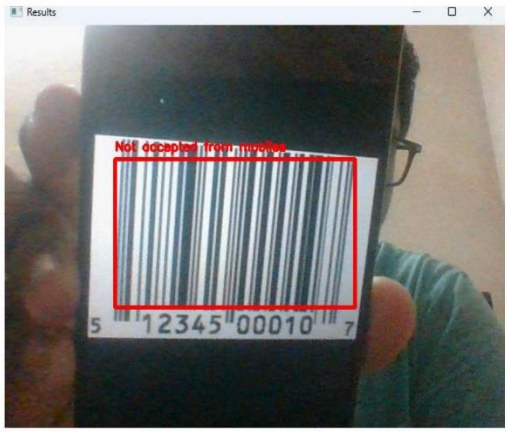


Fig.9 Barcode Scan Rejected from mobile screen

Fig. 10 Barcode accepted

C. *Face Recognition Results*

The face recognition system employs different models to detect and classify faces as real or fake. The models utilized include MobileFaceNet, MiniFASNetV1, and MiniFASNetV2. Each model is assessed based on its computational efficiency and parameter size, crucial factors for real-time face recognition tasks.

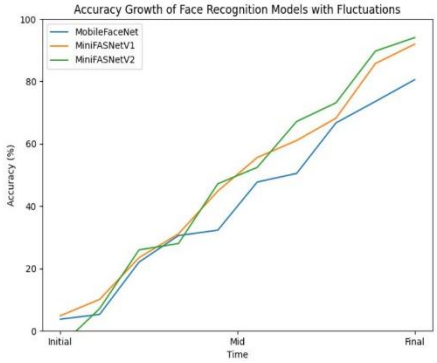


Fig.11 Accuracy of models used

These sample frames demonstrate the effectiveness of a silent face spoofing technique in distinguishing between real and fake faces. This capability enhances security in authentication systems by accurately identifying genuine facial appearances from fraudulent ones.

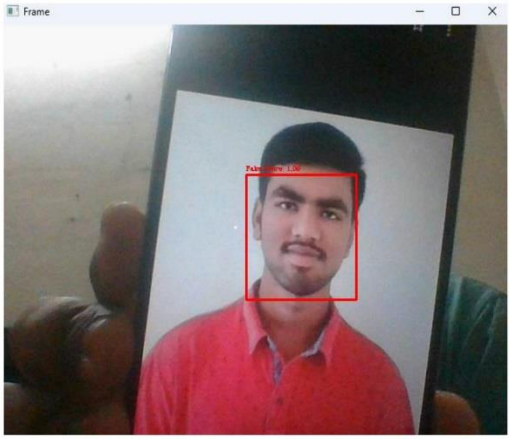


Fig.12 Fake face detection

Real face detection, combined with face grading, uses advanced technology to distinguish between genuine and fraudulent faces based on various facial features. This enhances security by ensuring that only authentic users are identified and granted access.

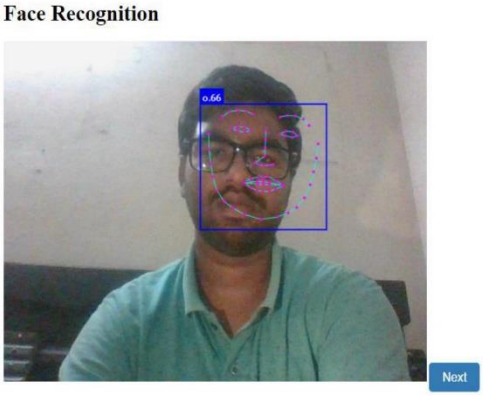


Fig.13 Real Face Detection

To enhance security and streamline attendance tracking, student data is securely stored in a centralized database. This database employs robust encryption protocols and access control measures to safeguard sensitive information. Additionally, it facilitates real-time updates and comprehensive reporting, ensuring accurate attendance records.

