

1 AN RFID-INTEGRATED ATTENDANCE SYSTEM WITH  
2 PHOTO VERIFICATION FOR CLASSROOM EFFICIENCY

3 A Special Problem Proposal  
4 Presented to  
5 the Faculty of the Division of Physical Sciences and Mathematics  
6 College of Arts and Sciences  
7 University of the Philippines Visayas  
8 Miag-ao, Iloilo

9 In Partial Fulfillment  
10 of the Requirements for the Degree of  
11 Bachelor of Science in Computer Science by

12 GALLEGO, Chester Ken  
13 KARIM, John Hamir  
14 MAGTOTO, John Luis

15 Francis DIMZON  
16 Adviser

17 April 28, 2025

## Abstract

19 The UP System started deployment of RFID/NFC-enabled UP ID in 2019. After  
20 several years since deployment, we have yet to see a system that fully utilizes  
21 the technology embedded in the UP ID. In particular, we see a great potential in  
22 using it as an access key for tracking the attendance of students in their classes.  
23 Professors currently either use the traditional pen and paper or a spreadsheet  
24 in their laptops to check for attendance. The mentioned practices are prone to  
25 forgery and takes precious time away from the class period.

26 Our paper proposes a fully digital attendance tracking system that can be  
27 used by professors to record the attendance of their students in real time. The  
28 system uses UP ID and facial recognition for a two-layer validation process ensur-  
29 ing accuracy of the records. Facial recognition uses a pretrained YoloV8 model  
30 for face detection running on the Raspberry Pi AI camera and FaceNet on the  
31 Raspberry Pi CPU. The proposed system allows the students to check in by  
32 tapping their ID to the RFID/NFC reader, and aligning their face in the camera.  
33 The current prototype takes only about 2-3 seconds per student to complete the  
34 whole validation and recording process, with more room for optimizations down  
35 the line.

36 **Keywords:** UP System, RFID, attendance, machine learning, facial  
recognition, YoloV8 model.

# Contents

38	<b>1 Introduction</b>	<b>1</b>
39	1.1 Overview . . . . .	1
40	1.2 Problem Statement . . . . .	2
41	1.3 Research Objectives . . . . .	3
42	1.3.1 General Objective . . . . .	3
43	1.3.2 Specific Objectives . . . . .	3
44	1.4 Scope and Limitations of the Research . . . . .	4
45	1.5 Significance of the Research . . . . .	4
46	<b>2 Review of Related Literature</b>	<b>6</b>
47	2.1 Importance of Attendance Tracking . . . . .	6
48	2.2 Attendance Tracking Methods . . . . .	6
49	2.2.1 Traditional Attendance Tracking Methods . . . . .	7
50	2.2.2 Biometric-Based Attendance Systems . . . . .	7
51	2.3 Chapter Summary . . . . .	9
52	<b>3 Research Methodology</b>	<b>10</b>
53	3.1 Research Activities . . . . .	10

54	3.2	RFID and Face Recognition . . . . .	11
55	3.2.1	RFID as a Token . . . . .	11
56	3.2.2	Face Recognition as a Verifier . . . . .	11
57	3.3	Face Recognition . . . . .	12
58	3.3.1	Face recognition model fine tuning . . . . .	12
59	3.4	Hardware Development Tools . . . . .	12
60	3.5	Software Development Tools . . . . .	13
61	<b>4</b>	<b>System Architecture and Model Evaluation</b>	<b>14</b>
62	4.1	System Architecture . . . . .	14
63	4.2	Process Diagrams . . . . .	15
64	4.2.1	Faculty CSV Import Process . . . . .	15
65	4.2.2	Student Registration Process . . . . .	15
66	4.2.3	Time In Process . . . . .	15
67	4.2.4	Time Out Process . . . . .	16
68	4.2.5	Attendance Record Export Process . . . . .	16
69	4.2.6	Reports Module . . . . .	16
70	4.3	Django Backend . . . . .	16
71	4.3.1	Models . . . . .	16
72	4.3.2	Database Tables . . . . .	17
73	4.3.3	REST API by Django Ninja . . . . .	17
74	4.3.4	Admin panel by Django . . . . .	18
75	4.4	Nuxt Frontend . . . . .	18
76	4.5	MobileFacenet in detail . . . . .	22

77	4.5.1 Model Architecture . . . . .	22
78	4.5.2 Metrics . . . . .	23
79	4.6 YoloV8n for Face Detection . . . . .	24
80	<b>5 Summary, Conclusions, and Recommendations</b>	<b>25</b>
81	5.1 Summary . . . . .	25
82	5.2 Conclusion . . . . .	25
83	5.3 Recommendation . . . . .	25
84	<b>References</b>	<b>27</b>
85	<b>A Appendix Title</b>	<b>29</b>
86	<b>B Resource Persons</b>	<b>30</b>

