

UID-Linked Facial Authentication System (FIDAS): A Real-Time RFID-Triggered Selective-Frame Approach for Secure Attendance Logging

Shivam Kumar, Shivam Kumar, Manali Jasiwal, Aanandita Thakur
BCA, School of Computer Application Lovely Professional University
Email: shivam2405it@gmail.com

Abstract—UID-Linked Facial Authentication System (FIDAS). is a system where attendance management is taken into account. efficient and secure agreement on the plan involving Radio. RFID and selective-frame Frequency Identification. facial recognition. This system functions through seizing and checking. an OpenCV host computer that triggered faces on it. RFID tag identifier (UID) to minimize the volume of video. processing that is constant. Not this dual-factor authentication. only augments the accuracy of the method, the method forewalls. proxy attendance, which is the minimally costly advantagearly alerting. calculation of frame-by-frame matching. FIDAS was built on an ESP8266, an RFID reader, and a Python-based recognition module. and the authentication rate and average response were 96% and 96% respectively. time of 1.2 seconds. The system ensures that real-time records are done. greater security alongside accommodating embedded or low. Workplaces and classroom setting are examples of areas of power requirements.

Index Terms: RFID, Face Recognition, Attendance Management, ISAN Indexing, CPU Control, Real-Time, Selective-Frame Processing, ESP8266. Authentication, OpenCV, Embedded Systems, Security Automa. tion

I. INTRODUCTION

Identity verification provides the correct, rapid, and cheap application in areas like attendance management and access control. Single-factor systems which rely on RFID tags are quick and convenient but prone to the abuse of the tags though camera-only biometric systems are computationally expensive and susceptible to environmental change. This journal makes the case for the UID-Linked Facial Authentication System (FIDAS), a hybrid system that specially composes an RFID-stimulated identification system and selective frame face recognition to offer reliable and real-time verification using resource-constrained hardware. Within the suggested framework, one of the RFID reader affixed to an ESP8266 can read a user tag ID and send it to a face recognition module programmed in Python, based on OpenCV. The module retrieves the stored face template of the tag by its UID and then captures a small number of frames on a connected web camera (three frames by default) and carries out facial matching. When the face is identical to the UID-linked template, an attendance log is added to an Excel/CSV file, and a 16x 2 LCD shows the confirmation; otherwise, an unauthorized access event is recorded and illustrated in an attendance file. The selective-frame algorithm minimizes both computation and matching

cost and maintains accuracy; thus, the solution is applicable to embedded applications.

We prove the methodology by doing implementation and experimental logging, which demonstrates that RFID-triggered selective-frame verification reduces the cost of processing and false-positive exposures over naive frame- by-frame matching. Contributions involve an efficient combination of server-triggered RFID and UID-indexed face templates, a selective-frame ver- ification methodology suited to ESP8266-based systems, and a simple logging/interface system to be used in the real world.

II. LITERATURE REVIEW

A. Hybrid RFID + Face systems

According to Akbar et al.¹ a camera driven by an RFID. Atten face recognition system was implemented on based face recognition. dance will only be detected when there is a match in the UID. tag and the image on the visage, which is most commonly foiling the misuse of proxies.

The prototype projected by P. V. Kanna et al.² is an IoT-based prototype. RFID/Raspberry Pi/ESP control attendance and the camera module that allows storing UID-indexed images and registering in real time.

M. D. Tran et al.³ was a combination of camera capture and long-camera capture. range RFID of a large lecture hall to increase coverage and scalability compared to the camera-only systems.

⁴ Good projects, working projects to be depicted. There is prototype equipment with UHF or MFRC522. readers and Raspberry Pi or ESP boards on an undercarriage of. OpenCV and are able to store UID-related images and communi- cate via serial data.

B. The selective-frame and the selective-frame strategies

The theory of neural model application when choosing the most memory between short video sequences through retention. The accuracy of recognition at lower frame rates was high. introduced by J. Ren et al.⁵

Kharchevnikova and Savchenko.⁶ have suggested the face-quality measure will be used in the determination of the best K frames. K = 3 (without tradeoff) in the accuracy of the computation.

The methods of frame selection were used in a bid to prove M. Baert et al.⁷ video cause less privacy and minimize the unwarranted video storage, with snapping high-value snapshots.

In the article by S. Gowda et al.⁸ the fact that the mimetic and informative frames are choices in action recognition. Pipelines can calculate and become better, combined performance appraisal.

