IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Hybrid Offline–Online Face Attendance System With Real-Time Recognition And Anti-Spoofing CNN Model

Aarthi Reddy. M[1], Anusha. A[2], Sai Kumar. A[3], Ramu Yadav. V[4],

Y. B. T. Sundari[5]

[1,2,3&4] IoT Dept, Holy Mary Institute of Technology and Science, Hyderabad, TS, India.

[5]Associate Professor ECE & IoT, Holy Mary Institute of Technology and Science, Hyderabad, TS, India,

Abstract - Attendance management is a fundamental aspect of educational institutions for monitoring student performance and maintaining official records. Traditional manual methods, such as roll calls and paper registers, are increasingly viewed as inefficient due to significant time consumption and susceptibility to human error or proxy attendance. While various automated solutions like biometric scanners and QR codes have emerged, they often necessitate expensive hardware, consistent internet connectivity, and physical contact. To address these limitations, this research proposes an automated face recognition attendance system designed for both offline and online functionality. Utilizing a standard laptop camera, the system performs real-time face detection while incorporating anti-spoofing measures to prevent deception via photographs or digital screens. Data is stored locally to ensure operational continuity in areas with poor network coverage and is synchronized with the cloud once a connection is established. Furthermore, the integration of a GSM gateway allows the system to send automated SMS notifications to parents regarding student absences without relying on the internet. This approach provides a secure, cost-effective, and hygienic solution for attendance tracking in diverse environments.

Keywords: Attendance management, real-time face recognition, GSM gateway, SMS

1. Introduction

1.1 Context and Problem Statement

Managing attendance is an important task in schools, colleges, and workplaces. It helps monitor participation, evaluate performance, and ensure compliance with institutional policies. However, traditional manual attendance systems that rely on paper registers or roll calls are time-consuming, error-prone, and vulnerable to proxy attendance [1]. In large classrooms, this process consumes valuable instructional time and creates difficulties in long-term record maintenance.

To overcome these limitations, several automated attendance systems have been proposed. QR-code based systems reduce manual effort but require students to actively scan codes and may still allow misuse [2]. RFID-based attendance systems automate identification but depend on additional hardware infrastructure [3]. Biometric systems such as fingerprint recognition improve authenticity but involve physical contact and hygiene concerns [4]. Iris-based systems offer higher accuracy but are costly and require specialized sensors [5].

Although these systems reduce manual workload, they introduce challenges such as dependency on additional devices, maintenance costs, and the need for reliable internet connectivity. These limitations make them less suitable for rural or resource-constrained environments.

Face recognition has emerged as a promising alternative because it is contactless and requires minimal user effort. Early approaches such as LBP-based recognition systems demonstrated feasibility in attendance automation [6]. Deep learning methods like FaceNet significantly improved recognition accuracy by generating robust face embeddings [7]. Transfer learning techniques further enhanced performance under varying classroom conditions [8], and classifiers such as Support Vector Machines (SVM) have been effectively used to classify deep face embeddings [9].

Despite these advancements, simple face recognition systems remain vulnerable to spoofing attacks using printed photos or videos. Research on liveness detection using LBP features [10], blink and micro-expression analysis [11], and CNN-based depth estimation methods [12] has shown that anti-spoofing mechanisms are necessary to ensure system reliability.

The main problem can be explained in three simple points:

- **Poor security and trust:**
  Simple face recognition systems can be easily tricked using photos or videos. This allows fake or proxy attendance, which makes the system unreliable.
- **Need for extra devices and internet:**
  Many existing attendance systems depend on additional machines or a continuous internet connection. This increases the cost and makes the system less dependable.
- **Not useful without internet:**
  Systems that work only through online services do not function properly when there is no internet or when the network is weak, which is a common issue in many places.

  Furthermore, most existing systems only focus on recording attendance data but fail to communicate it to the relevant stakeholders in real-time. In schools and colleges, parents are often left unaware of their child's absence until much later. Traditional communication methods like phone calls or emails are either manual and time-consuming or require a constant internet connection, which is not always available. This creates a communication gap that compromises student safety and institutional discipline.

1.2 Research Objectives and Contributions

This work focuses on solving the problems mentioned earlier by developing a face attendance system that works both offline and online. The system runs completely on a normal laptop using its built-in camera and does not need any extra devices.

The main goals of this work are:

- To create a face attendance system that works in real time without needing the internet.
- To make sure attendance is marked only for real people by checking that the person is actually present and not a photo or video.
- To save attendance records safely on the laptop itself.
- To upload the data to the cloud only when the internet is available, without affecting offline use.
- To bridge the communication gap by integrating an automated notification system that alerts parents or guardians immediately when a student is marked absent.

The main contributions of this work are:

1. A laptop-based attendance system that avoids extra hardware, making it low-cost and easy to use.
2. A secure attendance system that uses face recognition along with checks to stop fake or proxy attendance.
3. A system that works mainly offline, stores data locally, and syncs to the cloud only when a network connection is available, making it reliable even in areas with poor internet access.
4. An integrated GSM-based notification module that sends instant SMS alerts to parents without requiring internet access, ensuring high reliability and student safety in any environment.

2 Literature Review

2.1 Traditional and Automated Attendance Systems

For many years, schools and colleges have used manual methods to take attendance. These include calling out names or writing in registers. However, research shows that these methods are slow, waste class time, and often lead to mistakes such as wrong entries, repeated marking, or missing records[1]. Manual attendance also makes it easy for students to mark their friends' attendance, which makes the system unfair and unreliable.