# 87 List of Figures

88	4.1 System Architecture . . . . .	14
89	4.2 Time in . . . . .	15
90	4.3 Time Out . . . . .	16
91	4.4 Student model . . . . .	17
92	4.5 Database Tables . . . . .	18
93	4.6 API Documentation . . . . .	19
94	4.7 Django Administration . . . . .	20
95	4.8 Time in and Time out Page . . . . .	20
96	4.9 Successful Time In . . . . .	21
97	4.10 Django saving the attendance time instance in 24-hr format . . .	21
98	4.11 Fake Delay . . . . .	21
99	4.12 MobileFaceNet . . . . .	22
100	4.13 ROC AUC . . . . .	23
101	4.14 ROC AUC . . . . .	24

# 102 List of Tables

<small>103</small>	2.1 Comparison of Attendance Tracking Methods Using the CIA Triad	9
--------------------	---	---

# Chapter 1

## Introduction

### 1.1 Overview

Attendance plays an important role in improving the academic performance of students. There is evidence that students with lower attendance often have lower grades (Ancheta, Daniel, & Ahmad, 2021). Therefore, attendance is usually enforced and recorded at most higher education institutions. However, the systems in place for recording attendance are typically manual and time-consuming.

The traditional pen and paper attendance system has existed since the invention of paper itself. It is used for time keeping by manually writing or checking the “present” status in a paper log book. Manually writing names takes an average of 17 seconds per student (Shoewu, Makanjuola, & Olatinwo, 2014), and for class size of 30 students that leads to approximately 8 minutes of class time wasted. While it is recognized that such system is time-consuming and wastes resources, it persisted because of its familiarity. Going to class means bringing pen and paper for most students and teachers alike, so using the same material for recording attendance seemed the most practical.

In recent years, as laptops and portable computers became more accessible, some faculty of UP started transitioning to digital spreadsheets provided by services like Microsoft Excel. While it seemed to have moved the traditional pen and paper towards digitalization, another problem arises as this required manually roll calling students to say “present”. It had the same problem of being a manual process. It is easily disrupted by a noisy class. Some time that was supposed to be utilized for immediate teaching was used for roll call.



Both systems mentioned are prone to errors and unnecessarily increases administrative burden for the faculty. Reduction in teaching time means frequently moving the lesson discussions by the faculty, with some topics being rushed or skip entirely by the end of semester. This reduces overall the quality of education students received and may negatively impact their readiness for subsequent courses they may take.

It is also useful to analyze the traditional attendance methods from the lens of CIA triad since we are dealing with information security. It is a guiding model comprised of 3 key principles: Confidentiality - the protection of data from unauthorized access. Integrity - prevent that data from tampering. Availability - data is present whenever you need them (Cawthra et al., 2020). The traditional pen and paper violates confidentiality as there no strict restrictions on who accesses the paper for keeping the attendance data. As a consequence, integrity is also violated as anyone with a pen can easily modify attendance records. Availability also cannot be ensured since paper as a storage medium is easily destructible via wear or tear. Replacing paper with digital counterparts such as Microsoft Excel might address these violations, although indirectly. Teachers put passwords on their laptops, but no authentication is done for the Excel file itself unless it is explicitly encrypted. The file is also prone to accidental deletion.

Therefore, we propose a fully automatic, digital attendance system that addresses these concerns. We utilize the already distributed UP ID and pretrained face recognition models that ensures an easy, accurate, attendance keeping. It aims to ease the burden of faculty and students from manual methods of attendance system, allowing them to focus on class discussions instead.

## 1.2 Problem Statement

The current methods of taking attendance today such as the manual call roll, biometrics, and online or remote attendance provides challenges in terms of efficiency, security, and authenticity. Manual roll calls are time consuming, according to (Mahato & Suman, 2013, p. 5875), it consumes an average of 5 to 15 minutes in order to complete an attendance using manual roll call attendance. It also provides a burden to some of the teachers through the disruptive behaviors of the students which lower the efficiency of manual roll call ("How Teachers Can Meet the Challenges," 2015). Biometrics attendance systems like fingerprint and facial scanning provide efficiency in taking an attendance but it is more costly and widely not accessible. The online or remote attendance system is only advisable in virtual class and not in face to face class as it is prone to attendance fraud.

164 Failure to resolve efficiency and a secured attendance system may lead to  
165 inaccurate attendance records and high risks of attendance fraud. These gaps  
166 may also affect the integrity in terms of attendance of the university. To fill  
167 those gaps, the solution should be the integration of RFID and facial recognition  
168 technology but there are uncertainties which are the efficient ways to integrate  
169 the real-time face capture while managing the privacy concerns and also finding  
170 an optimal way to gather sensitive information which are the student's biometric  
171 and their RFID serial number.

