IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SmartID: IoT-Based Smart Attendance System with Dual Authentication Using Face Recognition and RFID

Vinay Kumar Gajendra [1], Ritik Kumar [2], Vineeth Menon [3], Jason Ralph Das [4], Neha Choubey [5]

[1,2,3,4] Students, Computer Science and Engineering (IoT, Cyber Security and Blockchain Technology)
Shri Shankaracharya Technical Campus

[5] Assistant Professor, Computer Science and Engineering
Shri Shankaracharya Technical Campus

ABSTRACT

In many educational institutions, traditional attendance systems often rely on manual entry or single-layer authentication methods, which can lead to inaccuracies, proxy attendance, and inefficient record management. To address these limitations, this paper presents "SmartID", an IoT-based smart attendance system that integrates dual authentication using face recognition and RFID technology. The system is designed to ensure secure, reliable, and automated attendance tracking. The proposed system combines real-time facial recognition with RFID card verification to provide an additional layer of authentication. A NodeMCU (ESP8266) module is used to establish communication between the hardware components and cloud-based services. Upon successful authentication, attendance data is transmitted and stored in Google Sheets, enabling centralized and easily accessible record management. Additionally, an automated email notification feature is incorporated to inform users of their login activity, enhancing transparency and security.

The system is capable of handling both login and logout events, along with calculating the duration of presence. By minimizing manual intervention and reducing the chances of proxy attendance, SmartID improves both accuracy and efficiency. The implementation demonstrates a practical and cost-effective solution suitable for academic institutions and other environments requiring secure attendance monitoring.

Overall, the integration of IoT with biometric and RFID-based authentication provides a scalable and reliable framework for modern attendance systems.

Index Terms - Smart Attendance System, Face Recognition, RFID, Internet of Things (IoT), Dual Authentication, NodeMCU (ESP8266), Google Sheets Integration, Email Notification.

I. INTRODUCTION

Over the past few years, the need for reliable and efficient attendance management systems has increased significantly, especially in educational institutions and organizations. Traditional methods of attendance recording, such as manual registers or card-based systems, are often time-consuming and prone to errors. These methods also fail to prevent proxy attendance, where one individual marks attendance on behalf of another, leading to inaccurate records and reduced system reliability.

With the advancement of technology, various automated attendance systems have been proposed, including biometric and RFID-based solutions. While these systems improve efficiency, they often rely on a single mode of authentication, which may still be vulnerable to misuse or unauthorized access. For instance, RFID cards can be shared among users, and standalone face recognition systems may face challenges in certain environmental conditions.

To overcome these limitations, this work introduces “SmartID”, an IoT-based smart attendance system that combines face recognition and RFID technologies to provide dual authentication. The integration of these two methods enhances the overall security and reliability of the system by ensuring that both identity verification and physical presence are validated simultaneously.

The system utilizes a NodeMCU (ESP8266) module to enable communication between hardware components and cloud-based services. Attendance data is automatically recorded and stored in Google Sheets, allowing for centralized and real-time access. Additionally, an email notification feature is incorporated to inform users about their login activity, further improving transparency and user awareness.

The proposed system is designed to handle both login and logout operations, along with calculating the duration of attendance. By reducing manual intervention and minimizing the chances of proxy attendance, SmartID provides a practical and efficient solution suitable for modern attendance management requirements.
The proposed approach focuses on combining multiple technologies in a practical and cost-effective manner to enhance the reliability of attendance systems. By integrating hardware and software components seamlessly, the system ensures real-time processing and efficient data management. This approach not only improves accuracy but also provides a user-friendly experience suitable for everyday institutional use.

II. LITERATURE REVIEW

Over the years, attendance management systems have undergone significant transformation, evolving from manual record-keeping methods to more automated and intelligent solutions. Traditional approaches, such as maintaining attendance registers or marking presence manually, are still widely used in many institutions. However, these methods are often time-consuming, prone to human errors, and susceptible to proxy attendance. Such limitations have motivated researchers and developers to explore technology-driven alternatives that can improve accuracy and efficiency.

One of the earliest advancements in automated attendance systems involved the use of RFID (Radio Frequency Identification) technology. RFID-based systems allow users to mark attendance by scanning a card or tag, which is linked to a unique identification number. This approach significantly reduces manual effort and speeds up the attendance process. Several studies have demonstrated that RFID systems are effective in environments where quick identification is required. However, these systems are not entirely secure, as RFID cards can be shared among users, leading to false attendance records.