To reduce this manual work, different automatic attendance methods have been introduced. In QR code–based systems, students scan a code using their mobile phones to mark attendance [2]. While this is faster, it still allows proxy attendance and needs a working internet connection. RFID-based systems use ID cards and card readers to mark attendance automatically [3]. Although they save time, students can share cards with others, which again leads to fake attendance. These systems also need extra devices, which increases cost and maintenance.

Biometric attendance systems try to solve identity problems by using physical features. Fingerprint systems are commonly used, but they have issues such as cleanliness, damage to sensors, and failure to work properly if fingers are dirty or wet [4]. Iris-based systems are very accurate, but they require costly equipment and controlled conditions, making them difficult to use in regular classrooms [5]. Due to these limitations, researchers began exploring face recognition as a more natural, contactless, and convenient solution for AM.

2.2 Face Recognition Techniques for Attendance Systems

Face recognition–based attendance systems identify people by looking at their faces, without needing any physical contact. Earlier systems used simple ways to recognise faces, but they did not work well when the lighting changed or when the face was not in the same position. Because of this, they often failed in real classroom situations.

Later research significantly improved recognition accuracy. LBP-based methods demonstrated better feature representation for attendance systems [6]. Deep learning approaches such as FaceNet introduced robust facial embeddings, enabling more accurate and scalable face recognition [7]. Transfer learning techniques further enhanced recognition performance under varying classroom conditions and limited training data [8]. Additionally, classifiers such as Support Vector Machines (SVM) have been effectively applied to deep face embeddings for accurate identity classification [9].

Even with these improvements, many face attendance systems still depend on the internet or special devices like small computers. This creates problems such as slow response, privacy issues, and failure when the internet is not available. These drawbacks are more common in rural areas or places with limited resources. As a result, face recognition systems that work completely offline on a normal laptop are more practical, reliable, and suitable for real-world classroom use.

2.3 Liveness Detection and Anti-Spoofing Methods

A major weakness of basic face recognition systems is their vulnerability to spoofing attacks. Individuals may attempt to deceive the system using printed photographs, recorded videos, or images displayed on mobile phones. Without additional verification, the system cannot distinguish between a live person and a fake image.

Several anti-spoofing techniques have been proposed to address this issue. Texture-based approaches using LBP features analyze surface patterns to differentiate real skin from printed materials [10]. Other methods detect natural facial movements such as blinking and micro-expressions to confirm live presence [11]. While effective under controlled conditions, these approaches may struggle under poor lighting or low camera quality.

More advanced techniques use deep learning–based depth estimation and convolutional neural networks (CNNs) to detect subtle differences in light reflection and surface texture between real faces and spoofing attempts [12]. These approaches offer higher reliability compared to traditional rule-based methods.

By integrating liveness detection into face attendance systems, security can be significantly enhanced. This ensures that attendance is recorded only when a real person is physically present, reducing proxy attendance and increasing overall system trustworthiness.

2.4 Summary of Research Gaps

From the studies reviewed, the following problems were found:

- Many systems depend on extra devices or internet-based services [2]–[5].
- Most systems do not work properly when there is no internet connection.
- There is not enough protection against fake attendance using photos or videos.
- Several face recognition systems lack robust protection against spoofing attacks [10]–[12].
- These systems are not suitable for rural areas or places with limited resources.
- The proposed system solves these problems by offering a secure face attendance system that works mainly offline on a normal laptop. It includes checks to ensure the person is real and uploads data to the cloud only when internet access is available.
- Lack of real-time communication: Most systems store data for administrative use but do not provide an automated, internet-independent way to notify parents or authorities about student absences immediately.

3 System Architecture and Methodology

The proposed face attendance system is a software system that operates entirely on a standard laptop using its built-in camera. It does not need any extra devices or constant internet access. Unlike systems that rely solely on hardware or online services, this system primarily operates offline while remaining safe and accurate. All face checking, attendance marking, and data saving are done on the laptop itself. When the internet is available, the data can be uploaded to the cloud in the background without affecting the system's offline use.

3.1 Three-Layer Architecture

The system is designed in three simple parts that work together. This helps the process move smoothly from capturing a person's face using the camera to safely saving their attendance record.

Physical Layer (Webcam Input Layer)

This part of the system uses the laptop's built-in camera to capture live video. The camera keeps taking pictures that may include one or more faces. Each captured image is marked with the time and then sent to the next part of the system for checking. Since it uses the laptop's own camera, no extra devices or equipment are needed. Additionally, it includes the GSM Module (SIM900A) connected via a serial port, which acts as the physical gateway to send SMS alerts to mobile networks.