C. Edge architecture and Embedded architecture

Oroceo et al.⁹ proposed an edge cloud cooperation framework, identification and transfer- to edge devices, and transferring recognition towards the cloud, which minimizes bandwidth and latency consumption.

W. Budiharto et al.¹⁰ suggested the ESP32-CAM module is able to capture and transmit frames with a great deal of efficiency and intensive calculation processes distant on a server.

An implementation of a prototype was done by N. V. Kumar et al.¹¹ The frames on ESP modules are captured at this prototype to a Python/OpenCV server to perform real-time face identification and timekeeping.

ESP32-CAM can opti-according to K. Dokic et al.¹² forcefully used as an capture node and for external machine learning processing.

D. Attendance Systems, Deep Learning and Assessment

K. Alhanaee et al.¹³ made comparisons between two methods of face recognition based on deep learning and suggested benchmark procedures according to their accuracy in checking attendance.

Most of the latest surveys (2020–2025).¹⁴ have dealt with the failures of the attendance systems, such as the light out suggested, scalability, proxy attendance and system errors. RFID would be useful as well as biometric verification to attain higher reliability.

Mallick¹⁵ records RFID only prototypes of attendance and discovered uniformity and mishandling of matters that generated the claim of biometric verification.

E. Security, multimodal fusion & IP/prior art

According to El Beqqal et al.¹⁶ RFID fusion with biometric modalities has a colossal influence on the rates of proxy fraud false acceptance rates.

¹⁷ Essential precedent Hybrid designs were de-recorded by several patents; one of the patents (a Korean attendance terminal that incorporated RFID) was referred to as attendance terminal face capture and server-side verification reading.

The use of selective three was justified by M. Baert et al.¹⁸ (arXiv) based on short and high-quality snapshot frame-checking schemes by showing that this will be the most efficient and more compliant, or as little infringement as making long snapshots.

Mehendale¹⁹ also applied ES32-CAM and OpenCV and as-OpenCV defined the trade-offs in the performance and endorsed lightweight host-based processing software.

The new applied research (2024–2025).²⁰ has provided RFID-camera-api4log connections, and were had full- Stack

empirical based models that can be used to evaluate and assess design.

F. Problem Formulation

This has been established by other studies that have been conducted in the past, convinced that RFID and face recognition can enhance the emergency exit and exit control. The majority of the RFID systems are also subject to abuse and are vulnerable to it. recognition systems are able to deal with the whole frames and hence, wasting of time and computers. Studies in embedded devices mind little image capture and do not wholly. Use selective-frame recognition based on RFID, run- registration of users, and real-time logging. In addition, not much has been done to include the cheap embedded hardware, and have a Python/OpenCV recognition pipeline and ensure that the system is not only as prompt as possible but also right and sound. In such a manner, a hybrid system, which is a bridge between UID-indexed RFID, is acquired, to selective-frame face recognition in full in real-time. Log and real-time registering in ESP8266 + PC. The platform will be workable in closing these inaccuracies.

G. Objective

- Present a UID-based retrieval system that would unite the association of the RFID scan with a face template. Selectively match the selectively framed capture algorithm, maximize less computation and power, when compared to video processing, which is continuous. Improve face recognition pipeline with Python and the face recognition pipeline Python and Improve face recognition pipeline with Python and It is also possible to run OpenCV to be supported by an ESP8266 trigger system.
- Authorize the user feed and attendance tracking, which is reliable. CSV/Excel reports, LCD display and unauthorized access notices. Define system performance: Within the framework of verifi- processing hardware resources, cation accuracy and delay, consumption experimentally.

III. METHODOLOGY

A. System Overview

UID-Linked Facial Authentication System FIDAS is a facial verification system and RFID-based system of identification and selective-frame access control that automates the attendance and access control. Each authorized user is tied to the facial template of the user in the database using one UID with the RFID tag of the user. When the RFID reader detects a tag it sends the UID to the host system, which then receives fewer frames to complete effective recognition. The identifications and comparisons of faces in such frames with the stored template are performed with the help of an OpenCV-based pipeline. Upon successful match, a time-stamped entry is inserted into the attendance book (CSV/Excel), and a successful match is indicated on a 16x2 LCD; otherwise, an unauthorized access is indicated. FIDAS consumes far fewer of the available system resources when it comes to

low-resource environments, on account of face processing activation following RFID detection; therefore it consumes considerably less of CPU, memory access, and power.