To overcome the limitations of single-factor authentication, biometric-based systems, particularly face recognition, have gained popularity. Face recognition systems use image processing and machine learning techniques to identify individuals based on their facial features. These systems provide a higher level of security compared to RFID, as facial characteristics are unique to each individual. Researchers have explored various algorithms for face detection and recognition, including Haar

cascades and deep learning-based models, to improve accuracy under different lighting and environmental conditions. Despite their advantages, face recognition systems may face challenges such as variations in lighting, facial expressions, and occlusions.

In recent years, there has been a growing interest in integrating multiple authentication techniques to enhance system reliability. Hybrid systems that combine RFID and biometric verification have been proposed to address the weaknesses of individual methods. Such systems ensure that both identity verification and physical presence are validated, thereby reducing the chances of misuse. Studies have shown that multi-factor authentication significantly improves the robustness of attendance systems, especially in academic and organizational environments.

With the advancement of the Internet of Things (IoT), modern attendance systems have started incorporating network-enabled devices for real-time data processing and storage. Microcontrollers such as the NodeMCU (ESP8266) have been widely used due to their built-in Wi-Fi capabilities and cost-effectiveness. These devices enable seamless communication between hardware components and cloud-based services. Integration with platforms like Google Sheets allows for centralized data storage, easy accessibility, and real-time updates without the need for complex database management systems.

Additionally, the inclusion of notification mechanisms, such as email alerts, has further enhanced the usability of smart attendance systems. These features provide immediate feedback to users and improve transparency by informing them of their attendance status. Such integrations demonstrate how combining IoT with cloud services can create efficient and user-friendly systems.

Although significant progress has been made in this domain, there is still a need for systems that are not only accurate and secure but also affordable and easy to implement. Many existing solutions either focus heavily on hardware complexity or require expensive infrastructure. This highlights the importance of developing a balanced system that integrates reliability, cost-effectiveness, and ease of use.

The proposed SmartID system builds upon these existing approaches by combining RFID and face recognition with IoT-based communication and cloud integration. By leveraging the strengths of each technology, the system aims to provide a practical and scalable solution for modern attendance management.

III. METHODOLOGY

The proposed SmartID system is designed to provide a secure, efficient, and automated attendance management solution by integrating face recognition, RFID authentication, and IoT-based communication. The system follows a multi-layered approach where both identity verification and physical presence are validated before recording attendance. This section describes the overall system architecture, working mechanism, and data flow involved in the implementation.

III. I System Architecture & Data Flow

The SmartID system consists of both hardware and software components that work together to ensure seamless operation. The primary hardware components include a camera module for capturing facial images, an RFID reader for scanning identification cards, and a NodeMCU (ESP8266) microcontroller that acts as the communication bridge. On the software side, Python-based face recognition is used for identity detection, while Google Apps Script is utilized to store attendance data in Google Sheets.
The system operates in a connected environment where the NodeMCU (ESP8266) sends HTTP requests to a cloud-based script, enabling real-time data storage and retrieval. This architecture eliminates the need for a dedicated server and makes the system cost-effective and scalable.
The overall system architecture and data flow of the proposed SmartID system is illustrated in Fig.1.

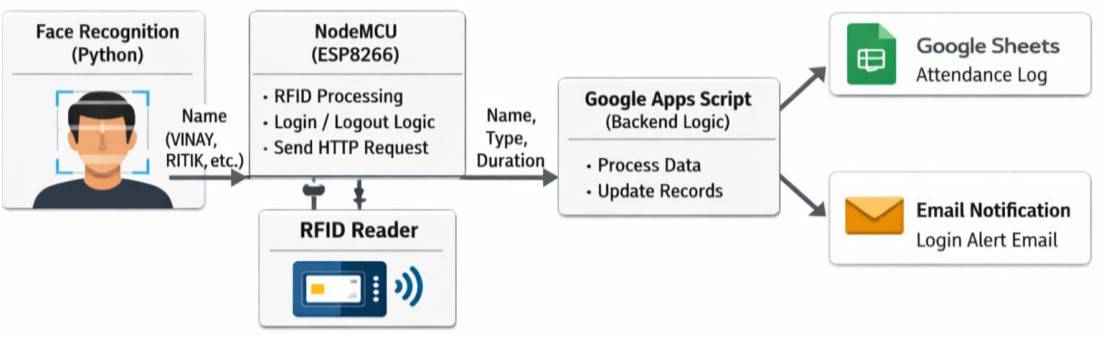

Fig. 1: System Architecture and Data Flow of Smart Attendance System

The data flow in the system is designed to be simple and efficient. Once authentication is completed, the NodeMCU (ESP8266) constructs a URL containing the required parameters and sends an HTTP GET request to the deployed Google Apps Script. The script extracts these parameters and processes them accordingly.