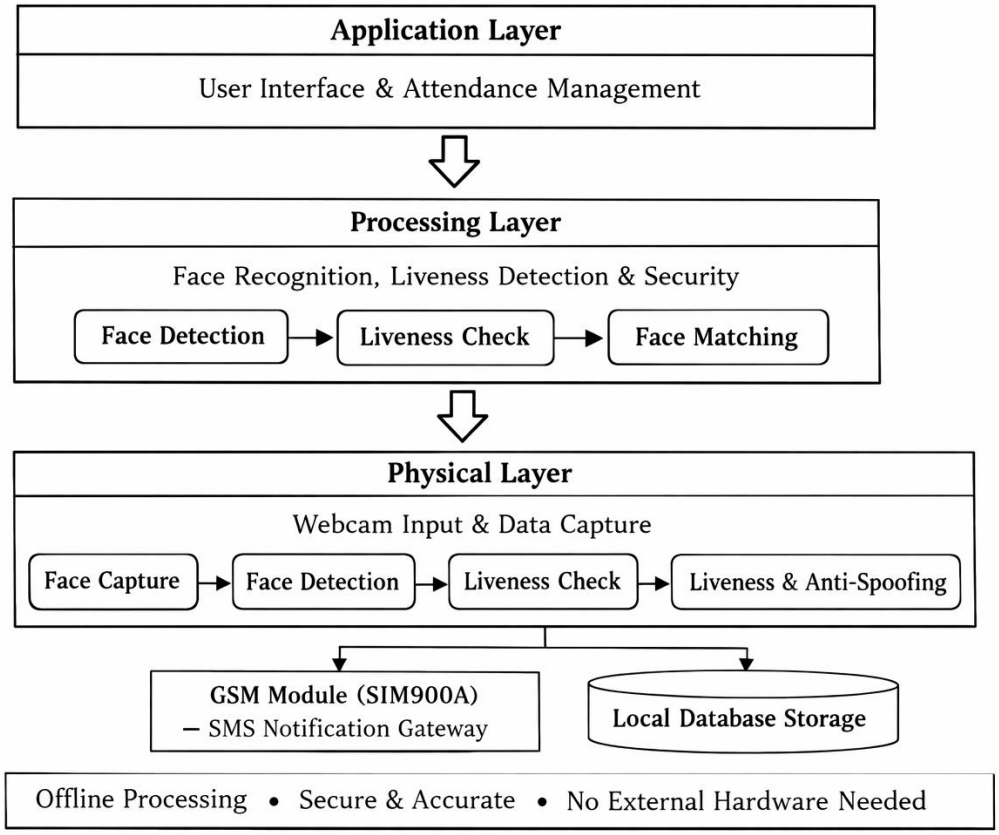

Figure 1: Three-Layer Architecture of the Proposed System.

Processing Layer (Face Recognition and Security Layer)

This part of the system does all the main work. It finds faces in the camera view, checks whose face it is, and makes sure the person is
really present. The system compares the detected face with saved face records. It also checks that the face is not a photo or a video being
shown to the camera. These checks help make sure that attendance is marked only for real people.

Application Layer (User Interface and Database Layer)

This part of the system is what the user sees and interacts with. It shows the live camera view, the names of recognized people, and whether their attendance has been marked. The attendance details are saved safely on the laptop itself. When the internet is available, the system can upload these records online in the background without disturbing normal use. It now includes the Notification Engine, which identifies students marked as "Absent" and triggers the GSM module to send real-time SMS alerts to parents.

3.2 Face Attendance System Workflow

The system works in a simple step-by-step way:

- **Face Capture:** The laptop camera takes live video.
- **Face Detection:** The system finds all faces in the video.
- **Face Recognition:** It checks if the faces match with registered users.
- **Liveness & Anti-Spoofing Check:** It makes sure the person is real and not a photo or video.
- **Attendance Marking:** Attendance is recorded only after the face is verified.
- **Automated Notification:** The system compares the "Present" list against the master "Student" list. For students found absent, the GSM module automatically sends an SMS notification to the registered parent's phone number.
- **Data Storage:** Records are saved on the laptop and can be uploaded to the cloud when internet is available.

This process makes the system fast, reliable, and secure.

3.3 System Data Model (Attendance Record)

The core digital entity in the system is the **Attendance Record**, which stores information related to recognized users and attendance events.

Field Name	What it means	Who updates it
User ID	A unique ID for each registered user	Registration Module
User Name	Name of the person	Database
Face Encoding	A stored digital version of the person's face	Face Registration
Date	The day attendance is recorded	Attendance Module
Time Stamp	The exact time attendance is recorded	Attendance Module
Status	Whether the person is Present or Absent	Decision Logic
Verification	Result of checks to make sure the person is real and not a photo/video	Security Module
Parent Contact	The mobile number used for SMS alerts	Registration Module
Notification Status	Whether the SMS was Sent or Failed	GSM/Notification Module

This organised way of storing data makes it easy to access, keeps it consistent, and ensures it is stored safely.

3.4 Liveness Detection and Anti-Spoofing Decision Logic

The Security Module is the smart part of the system. It makes sure that attendance is marked only for real people who are actually present.

3.4.1 Input Features and Attributes

The system looks at different details from the live video to check if the person is real:

Things it checks (Condition Attributes):

- **Facial motion:** Movements like blinking eyes or turning the head.
- **Texture patterns:** Difference between real skin and a photo or screen.
- **Frame consistency:** Whether the face looks natural over time in the video.
- Decision (Decision Attribute):
- Verification Status: Either Live (real person) or Spoof (fake photo/video).