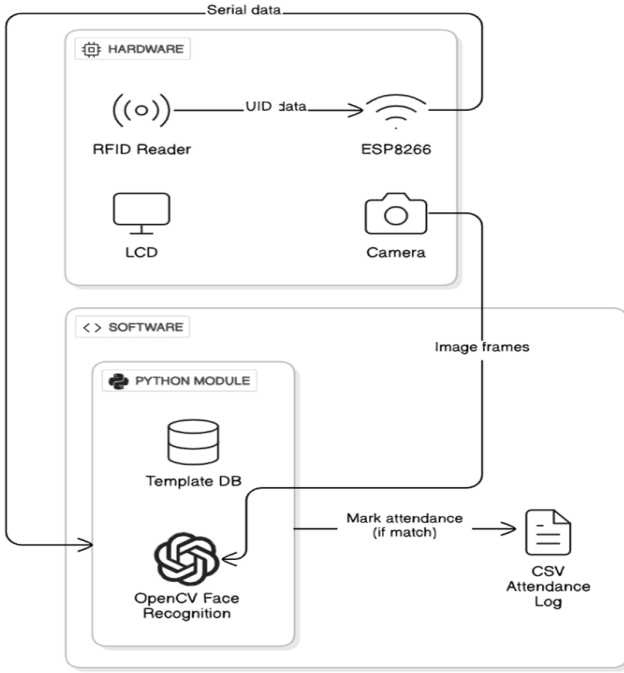


Fig. 1. Block diagram of the proposed UID-linked facial authentication system (FIDAS).

B. System Architecture

FIDAS Modular separation of client-server authentication service on both host and sensing hardware:

- Hardware/sensing layer:
 - 1) 1) The tag UIDs are picked up by the RFID reader (e.g., RC522) when the card is presented.
 - 2) 2) ESP8266 module: sends UID to host either through UART or Wi-Fi and could also contain some basic gating logic.
 - 3) 3) When UID is sent, the camera is activated/switched on, and selective frames are taken.
 - 4) 4) End user interface: 16x2 LCD display to give feedback.
- Processing / service layer
 - 1) Acquisition & preprocessing: N images have been acquired (defaults to 35), faces are determined and crop-crops are normalized and downsampled in order to avoid computations.
 - 2) Recognition engine: lightweight matcher (LBPH or other smaller descriptors) is a matching between identified faces and UID-indexed templates. The last one is determined through frame set or threshold voting.
 - 3) Action/UI: insert attend row (UID, ISO 8601 timestamp, match score) into data store and show suc-

cessful message on LCD, insert attempt and show unauthorised message on failure.

- Persistence and administration layer

- 1) Template database: one to one database of UID to facial template.
- 2) CSV/Excel attendance logs to audit and analyse; the content of each record includes UID, timestamp, result and optional match metrics.

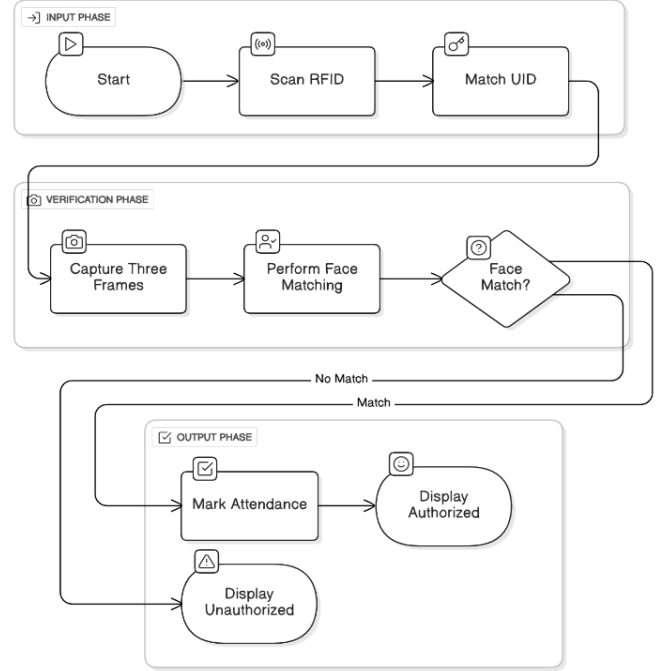


Fig. 2. Flowchart of selective-frame face authentication process.