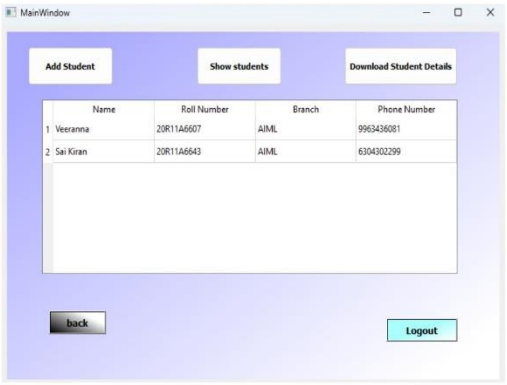


Fig.14 Display of Student data

The use of a secured database ensures data integrity and confidentiality, promoting trust and compliance with privacy regulations. Moreover, it enables efficient management of attendance data, contributing to the overall effectiveness of educational institutions.

Name	RollNumber	Time
Veeranna	20R11A6607	17:26:33
Sai Kiran	20R11A6643	17:26:46

Fig. 15 Sample Attendance result

D. Voice Verification Results

Voice verification is a biometric authentication method that utilizes unique vocal characteristics to verify an individual's identity. It involves analysing various voice features such as pitch, tone, and pronunciation to determine authenticity. This process offers a seamless and passive form of authentication, eliminating the need for traditional methods like passwords or PINs.

The following are the experimental results for Voice verification.

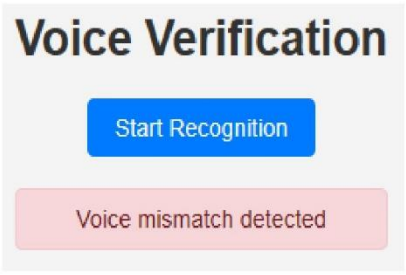


Fig.16 Voice Mismatch

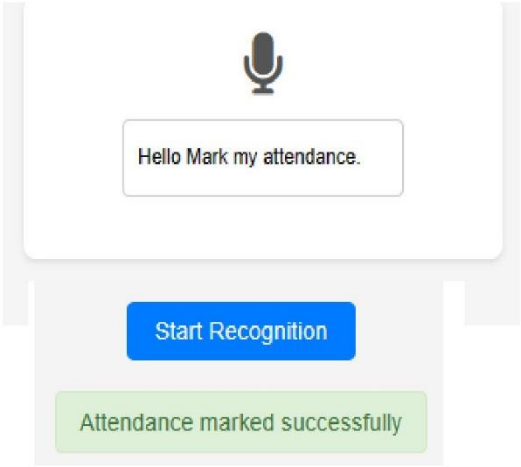


Fig.17 Voice matched and attendance marked successfully

V. CONCLUSION

The proposed Multi-Factor Attendance System represents a significant advancement in attendance management for educational institutions. By integrating voice matching, facial recognition, and barcode scanning technologies, the system addresses vulnerabilities present in traditional approaches, such as inaccuracies in data entry and susceptibility to unauthorized access. The multi-layered authentication procedure enhances security while reducing human data entry errors, resulting in more reliable attendance records. Additionally, real-time updates provided by the centralized database offer valuable insights into attendance trends and patterns, empowering administrators to make informed decisions. Overall, this innovative approach has the potential to greatly improve attendance management and contribute to the technological advancement of educational institutions.

VI. FUTURE SCOPE

The future scope of the Multi-Factor Attendance System includes leveraging biometric technologies like voice matching, facial recognition, and barcode scanning for accuracy. Integration with IoT devices allows seamless data collection and real-time updates. Machine learning algorithms can predict attendance trends for better resource allocation. Mobile apps enhance remote access, while ensuring data security and privacy remains a priority.

ACKNOWLEDGMENT

We express our gratitude to the Department of Computer Science and Engineering (AI&ML), GCET for their unwavering support throughout the execution of this project.