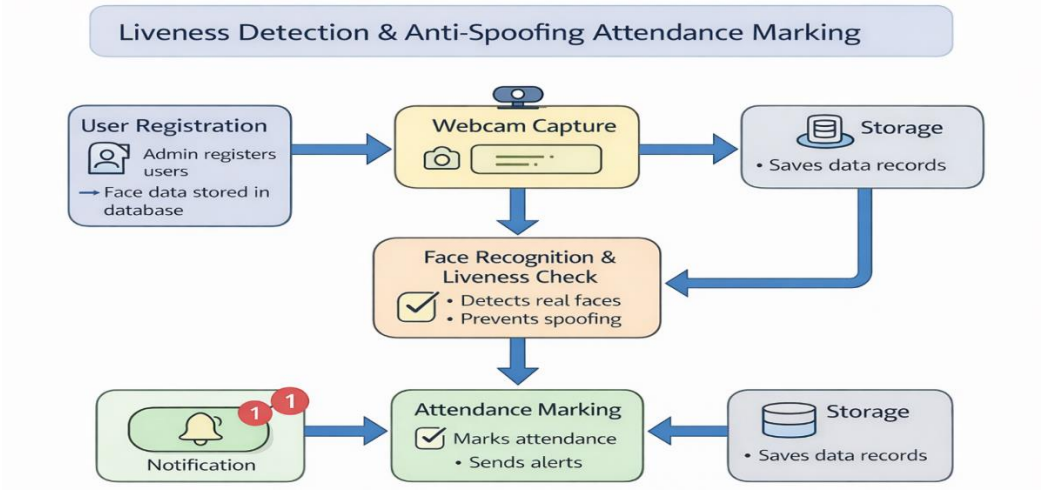

Figure 2: Input Features and Attributes

3.4.2 Verification Logic

The system looks at several video frames in a row to check if the face is moving naturally and if the skin looks real. Smart models (CNN-based) also check visual details to tell the difference between a real face and a fake one, like a photo or video.

- **Live Face:** The face shows natural movements and real skin texture.
- **Spoof Face:** The face looks flat, has unusual reflections, or does not move naturally.
- Only faces that are recognized as **Live** are allowed to have their attendance marked.

3.4.3 Rule Execution and Decision Making

The system uses simple decision rules, learned from training data, to decide if a face is real or fake.

Example Rules:

- **Rule 1:**
  If the face moves naturally **and** the skin looks real → mark as **Live**
- **Rule 2:**
  If the face does not move or the skin looks flat → mark as **Spoof**
- The system checks these rules in order, and the first rule that matches decides the result. This helps the system make quick decisions in real time.

3.5 Attendance Marking Workflow

The full attendance process works in these simple steps:

1. **User Registration:**
   The admin adds users, and their facial information is saved in the system.
2. **Live Recognition:**
   The laptop camera captures faces, and the system identifies who they are.
3. **Security Check:**
   The system checks that the person is real using liveness detection and anti-spoofing.
4. **Attendance Update:**
   If the face is verified as real, attendance is marked as **Present**.
5. **Data Storage and Sync:**
   Attendance records are saved on the laptop and can be uploaded to the cloud when the internet is available.
6. **Absentee Notification:** The system runs a cross-check algorithm to find missing students and uses the GSM Gateway to send instant SMS alerts to parents, ensuring transparency even without internet access.

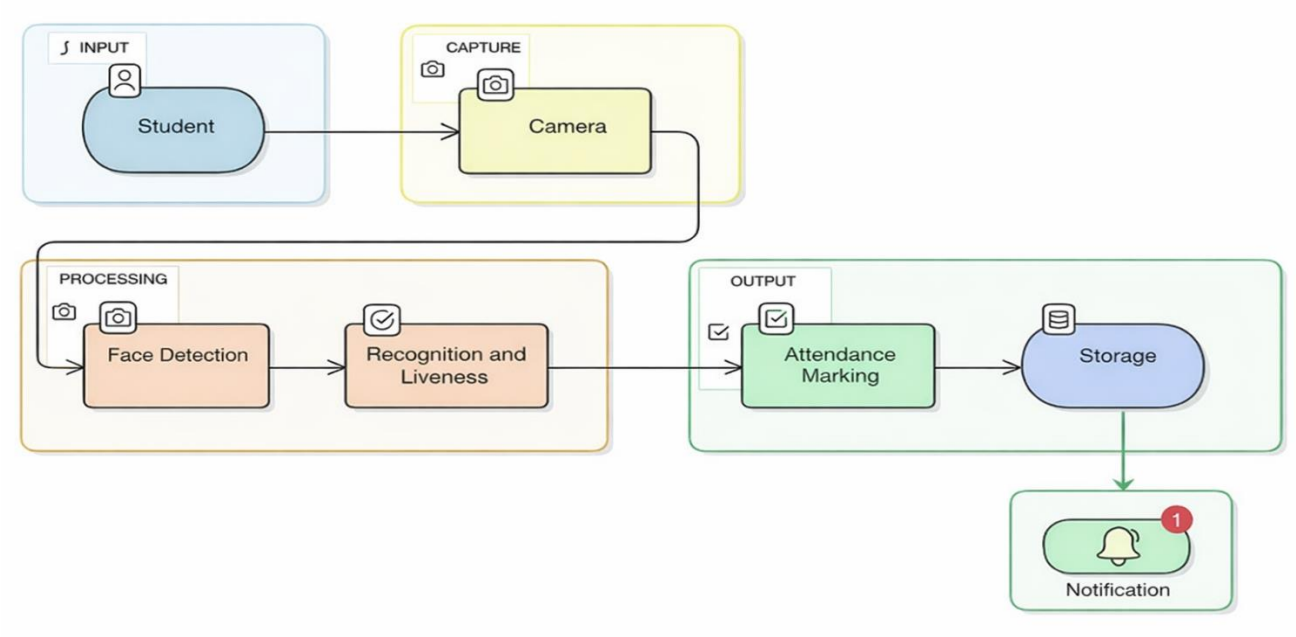

Figure 3: System Architecture of the proposed System

4 Implementation and Performance Analysis

4.1 Experimental Setup

The proposed face attendance system was built and tested on a normal laptop without needing any extra devices or constant internet. Everything runs on the laptop itself to check how well it works in real-time offline.