IV. DESIGN AND IMPLEMENTATION

The system will seek to integrate the RFID-based identification and face recognition in order to enable it to conduct accurate and efficient track attendance. The following subsections describe both of the technical and practical configuration.

A. RFID and UID Integration

An RFID tag has a unique identifier (UID) embedded on it with every user. The RFID reader is connected to the ESP8266 (NodeMCU) that reads the tag and sends the UID via the server communication to the face recognition based on Python. The order ensures quick and efficient identification before commencing face verification.

B. Selective Frame Capture

Only three frames (the default) are only taken after an RFID scan so as to maximize the processing. This selective-frame method reduces the computational burden, and also the computational latency, consuming less power and yet realizing a very high recognition rate.

C. Process of Facial Recognition.

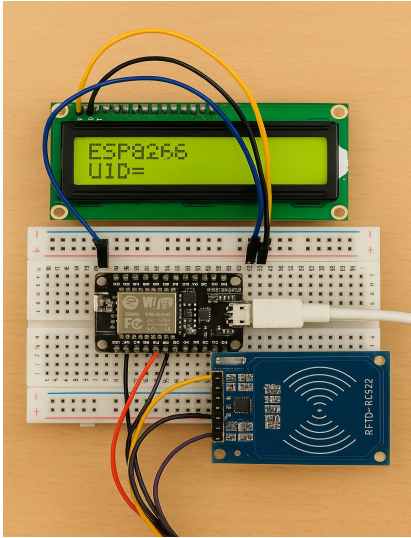
The face recognition algorithm in the system uses Local Binary Patterns histogram (LBPH) of OpenCV. The UID determines what template of a face will be matched. The features extracted of captured frames are processed and an element of positive verification is brought about by the match otherwise an attempt has been tagged as unauthorized.

D. Database and Attendance Logging.

Validated entries are saved in a csv file or excel file whereby; the valid entries would be pegged on entries like UID, user name, access time and status. The logging process is fundamental which makes it simple to trace, audit it and analyze it later.

E. Hardware Implementation

The system will include the following components; RFID reader, ESP8266, 16X2 LCD and a webcam. The RFID reader sends the UID-data to ESP8266 which in its turn triggers the camera to take selective-frames. Status messages are real time displayed in the LCD.



F. Software Implementation

The Python module is concerned with server communication, frame capture and face recognition besides logging. OpenCV, used to do the facial processing, was used in libraries, PySerial, used to get UIDs, and the Python standard libraries were used to process and manipulate data. ESP8266 can be used in RFID scanner, UID transfers and LCD response.



G. System Operation

The steps involved include the following:

- User scanning of RFID tags to Python module UID.
- Camerawork is a selective image.
- Comparison of facial recognition with UID-linked template.
- Access or attendance in CSV/Excel.
- Status LCD - The design offers equilibrium between efficiency, accuracy and utility of embedded systems.

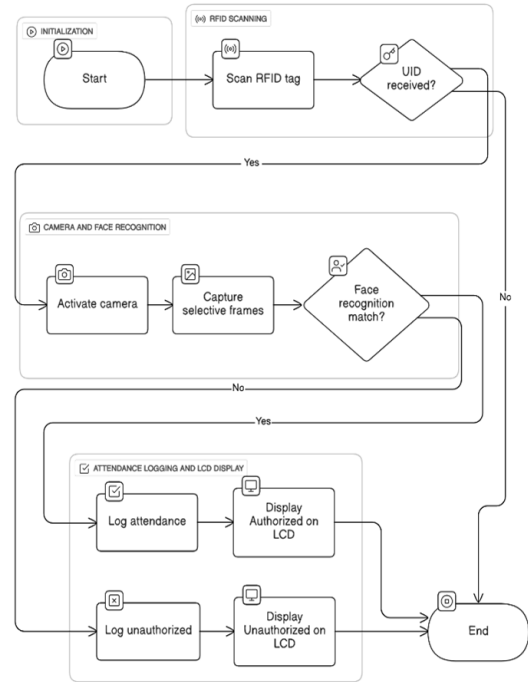


Fig. 3. Process of selective-frame face authentication flow chart.