172 Given the gaps of the current attendance system method, there is a need to  
173 design an attendance system with the integration of RFID and facial recognition  
174 technology which are:

- 175 1. Efficiently captures the real-time data using the RFID and facial recognition  
176 technology.
- 177 2. Ensure and maintain security and privacy of the student's sensitive data  
178 such as their facial biometrics and unique serial number of their RFID.
- 179 3. Ensure compatibility with the university infrastructure which is the avail-  
180 ability of RFID and the hardware for facial scanning.
- 181 4. Determine the effectiveness of the combination of the RFID and facial tech-  
182 nology in the attendance system.

## 183 **1.3 Research Objectives**

### 184 **1.3.1 General Objective**

185 This project aims to develop a web application that effectively uses the current UP  
186 RFID and face recognition for attendance checking and recording in the University  
187 of the Philippines Visayas. Additionally, it also aims to assess the performance of  
188 the application in terms of accuracy and efficiency.

### 189 **1.3.2 Specific Objectives**

- 190 1. To develop a full stack web application that uses an RFID scanner and  
191 facial recognition models for an accurate and efficient tracking of student  
192 attendance.

- 193      2. To enhance application security by implementing the principles of Confiden-  
194      tiality, Integrity, and Availability.
- 195      3. To analyze the application's performance based on metrics such as accuracy,  
196      efficiency and security.

## 197    1.4    Scope and Limitations of the Research

198    The focus of this project is to create an attendance system that uses RFID together  
199    with facial technology. This project takes real time attendance by scanning the  
200    student's RFID and verify the student's identity using facial technology. It also  
201    focuses on the User Experience part where students can take their attendance as  
202    quickly as possible by aligning their faces while they scan their RFIDs. In that way  
203    this approach enhances the overall efficiency and accuracy of taking attendance  
204    in the university.

205      This project does not involve the training of face recognition models, as there  
206    are high-performance, pretrained models readily available. Instead, it utilizes  
207    these existing face recognition models for the development of an effective atten-  
208    dance tracking system. This project will only limit face to face classes and does  
209    not cover the virtual or online classes, it will also not cover the other forms of  
210    biometric authentication such as fingerprint and eyes (iris scanning) because of  
211    its expensive hardware and the privacy concerns of the students.

## 212    1.5    Significance of the Research

213    Facial recognition has been in use mobile applications for validation of identity  
214    and the performance has significantly improved over the years. This allowed us to  
215    explore the possibility of using it in attendance tracking of students in UP Visayas  
216    as there are currently no system like it in place. We also intend for this project to  
217    be open-source. Some of the people that will benefit from our developed app are:

- 218      • Students - will benefit from the increased class time. This allow better  
219      retention of topics and lesson discussions. This complements the goal of  
220      recording attendance itself, which is to increase the quality of education the  
221      students receive.

222     • Faculty - will also benefit from the increased class time. An automated  
223       system will allow them to focus entirely on delivering the topics that need  
224       to be covered. It will lessen the possibility of skipping modules or topics  
225       needed by students to learn before taking their subsequent courses.

226     • UP System - Since the UP RFID are used across all constituent units of the  
227       UP System, our project can be used by any faculty under the UP System.  
228       They may also choose to create their own version as long as they also make  
229       it open source, as stipulated in GNU GPLv3 license.

230     • Society benefits - this project is significant in our society. The project is  
231       scalable and when it is improve more in the future, there is a high possibil-  
232       ity that it can be applicable not only to tertiary, higher or in any education  
233       but also it will be applicable to large organizations or corporations as it can  
234       improve taking attendance plus it can reduce the fraud in taking attendance  
235       because one of the gaps to be filled by this project is the integrity, the com-  
236       bination of RFID and the real-time face capture can help the organizations  
237       to have integrity in terms attendance.

238       We also hope that this project will bring focus on the growing accessibility  
239       of facial recognition technologies and inspire the community to explore on how it  
240       can be incorporated their own projects.

## Chapter 2

# Review of Related Literature

### 2.1 Importance of Attendance Tracking

Attendance has become increasingly important in every organization, institution, and workplace to ensure accountability, productivity, and engagement. For example, in schools, it ensures that students are present, participating, and fulfilling their responsibilities. Taking students' attendance is important for monitoring their performance in class. Good attendance is usually linked to good class performance, and vice versa (Zhi, Ibrahim, & Aris, 2014). Additionally, (Romero & Lee, 2007) suggest that attendance is important to reduce the cases of absenteeism in terms of academic performance as mostly, attendance is now part of the grades, motivating the students to attend classes.