The attendance data is then stored in Google Sheets, which acts as a centralized and easily accessible database. The use of cloud storage ensures that data can be accessed from anywhere without requiring additional infrastructure.
The communication between components is carried out over Wi-Fi, making the system flexible and easy to deploy in various environments. The use of lightweight protocols ensures minimal delay and efficient data transmission.

III. II Working Procedure

The working of the system begins with user identification through face recognition. When a user appears in front of the camera, the system captures the facial image and compares it with the trained dataset. If a match is found, the system proceeds to the next level of authentication using RFID.

The user is then required to scan their RFID card, which contains a unique identifier. The system verifies whether the scanned RFID corresponds to the recognized face. This dual authentication mechanism ensures that unauthorized access and proxy attendance are minimized.

Once both authentication steps are successfully completed, the NodeMCU (ESP8266) sends a request to the Google Apps Script web service. The request includes parameters such as user name, login or logout status, and duration (in case of logout). The script processes this data and records it in Google Sheets along with the current date and time.
Additionally, an email notification is triggered during login events, informing the user about their attendance entry. This feature enhances transparency and allows users to track their activity in real time.

III. III Key Features of the Proposed System

The proposed SmartID system incorporates several important features that enhance both security and usability. One of the key aspects of the system is the implementation of dual authentication, where both face recognition and RFID verification are required to validate user identity. This significantly reduces the possibility of proxy attendance and unauthorized access.
Another notable feature is the integration of IoT-based communication using the NodeMCU (ESP8266) module, which enables real-time data transmission to cloud-based services. The use of Google Sheets for data storage provides a centralized and easily accessible platform for managing attendance records without the need for complex database systems.
In addition to this, the system includes an automated email notification mechanism that informs users about their login activity. This feature improves transparency and ensures that users are aware of their attendance status.

Furthermore, the system is capable of handling both login and logout events while automatically calculating the duration of attendance. This provides more detailed insights into user presence and enhances the overall functionality of the system.
The design of the SmartID system focuses on simplicity, cost-effectiveness, and scalability, making it suitable for deployment in educational institutions and other environments requiring reliable attendance monitoring.

IV. IMPLEMENTATION AND RESULTS

The SmartID system was implemented by integrating multiple hardware and software components to achieve a reliable and automated attendance solution. The system was tested under real-time conditions to evaluate its performance in terms of accuracy, response time, and reliability. This section describes the implementation details of individual modules and presents the observed results.

IV. I System Setup and Tools

The implementation of the SmartID system involves both hardware and software components. The hardware setup includes a NodeMCU (ESP8266) microcontroller, an RFID reader module, and a camera for capturing facial data. The NodeMCU (ESP8266) is responsible for handling RFID inputs and communicating with cloud services through Wi-Fi.

On the software side, Python is used for implementing the face recognition module, utilizing image processing techniques to identify users. Visual Studio Code is used as the development environment for executing and monitoring the system. Google Apps Script is deployed as a web service to handle incoming data and update attendance records in Google Sheets.
The integration of these components enables seamless communication between the local system and cloud-based services, ensuring real-time data processing and storage.

The SmartID system includes a NodeMCU (ESP8266), RFID reader, LCD display, and supporting circuitry. The RFID reader scans user cards, while the LCD displays system status. The NodeMCU (ESP8266) controls the system and manages communication with cloud services. The hardware setup is shown in Fig. 2.

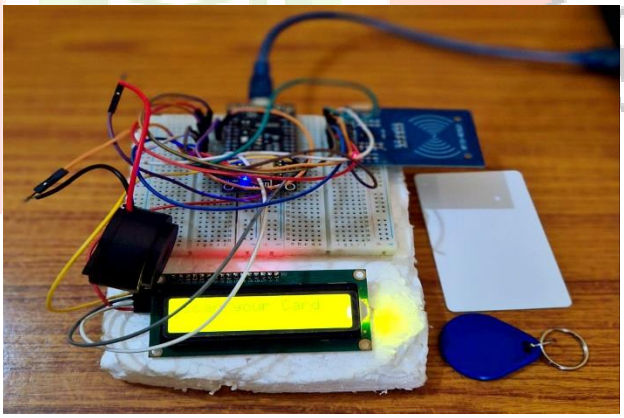

Fig. 2: Hardware Setup of SmartID Attendance System

IV. II Face Recognition Module

The face recognition module detects and analyzes facial features using a trained dataset of registered users. The system captures real-time video and extracts key facial patterns, which are compared with stored data to identify the user. This process ensures reliable recognition under normal variations such as lighting and facial expressions.
Once a face is detected, it is compared with the stored dataset, and the corresponding name is identified. The recognized name is then passed to the next stage of the system for further verification.