REFERENCES

[1] Prerak Moolchandani, Shreya Hegde, Muskan Hassanandani, Garv Jhangiani, Gresha Bhatia, Abha Tewari, Shashikant Dugad, "Pehchaan: A Touchless Attendance System", 2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1), pp.1-5, 2023.

[2] Ss, Poornima & Sripriya, N & Vijayalakshmi, B & Vishnupriya, P. (2017). Attendance monitoring system using facial recognition with audio output and gender classification. 1-5. 10.1109/ICCCSP.2017.7944103.

[3] Smitha, & Hegde, Pavithra & Afshin,. (2020). Face Recognition based Attendance Management System. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS050861.

[4] Soewito, Benfano & Lumban Gaol, Ford & Simanjuntak, Echo & Gunawan, Fergyanto. (2016). Smart mobile attendance system using voice recognition and fingerprint on smartphone. 175-180. 10.1109/ISITIA.2016.7828654.

[5] Ajinkya Patil, Mrudang Shukla(2014) "Implementation of classroom attendance system based on face recognition in class", International Journal of Advances in Engineering & Technology, Vol. 7 Issue 3, pp976-978.

[6] https://www.dynamsoft.com/codepool/barcode-scanning-accuracy-benchmark-and-comparison.html

[7] https://paperswithcode.com/task/face-anti-spoofing

[8] https://www.pingidentity.com/en/resources/blog/post/introducing-voice-verification.html

[9] https://www.idrnd.ai/voice-biometrics

[10] https://speechprocessingbook.aalto.fi/Recognition/Speaker_Recognition_and_Verification.html

[11] https://domino.ai/blog/building-a-speaker-recognition-model

PLAGIARISM REPORT

SwiftVerify: A Multi-Modal Smart Attendance System

ORIGINALITY REPORT

2%	2%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.dynamsoft.com Internet Source	<1%
2	Submitted to University of Central England in Birmingham Student Paper	<1%
3	Submitted to Excelsior University Student Paper	<1%
4	www.irdindia.in Internet Source	<1%
5	www.businessoffashion.com Internet Source	<1%
6	www.ijraset.com Internet Source	<1%
7	www.itm-conferences.org Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

DIGITAL RECEIPT

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission authors:	Bhukya Veeranna, Madanu Shalini, Peladolu Sai Kiran
Assignment title:	07
Submission title:	SwiftVerify: A Multi-Modal Smart Attendance System
File name:	A6_Technical_Paper.docx
File size:	2.4M
Page count:	8
Word count:	3,658
Character count:	24,235
Submission date:	29-Mar-2024 02:02PM (UTC+0800)
Submission ID:	2303204049

SwiftVerify: A Multi-Modal Smart Attendance System

[1]Bhukya Veeranna, CSE(AI&ML), GCET, Hyderabad, India, 20r1a6697@gcet.edu.in
[2]Madanu Shalini, CSE(AI&ML), GCET, Hyderabad, India, 20r1a6619@gcet.edu.in
[3]Peladolu Sai Kiran, CSE(AI&ML), GCET, Hyderabad, India, 20r1a6619@gcet.edu.in
[4]V. Madhusudhan Rao, Professor & Dean, school of CS&T, GCET, Hyderabad, India, madhusrekhindi.cse@gcet.edu.in

Abstract - In response to the growing demand for enhanced attendance systems in educational institutions, this paper proposes a ground breaking Multi-Factor Attendance System. Vulnerabilities in traditional approaches include inaccuracies in human data entry and vulnerability to unauthorised access. Our technology offers a multi-layered authentication procedure by combining voice matching, facial recognition, and barcode scanning technologies to overcome these issues. By doing this, security is improved and human data entry errors are reduced. In addition, our system's centralised database allows for real-time attendance updates, providing relevant information on attendance trends and patterns. We hope to enhance attendance management and make a major technological contribution to the development of educational institutions with this creative approach.