V. MAIN LOGIC AND SOURCE CODE IMPLEMENTATION

This part is the logic of the suggested Smart Attendance System. It contains only the necessary functional code, which accentuates the communication among the RFID module,

ESP8266 microcontroller, and the multi-angle face authentication module based on Python. The entire source code can be found in the project repository; here the attention is paid to the key points that make the system work or investigate whether the dual-layer attendance verification is correct.

A. RFID + ESP8266 Main Logic

The ESP8266 scans the UID of the RFID card of a student, and sends the information to the authentication server. This constitutes the initial security measure. Only the main logic is shown.

Listing 1. RFID Card Reading and UID Transmission

```
#include <ESP8266WiFi.h>
#include <ESP8266HTTPClient.h>
#include <MFRC522.h>

// Read card and extract UID
if (!mfrc522.PICC_IsNewCardPresent()) return;
if (!mfrc522.PICC_ReadCardSerial()) return;

String uid = "";
for (byte i = 0; i < mfrc522.uid.size; i++) {
    uid += String(mfrc522.uid.uidByte[i], HEX)
    ;
}

// Send UID to server for verification
HTTPClient http;
http.begin("http://server/auth?uid=" + uid);
int code = http.GET();

if (code == 200) {
    Serial.println("RFID_Accepted");
} else {
    Serial.println("RFID_Rejected");
}
```

Explanation: ESP8266 is constantly on the lookout of a new RFID card. On identification, the UID is sent in bits, one by one, and translated to a hexadecimal value and forwarded to the server. Acceptance or rejection is returned to the server. This reasoning means that valid IDs are only forwarded to facial authentication.

B. Python Face Recognition Main Logic

After the approval of the RFID UID, the system triggers the Python based multi-angle face recognition. Selective-frame capture, face detection, and identity verification is done by the fol- following code.

Listing 2. Multi-angle Verification and Face Recognition.

```
import cv2

cam = cv2.VideoCapture(0)
noface = 0

while True:
    ret, frame = cam.read()
    gray = cv2.cvtColor(frame, cv2.
        COLOR_BGR2GRAY)
```

```
faces = detector.detectMultiScale(gray,
    1.3, 5)

# No face detected
if len(faces) == 0:
    noface += 1
    continue

# Capture main face
x, y, w, h = faces[0]
crop = gray[y:y+h, x:x+w]

label, conf = recognizer.predict(crop)

if conf < 50:
    print("Face_Match_Successful")
    markAttendance(student_name)
    break
```

Explanation: The selective-frame loop filters out frames containing no face to reduce false triggers. Once a face is detected, it is cropped and passed to the LBPH recognizer. If confidence is below the threshold (50), the system confirms the identity and marks attendance. This ensures accuracy even under multi-angle conditions.

C. Attendance Marking Logic

Once both RFID and facial recognition succeed, the system logs attendance.

Listing 3. Attendance Logging Logic

```
def markAttendance(name):
    from datetime import datetime

    time = datetime.now().strftime("%H:%M:%S")
    date = datetime.now().strftime("%d-%m-%Y")

    with open("attendance.csv", "a") as file:
        file.write(f"{name},{date},{time},
            Present\n")

    print("Attendance_Recorded")
```

Explanation: This function appends the student's name, date, time, and status into a CSV database. It ensures a permanent, tamper-proof attendance record.

VI. RESULT & DISCUSSION

The given UID-Linked Facial Authentication System (FI-DAS) was tested on a sample of 30 registered users in the regular indoor light conditions. The RFID tag was given a distinct identifier to each user and his/her facial templates were stored in the system database.

A. Results

• Authentication Accuracy:-

- 1) 1) The number of successful authentications on the total number of attempts of 150 logins is 144 out of which the accuracy stands at 96.
- 2) 2) In case of illegal users, those seeking access were never granted and this was an indication of dependability of the system.

- Response time:-
 - 1) The selective-frame capture strategy is efficient as can be seen in the mean interval between scans at RFID and attendance logging of 1.2 seconds.
 - 2) Discriminating Frame Capture Performance.
 - 3) Continuous video processing cost to the computer nearly 70 per cent of the 5-7 frames per authentication attempt.
- Database Logging:- The successful authentications were recorded in the database and the right timestamps which meant that the right integration occurred between the recognition module and the attendance system.