Experimental Setup:

- **Laptop**: Standard laptop with a built-in webcam, Intel processor, and at least 8 GB RAM.
- **Programming:** Python was used to write the system.
  - **GSM Module**: SIM900A Modem connected via USB-to-TTL converter to the laptop's USB port.
  - **SIM Card:** A standard active SIM card with SMS credits for sending notifications.
  - **Libraries/Tools:** OpenCV (Face Detection), PySerial (to communicate with the GSM hardware via AT Commands), and SQLite.
- **User Interface:** A simple Python GUI using Tkinter or PyQt.
- **Database:** SQLite to store attendance records locally.
- **Camera:** Laptop webcam for live video.

The system was tested in indoor, classroom-like settings with different lighting and multiple people in the camera view. All tests were done offline, and the cloud sync was turned off to see how well the system works without internet.

4.2 Performance Evaluation Metrics

The system's performance was checked using some important measurements commonly used for RTFR:

1. How often the system correctly identifies registered users.
2. **Processing Latency (ms):**
   The time it takes to detect, recognize, and verify a face from the live video.
3. **Multi-Face Handling:**
   Whether the system can detect and recognize more than one face at the same time.

4. **Spoof Detection Accuracy:**
   How well the system can detect fake faces, like photos or videos, and block them.
5. **Notification Latency (s):** The time taken from the moment a student is identified as "Absent" to the moment the SMS is successfully delivered to the mobile network.

These measurements show how fast, reliable, and secure the system is.

4.3 Results and Analysis of Recognition Performance

The system was tested with different numbers of registered users in various situations. The results showed that it could recognize faces accurately and work smoothly.

Table 2: Recognition Performance under Varying Face Counts

Scenario	Number of Faces	Recognition Accuracy	Performance Impact
Single User	1	High	Very Low Processing Load
Small Group	3-5	High	Low Processing Load
Classroom Setup	6-10	Slightly Reduced	Moderate Load

The system recognized faces very well for one person or small groups. In larger groups, accuracy dropped a little because the system had more work to do, but it still worked in real time without any noticeable delay.

Processing Latency Analysis

Processing latency directly affects user experience in real-time systems. The average processing times observed were:

Table 3: Processing Latency Analysis of the Proposed System

Operation	Average Time (ms)	Description
Face Detection	20–30 ms	Finds faces in the video
Face Recognition	30–40 ms	Matches the face with saved records
Liveness & Anti-Spoofing	25–35 ms	Checks that the face is real, not a photo or video
Total Frame Processing	80–100 ms	Time to complete all steps for one video frame

The total time per frame shows that the system works smoothly in real time. Since everything happens on the laptop itself, there is no delay from the internet.

4.4 Analysis of Liveness Detection and Anti-Spoofing

The anti-spoofing part of the system was tested using printed photos, images on mobile phones, and recorded videos. The system was able to block most fake attempts by checking how the face moves, the skin texture, and how the face looks over several frames.

Key points from testing:

- Printed photos did not show natural face movements.
- Mobile phone images looked flat and had reflection spots.
- Real people showed smooth and consistent face movements over time.
- These results show that checking for live faces makes the system much more secure and stops fake or proxy attendance.

4.5 Discussion on System Effectiveness

The implemented system achieved several important results:

1. **Works Offline:**
   The system runs reliably without the internet, so attendance can be marked anytime.
2. **High Security:**
   Using face recognition along with checks for fake faces stops proxy or fake attendance.
3. **Low Cost:**
   It only needs a normal laptop and webcam, so it is cheap to set up.
4. **Easy to Expand:**
   The system is designed in parts, so new features or cloud services can be added later without changing the whole system.

4.7 Results and Analysis of the Notification System

The notification system was tested by purposefully leaving registered students out of the camera view to trigger "Absent" alerts.

Table 4: GSM-Based Notification System Performance Analysis

Notification Task	Average Time	Success Rate
Absentee Identification	1.2 Seconds	100%
GSM Port Initialization	2.5 Seconds	98%
SMS Delivery (Network)	5.0 - 8.0 Seconds	95% (Signal dependent)

Analysis: The system successfully identified absentees by comparing the live attendance file against the master student list. The SIM900A module showed high reliability in sending SMS messages even when the laptop had no internet connection, proving the system's effectiveness for rural or offline environments.