The module is designed to operate in real time, ensuring minimal delay in recognition.

The output of the face recognition process is illustrated in Fig. 3, where the system successfully detects and identifies a registered user in real time. The displayed output confirms that the trained dataset is effectively utilized for accurate identification, enabling seamless progression to the next stage of authentication.

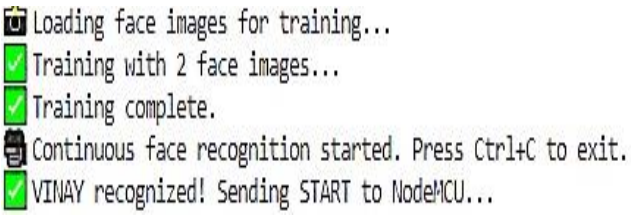

Fig. 3: Face Recognition Module Identifying Registered User

IV. III RFID Authentication Module

RFID technology is used as a second layer of authentication to enhance system security. Each user is assigned a unique RFID tag containing identification data. The RFID reader retrieves this data through contactless communication, enabling fast and efficient verification.

The system verifies whether the scanned RFID corresponds to the recognized face. This dual authentication mechanism ensures that only authorized users are allowed to mark attendance, thereby reducing the chances of proxy attendance.
The RFID-based authentication process is demonstrated in Fig. 4, where the system reads the card data and verifies it against the recognized user. The output confirms successful authentication, ensuring that only authorized users are allowed to proceed with attendance marking.

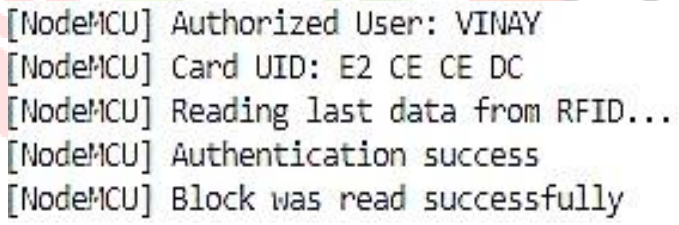

Fig. 4: RFID-Based Authentication and User Verification

IV. IV Data Transmission and Cloud Integration

Once both authentication steps are completed successfully, the NodeMCU (ESP8266) constructs an HTTP request containing user details such as name, login or logout status, and duration of attendance. This request is sent to a Google Apps Script deployed as a web service.

The script processes the received data and records it in Google Sheets along with the current date and time. The system also triggers an email notification during login events, informing the user about their attendance entry. This integration ensures centralized data storage and real-time accessibility.

Once authentication is complete, the system sends user data to a cloud-based Google Apps Script. The login event is recorded and transmitted using an HTTP request, enabling real-time data processing. This

process is shown in Fig. 5.

Date	Time	Name	Status	Type	Duration
01/04/26	9:19:03	VINAY	Present	Login	
01/04/26	9:20:50	VINAY	Present	Logout	1 min 47 sec
01/04/26	9:29:23	RITIK	Late	Login	
01/04/26	9:33:28	RITIK	Late	Logout	4 min 3 sec

Fig. 5: Login Event and Data Transmission to Cloud

The attendance data is stored in Google Sheets, which acts as a centralized database. It records details such as date, time, user name, status, and duration, allowing easy access and management. The stored data is shown in Fig. 6.