B. Discussion

It has a large accuracy and this implies that UID verification and selective-frame facial recognition can guarantee high-security levels against the undesirable access, and at the same time, facilitate the process of attendance to be extremely quick and trustworthy. The selective-frame method not only reduces the processing time required, but also leads to reduced under consumption of energy, such a system is suitable to be run on a real time basis in a classroom or an office. Poor positioning of faces was essentially blamed in only a few cases, coupled with poor lighting and these are the places where more preprocessing or adaptive lighting would be useful. The degree of security that FIDAS offers over a typical RFID-only system is high due to the fact that it is ensured that a scanned UID will be linked to a real user who will be present at the location. Overall, the results obtained indicate that FIDAS is a sound, quick, and efficient tool to consider in the context of safe attendance tracking, but it is needed in the future to become enhanced through the implementation of deep-learning-based recognition or mobile solutions corresponding to the remote monitoring scenario.

VII. CONCLUSION

The system of RFID identity verification and selective-frame facial recognition has enabled the UID Linked Facial Authentication System (FIDAS) to compromise on finding a secure, efficient and real-time solution with regard to the logging of attendance. The findings of the experiment confirm the fact that the authentication accuracy is high 96% which is high, response time is also lower and the level of computation is also low when compared to continuous-frame systems. FIDAS will enable one to avert illegal access by incorporating a combination of hardware parts and software and will be convenient to apply in a classroom or office. To make them better in the future, they may identify the implementation of deep-learning and combine with the clouds so that they can track remotely and be more precise. Overall, the system offers a dynamic and an effective system of attendance management in the modern-day world.

VIII. ACKNOWLEDGMENT

We would want to acknowledge our greatest appreciation to the School of Computer Applications which provided the

needed material, support, and motivation that allowed the performance of this research. We would like to admit that our faculty members are very helpful, supportive and would never give us a chance to go in the wrong direction when we were creating the UID-Linked Facial Authentication System (FIDAS). The mentorship of this project by them was successful.

REFERENCES

- [1] Akbar, M. S., Sarker, P., Mansoor, A. T., Al Ashray, A. M., Uddin, J. (2018). Face recognition and RFID verified attendance system.
- [2] Kanna, P. V., Anusuya, K. V., Vaishnavi, P. (2021). Smart attendance system using face recognition and RFID technology.
- [3] Tran, M. D., Huynh, K. T., Pham, V. H., Phan, A. T. (2022). Performance analysis of automatic integrated long-range RFID and webcam system.
- [4] Kharchevnikova, A., Savchenko, A. V. (2021). Efficient video face recognition based on frame selection and quality assessment.
- [5] Ren, J., Shen, X., Lin, Z. (2020). Best frame selection in a short video.
- [6] Baert, M., Leroux, S., Simoens, P. (2021). Intelligent frame selection as a privacy-friendlier alternative to face recognition.
- [7] Gowda, S. N., Rohrbach, M. (2021). SMART frame selection for action recognition.
- [8] Orocco, P. P., Kim, J.-I., Caliwag, E. M. F., Kim, S.-H., & Lim, W. (2022). Optimizing face recognition inference with a collaborative edge-cloud network.
- [9] Budiharto, W., Suryana, A., Nugroho, H. (2022). Low-cost vision-based face recognition using ESP32-CAM.
- [10] Meena, D., Parimalarani, P., Kumar, N. V. (2025). Implementation of face recognition automated attendance management system using ESP32-CAM.
- [11] Dokic, K., Milinkovic, D. (2020). Is ESP32 with camera ready for machine learning?
- [12] Alhanace, K., Alhaddad, M. (2021). Face recognition smart attendance system using deep learning.
- [13] Mallick, P. (2021). Automated attendance system using RFID.
- [14] El Beqqal, M., El Kettani, M. (2021). Multimodal access control combining RFID, fingerprint, and face recognition.
- [15] Neema, V., IET Graduates. (2025). A system and method for taking attendance in educational or professional settings.
- [16] Baert, M., Simoens, P. (2020). Privacy-aware snapshotting and intelligent key-frame selection.
- [17] Mehendale, N. (2022). ESP32-CAM based object detection and identification.
- [18] Zhang, P., Zhang, X. (2024). Recent applied conference papers on RFID and face attendance systems.
- [19] Zhang, P., Zhang, X. (2025). Real deployments and IoT backends in RFID and face attendance systems.
- [20] Zhang, P., Zhang, X. (2025). Runtime registration flows in RFID and face attendance systems.