Keywords- Multi-Factor Attendance System, Educational Institutions, Vulnerabilities, Security, Real-time Attendance Updates, Centralized Database, Attendance Trends, Attendance Management

I. INTRODUCTION

Traditionally, maintaining student involvement and operational efficiency in the context of educational institutions has depended heavily on the supervision of attendance. Historically, manual techniques like paper-based registers or crude electronic systems have been used for attendance tracking. These methods, however, are time-consuming, prone to error, and devoid of the strong security features required to protect confidential attendance information. The demand for more advanced attendance systems has arisen due to the rapid growth of technology. These systems must be able to reliably record attendance, ensure strict authentication, and provide meaningful data for decision-making processes.

To overcome these issues, this study presents a ground breaking Multi-Factor Attendance System. Our solution combines voice matching, facial recognition, and barcode scanning technologies, drawing on the development of attendance management systems and biometric technology improvements. Our system's cornerstone, multi-factor authentication, requires numerous kinds of authentication to ensure thorough user verification. This strategy reduces the drawbacks connected to single-factor authentication techniques while also improving security. By using a range of biometric modalities, our system provides a strong and dependable authentication method, reducing the possibility of identity theft and unwanted access.

By offering a complete and safe solution that expedites procedures and improves data accuracy, our research aims to completely transform attendance management in educational institutions. In addition to providing increased security, our system makes use of cutting-edge technology like voice-recognition and facial identification to deliver insightful data about attendance patterns and trends. With the ability to make decisions and allocate resources more efficiently based on real-time attendance data, educational institutions will be better equipped as a result. Ultimately, our Multi-Factor Attendance System contributes to increased effectiveness, security, and transparency in learning environments by marking a substantial technological development in attendance management systems.

II. RELATED WORK

[1] Despite technological developments, the outdated practice of human attendance logging has continued, leading to errors and inefficiencies. Using speech recognition technology presents a viable way to solve this problem and provide accurate, automatic attendance tracking. Utilising Google's speech recognition module is proposed system, which is incorporated into an easy-to-use Kivy application that runs in a Python environment. This technology guarantees precision and dependability in attendance recording while also doing away with the need for personal intervention. Furthermore, stakeholders in corporate offices and educational institutions can easily access through attendance status thanks to the integration of a sophisticated user interface.

Through the implementation of this novel strategy, this successfully address the persistent issue of imprecise attendance recording, opening the door to more efficient and streamlined operations. Approach, which is based on speech-recognition technology, reduces errors and improves accessibility for both staff members and students. Moreover, the accuracy rate of 95% indicated in "Mary Meeker's annual Internet Trends Report highlights" how well answer meets the evolving requirements of attendance tracking.

[2] The manual method of keeping track of student attendance in classes is prone to manipulation and is therefore often unsuccessful. In an attempt to automate the process of tracking attendance, the Automated Attendance System (AUDACE) was created in response to this problem. AUDACE uses face recognition technology to identify pupils in the classroom automatically and in real-time. The technology precisely tracks attendance by taking pictures in real-time and comparing them to reference faces stored in the dataset.

DOCUMENTATION PLAGIARISM REPORT

SwiftVerify: A Multi-Modal Smart Attendance System

ORIGINALITY REPORT

13%	8%	3%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Hertfordshire Student Paper	5%
2	suspace.su.edu.bd Internet Source	<1%
3	Submitted to Swinburne University of Technology Student Paper	<1%
4	www.coursehero.com Internet Source	<1%
5	Submitted to University of East London Student Paper	<1%
6	www.ijirset.com Internet Source	<1%
7	Lee Boonstra. "The Definitive Guide to Conversational AI with Dialogflow and Google Cloud", Springer Science and Business Media LLC, 2021 Publication	<1%
8	Submitted to Sunway Education Group Student Paper	<1%