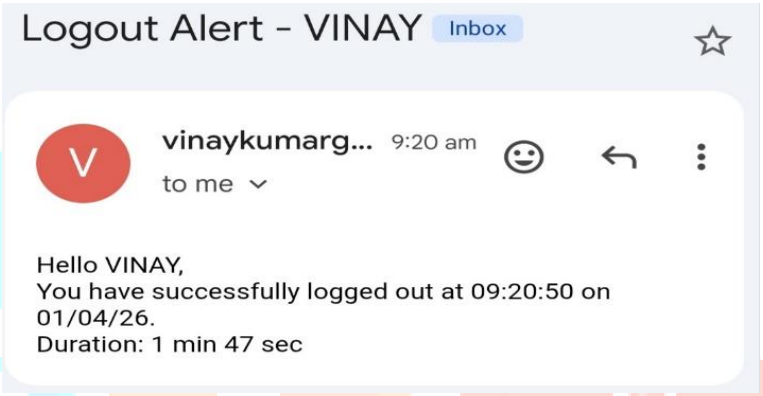

Fig. 6: Attendance Data Stored in Google Sheets

An email notification feature informs users about their attendance activity. After login or logout, a message is sent containing details such as time and duration. This improves transparency and user awareness. A sample notification is shown in Fig. 7.

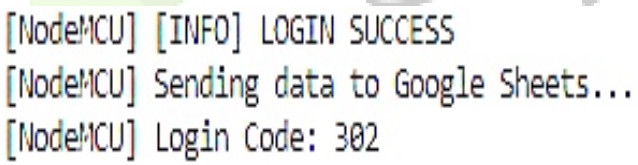

Fig. 7: Email Notification Sent to User After Attendance Event

IV. V Results and Observations

The SmartID system was tested under different scenarios to evaluate its performance and reliability. The system responded efficiently to user interactions and maintained proper synchronization between hardware components and cloud services.

The integration with Google Sheets allows for efficient data management, while the email notification feature enhances transparency. The system demonstrated consistent performance with minimal delay in processing, making it suitable for practical deployment in academic and organizational environments. Overall, the implementation confirms that the proposed system provides a reliable, cost-effective, and scalable solution for attendance management.

The final system output, including logout event and duration calculation, is shown in Fig. 8. The results demonstrate that the system accurately records both login and logout activities while automatically computing the duration of presence, validating the effectiveness of the integrated approach.

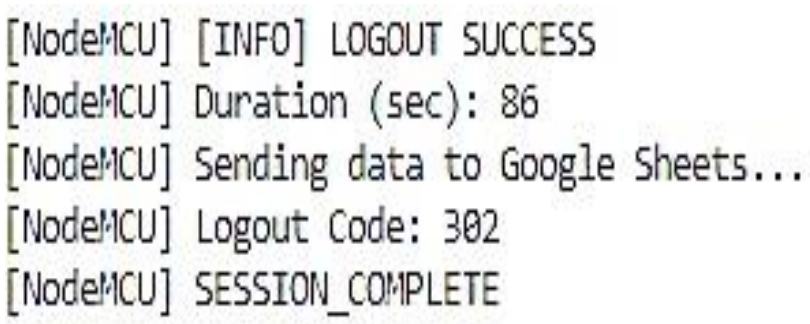

Fig. 8: Logout Event and Duration Calculation

V. CONCLUSION

The SmartID system provides an efficient and reliable solution for automated attendance management by integrating face recognition and RFID-based authentication. The dual authentication approach enhances security by verifying both identity and physical presence, reducing the chances of proxy attendance.

The system successfully records attendance in real time, calculates duration, and stores data in Google Sheets for easy access. The addition of email notifications further improves transparency. Overall, the system demonstrates a practical, cost-effective, and scalable approach suitable for educational and organizational use.

VI. FUTURE SCOPE

The SmartID system can be further improved by integrating a mobile or web-based interface for easier access to attendance records.

The face recognition module can be enhanced using advanced models to improve accuracy under different conditions.

Additionally, the use of a dedicated database instead of Google Sheets can improve scalability for larger datasets.

Security can also be enhanced by incorporating features such as liveness detection.

These improvements will make the system more robust and suitable for real-world deployment.

VII. REFERENCES

[1] OpenCV, “Open-Source Computer Vision Library”, https://opencv.org/

[2] A. Geitgey,“Face Recognition Library Documentation”, https://github.com/ageitgey/face_recognition

[3] Espressif Systems, “ESP8266EX Datasheet”, https://www.espressif.com/

[4] Google Developers, “Google Apps Script Documentation”,https://developers.google.com/apps-script/

[5] Google Developers, “Google Sheets Integration Guide”, https://developers.google.com/sheets/api/

[6] MFRC522 RFID Module Documentation, NXP Semiconductors.

[7] Python Software Foundation, “Python Documentation”, https://docs.python.org/

[8] S. Z. Li and A. K. Jain, “Handbook of Face Recognition,” Springer, 2011.

[9] K. Finkenzeller, “RFID Handbook: Fundamentals and Applications,” Wiley, 2010.