5 Results

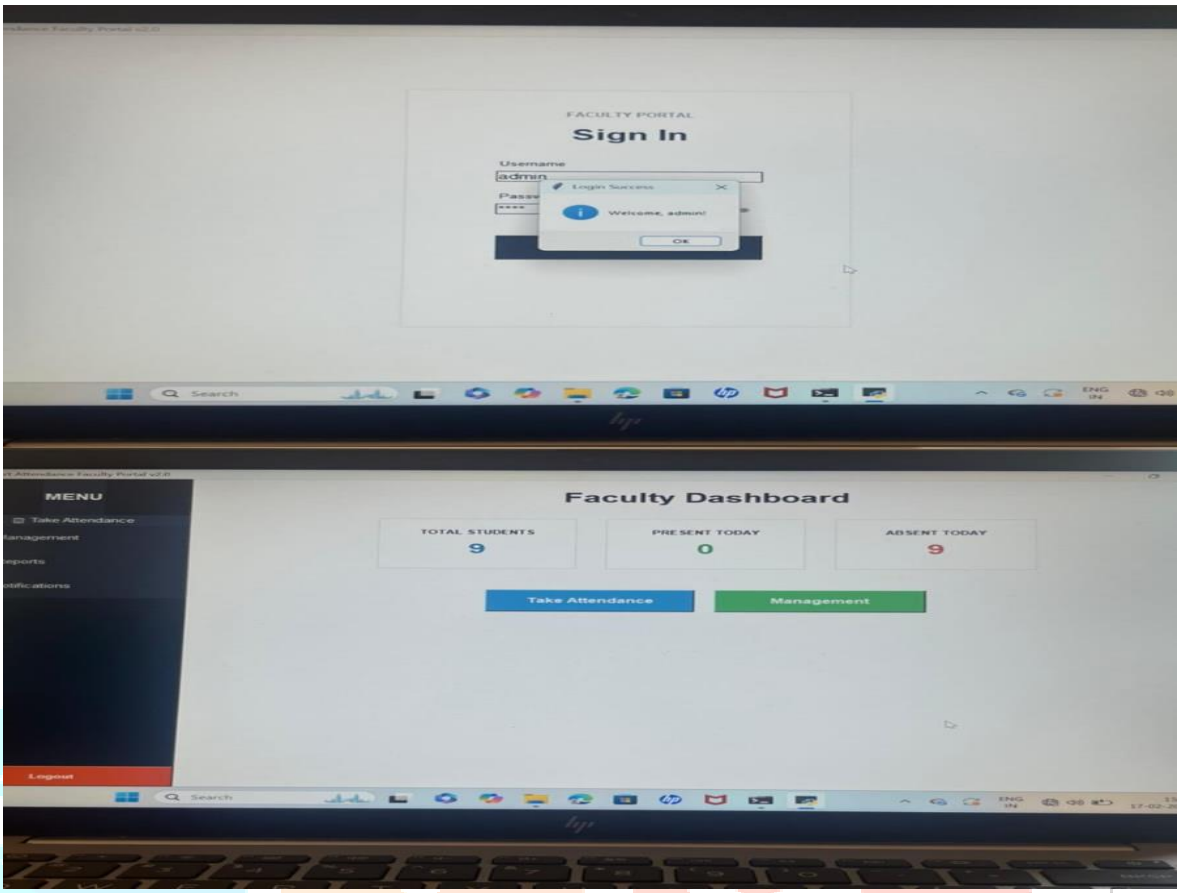

Figure 3: The login page with a welcome, admin message and the faculty dashboard that opens with the successful entry of the right credentials in the login page

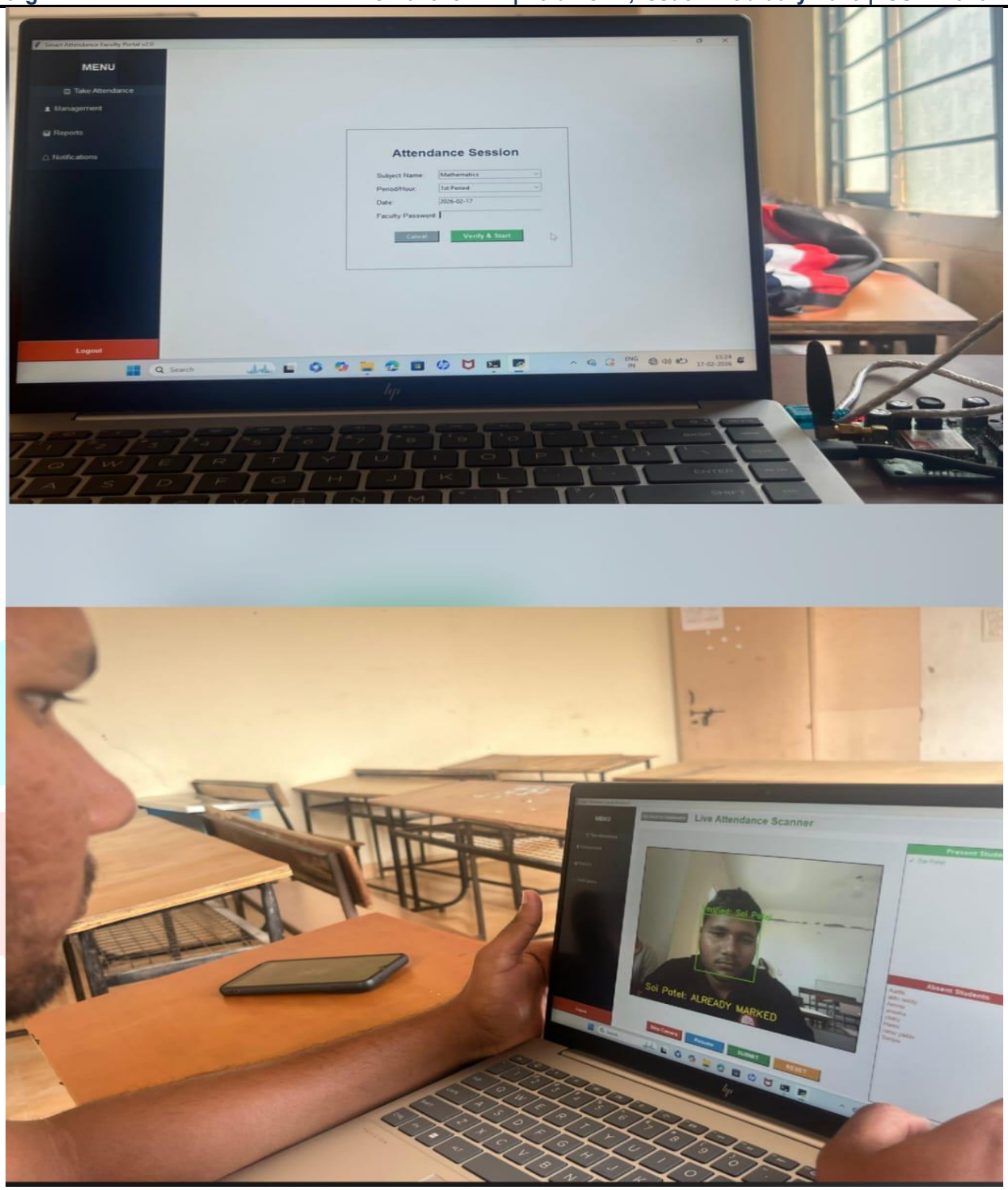

Figure 4: The Attendance page shows the subject, period, date, and faculty password to enter. After entering the correct credentials, it will open the webcam with recognizes the student with liveness detection using blink detection and head movement.