9	Submitted to University of Warwick Student Paper	<1 %
10	open-innovation-projects.org Internet Source	<1 %
11	Submitted to Victoria University Student Paper	<1 %
12	programtalk.com Internet Source	<1 %
13	www.ijraset.com Internet Source	<1 %
14	www.slideshare.net Internet Source	<1 %
15	Submitted to University of Greenwich Student Paper	<1 %
16	www.kluniversity.in Internet Source	<1 %
17	Submitted to CSU, San Jose State University Student Paper	<1 %
18	Submitted to Griffith College Dublin Student Paper	<1 %
19	goo.by Internet Source	<1 %
20	Submitted to Aalto Yliopisto Student Paper	<1 %

21	Submitted to Cornell University Student Paper	<1%
22	Submitted to Colorado Technical University Student Paper	<1%
23	invozone.com Internet Source	<1%
24	Submitted to University of Maryland, Global Campus Student Paper	<1%
25	python.hotexamples.com Internet Source	<1%
26	soloway.tech Internet Source	<1%
27	www.hackster.io Internet Source	<1%
28	"Computer Vision – ECCV 2018", Springer Nature America, Inc, 2018 Publication	<1%
29	Submitted to St Joseph's Nudgee College Student Paper	<1%
30	en.wikiversity.org Internet Source	<1%
31	export.arxiv.org Internet Source	<1%

DOCUMENTATION DIGITAL RECEIPT

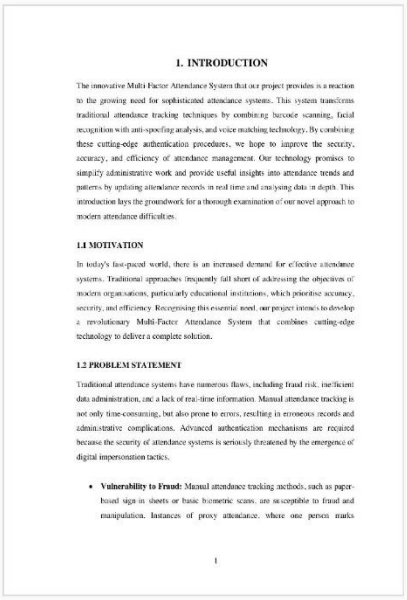
turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission authors:	Bhukya Veeranna, Madanu Shalini, Peladolu Sai Kiran
Assignment title:	08
Submission title: File name:	SwiftVerify: A Multi-Modal Smart Attendance System A6_Major_Documentation.pdf
File size:	1.47M
Page count:	58
Word count:	8,706
Character count:	54,680
Submission date:	05-Apr-2024 06:13PM (UTC+0800)
Submission ID:	2303834949



1. INTRODUCTION

The innovative Multi Factor Attendance System that our project provides is a reaction to the growing need for sophisticated attendance systems. This system transforms traditional attendance tracking techniques by combining barcode scanning, facial recognition with anti-spoofing analysis, and voice matching technology. By combining these cutting-edge authentication procedures, we hope to improve the security, accuracy, and efficiency of attendance management. Our technology promises to simplify administrative work and provide useful insights into attendance trends and patterns by updating attendance records in real time and analysing data in depth. This introduction lays the groundwork for a thorough examination of our novel approach to modern attendance difficulties.

1.1 MOTIVATION

In today's fast-paced world, there is an increased demand for effective attendance systems. Traditional approaches frequently fall short of addressing the objectives of modern organisations, particularly educational institutions, which prioritise accuracy, security, and efficiency. Recognising this essential need, our project intends to develop a revolutionary Multi-Factor Attendance System that combines cutting-edge technology to deliver a complete solution.

1.2 PROBLEM STATEMENT

Traditional attendance systems have numerous flaws, including fraud risk, inefficient data administration, and a lack of real-time information. Manual attendance tracking is not only time-consuming, but also prone to errors, resulting in erroneous records and administrative complications. Advanced authentication mechanisms are required because the security of attendance systems is seriously threatened by the emergence of digital impersonation tactics.

- **Vulnerability to Fraud:** Manual attendance tracking methods, such as paper-based sign-in sheets or basic biometric scans, are susceptible to fraud and manipulation. Instances of proxy attendance, where one person marks

1