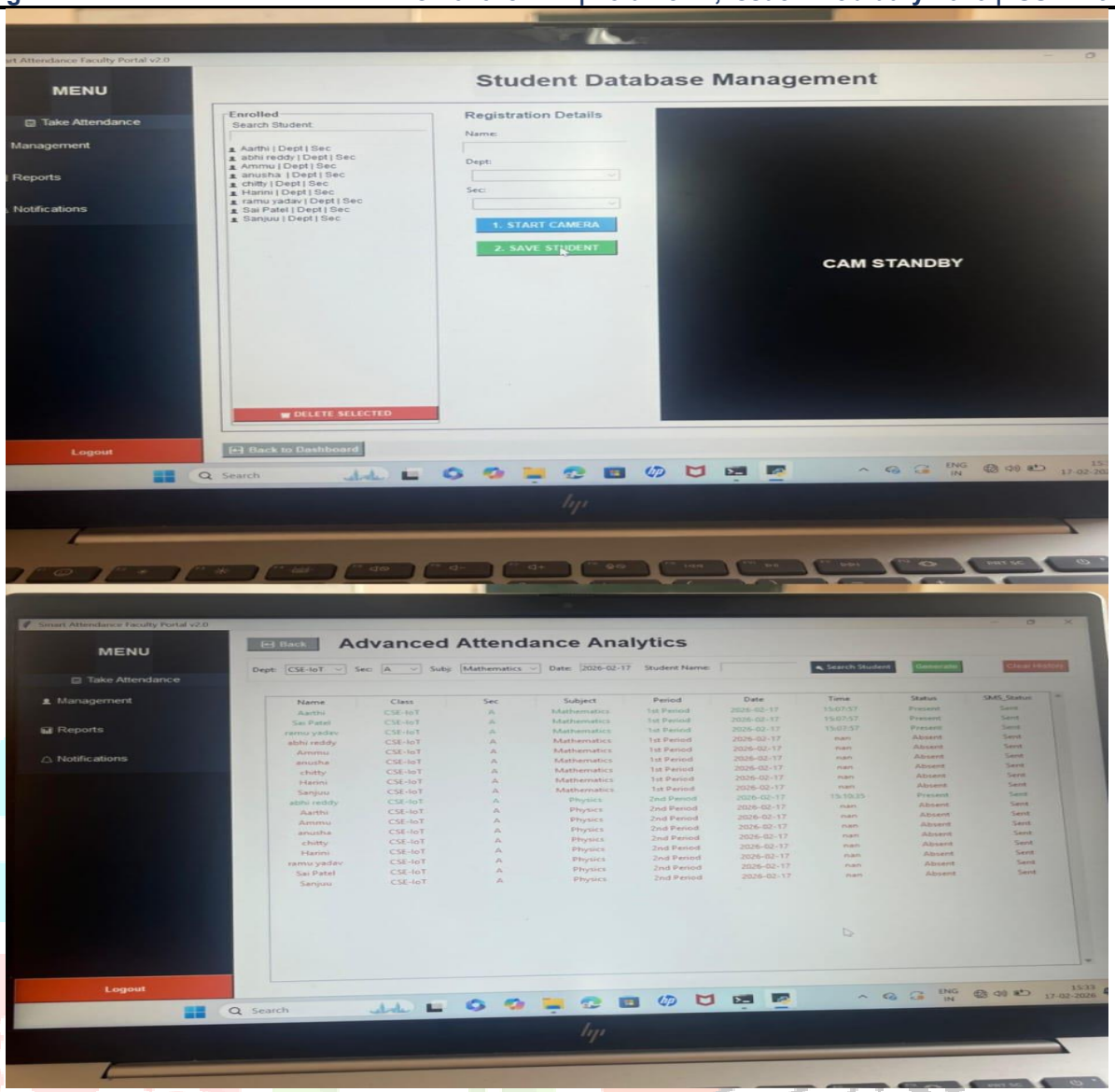

Figure 5: The management page helps to enrol a new student into the database using a webcam. And the reports page will show the attendance reports of students based on their department and section, with the subject, period, date and time, and the status of present and absent.

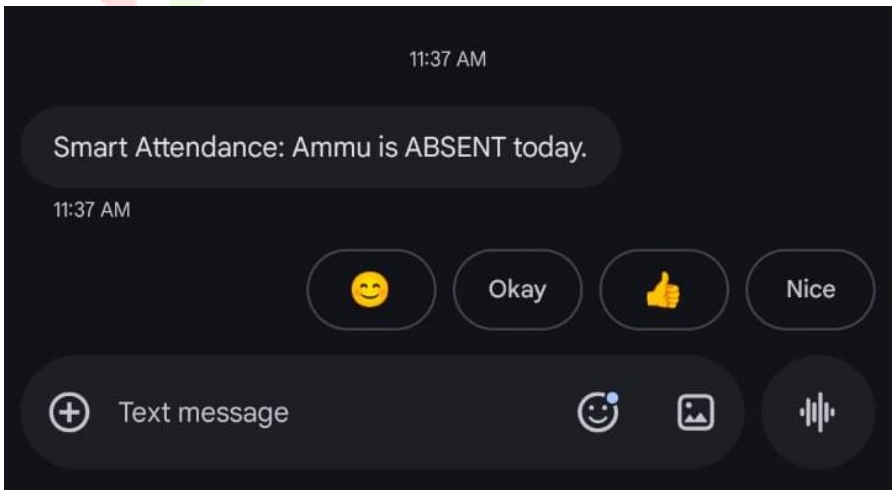

Figure 6: Notification sent to parents if their child is absent, using the SIM900A GSM Modem.

6 Conclusion and Future Work

6.1 Conclusion

This research successfully created and tested a face attendance system that works both offline and online. It uses real-time face recognition along with checks to make sure the person is really there and not a photo or video. The system runs completely on a normal laptop using its built-in camera, so it doesn't need extra devices or constant internet. This makes it cheap, easy to use, and suitable for schools or colleges with limited resources.

By adding liveness detection and a smart anti-spoofing model, the system can prevent fake attendance using photos, videos, or mobile screens. Tests showed that it recognises faces accurately, works quickly, and handles multiple people in real time. Because it mainly works offline, attendance can be recorded without interruption, and data can be safely backed up to the cloud when the internet is available. A significant feature of this system is the integration of an automated notification module. By utilising a GSM-based gateway, the system bridges the gap between attendance marking and parental awareness. It identifies absentees in real-time and immediately sends SMS alerts to guardians without requiring an internet connection. This ensures that the system is not only a tool for record-keeping but also a proactive security measure. Overall, this system provides a reliable, secure, and practical way to take attendance automatically, solving the main problems of traditional and existing automated systems.

6.2 Future Work

While the current system performs reliably, there are several avenues for future enhancement:

- **Advanced Liveness and Security:** Future iterations could integrate 3D facial mapping and depth sensors to further strengthen anti-spoofing capabilities. Incorporating "active" liveness checks, such as asking a student to blink or smile on command, would add an extra layer of security.
- **Enhanced Communication Channels**: While the GSM SMS feature is highly reliable for offline areas, future updates could include multi-channel notifications. This would allow the system to send WhatsApp messages, automated emails, or push notifications through a dedicated mobile app when an internet connection is detected, providing more detailed reports to parents.
- **Smart Analytics and Scalability:** The system can be upgraded to include a predictive analytics dashboard. This would allow administrators to track long-term attendance patterns, identify students at risk of falling behind due to absenteeism, and generate automated performance insights.
- **Edge Computing Integration:** To support very large institutions, the recognition models could be optimised to run on "Edge" devices like Raspberry Pi, allowing multiple classrooms to be monitored simultaneously while syncing to a single central faculty dashboard.

7 Acknowledgment

We would like to express our sincere gratitude to our project guide, **Mrs Y.B. T. Sundari, for her continued support, valuable guidance, and constructive suggestions throughout the development of our research**. Her encouragement, insightful feedback, and technical expertise greatly contributed to the successful completion of our Smart Face Attendance System project.

We are deeply thankful to the Department of **CSE–IoT** at **Holy Mary Institute of Technology and Science** for providing us with the necessary facilities, infrastructure, and academic environment to carry out this research successfully.

We also extend our heartfelt appreciation to all the faculty members for their support and cooperation. Finally, we would like to thank our families and friends for their constant encouragement, understanding, and motivation throughout the course of this project.

8 References

[1] R. Kumar, A. Verma, and S. Gupta, "Manual attendance systems: challenges and inefficiencies," Journal of Educational Technology, vol. 12, no. 3, pp. 44–50, 2018.

[2] P. Sharma and K. Patel, "QR-code based student attendance tracking," International Conference on Smart Systems, pp. 112–118, 2019.

[3] S. Chatterjee, M. Roy, and R. Sen, "RFID-enabled attendance management system," IEEE Int. Conf. on Computing, Power and Communication, pp. 264–269, 2017.

[4] D. Prasad and V. Rao, "Fingerprint biometric attendance for academic institutions," IEEE Int. Conf. on Intelligent Computing, pp. 89–94, 2016.

[5] A. Jain and R. Desai, "Iris-based biometric authentication for attendance automation," IEEE Sensors Journal, vol. 18, no. 9, pp. 3801–3808, 2018.

[6] A. Mahmood, L. Khan, and S. Ali, "LBP-based face recognition attendance system," International Journal of Image Processing, vol. 14, no. 2, pp. 55–63, 2020.

[7] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition," IEEE CVPR, pp. 815–823, 2015.

[8] M. Rahman and N. Ahmed, "Transfer learning for robust student face recognition," IEEE Access, vol. 7, pp. 176448–176459, 2019.

[9] Y. Jiang and W. Lee, "SVM classification of deep face embeddings," Pattern Recognition Letters, vol. 138, pp. 223–229, 2020.

[10] D. Wen, H. Han, and A. Jain, "Face liveness detection using LBP features," IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746–760, 2015.

[11] J. Kannala et al., "Micro-expression and blink detection for anti-spoofing," IEEE Int. Conf. on Biometrics, pp. 1–8, 2018.

[12] X. Zhang, Y. Guo, and F. Li, "CNN-based depth estimation for face spoof detection," IEEE Transactions on Biometrics, vol. 5, no. 2, pp. 145–156, 2021.