### 2.2 Attendance Tracking Methods

There are various methods to track classroom attendance, from traditional manual approaches, such as roll call or pen-and-paper methods, to modern technology-based systems, including biometric like fingerprint or facial recognition. The advantages and disadvantages of these systems will be discussed in the following subsections using the Confidentiality, Integrity, and Availability (CIA) Triad.

The CIA Triad is a commonly used information security model that helps organizations develop secure systems (Fruhlinger, 2024). Confidentiality refers to the protection of information from unauthorized access to ensure that only authorized users can access or modify data. Integrity ensures that data remains

complete, trustworthy, and unaltered by unauthorized users, whether accidentally or maliciously. Availability ensures that authorized users can access the data when needed. These three principles are often used to identify vulnerabilities in a system.

### 2.2.1 Traditional Attendance Tracking Methods

The traditional method of taking attendance is through a manual roll call. According to Uniyal (2022), using manual attendance is cost-effective, simple to use, and remains functional during power interruptions. However, despite these advantages, manual attendance has several flaws. For instance, the roll call method is time-consuming as it can waste 5 to 15 minutes of class time which could otherwise be spent on actual learning (Mahato & Suman, 2013, p. 5875). Additionally, there is a problem in integrity when ledger sheets are used as it is easy for students to fake another student's attendance by forging their name and signature or erasing an already marked attendance. Furthermore, according to (Dewa & Nyanga, 2020), traditional attendance tracking method which is the ledger sheets are not friendly to our environment as there are some cases where excessive use of paper occurs but mostly their study highlighted that switching to another attendance system, especially to digital can reduce paper consumption while achieving more efficient way of taking attendance.

CIA Triad Analysis:

- Confidentiality: Traditional attendance tracking methods may offer low confidentiality as attendance can easily be accessed by unauthorized individuals, especially with the pen-and-paper method.
- Integrity: Traditional attendance tracking methods have low integrity as it is easy for students to forge another student's attendance or alter existing records.
- Availability: Traditional attendance tracking methods have high availability as attendance can always be taken during class, regardless of technological failures.

### 2.2.2 Biometric-Based Attendance Systems

Biometric systems such as fingerprint recognition have addressed some of the shortcomings of manual attendance methods. According to Walia & Jain (2016),

295 replacing traditional attendance methods with biometric fingerprint systems im-  
296 proves confidentiality and integrity. However, while biometric fingerprint atten-  
297 dance systems have high reliability, they still come with some limitations (Truein,  
298 2024). For example, if a person’s finger is injured or dirty, the system may fail  
299 to recognize the fingerprint which can affect the system’s effectiveness. Moreover,  
300 the cost of deployment can be high due to the need for specialized hardware and  
301 maintenance.

302 CIA Triad Analysis:

- 303 • Confidentiality: Biometric systems provide better confidentiality compared  
304 to manual methods as biometric data is unique to each individual and stored  
305 securely. However, if the data is compromised, the consequences can be  
306 severe because biometric data cannot be changed, unlike passwords.
- 307 • Integrity: Biometric systems provide high integrity as it is almost impossible  
308 to forge or alter fingerprint data.
- 309 • Availability: While biometric systems are generally available, they may face  
310 limitations if the finger is injured or dirty or in areas with an unreliable  
311 power supply.

312 Facial recognition technology has emerged as an even more accurate and con-  
313 venient alternative to fingerprint systems (Truein, 2024). According to Yang &  
314 Han (2020), real-time video processing in facial recognition systems has an accu-  
315 racy rate of about 82%, which is higher than other attendance tracking methods.  
316 Facial recognition can also help reduce truancy rates by identifying students in  
317 real time in order to prevent them from skipping classes.

318 CIA Triad Analysis:

- 319 • Confidentiality: Facial recognition systems, like fingerprint systems, have  
320 high confidentiality as biometric data is unique to each individual and stored  
321 securely.
- 322 • Integrity: The integrity of facial recognition systems is typically high as it  
323 is difficult for students to falsify their identity without being detected.
- 324 • Availability: Facial recognition systems are generally highly available, par-  
325 ticularly in environments with stable lighting conditions.

## 2.3 Chapter Summary

This chapter discussed various classroom attendance tracking methods and analyzed their advantages and disadvantages using the CIA Triad. Traditional manual systems, while cost-effective, lack both confidentiality and integrity. Fingerprint systems offer better security but may suffer from availability issues when the finger is dirty or injured. Facial recognition systems, with higher accuracy and efficiency, provide significant improvements in terms of data confidentiality and integrity.

A table comparing these systems, based on the CIA Triad, is provided below:

Attendance Tracking Method	Confidentiality	Integrity	Availability
Traditional	Low	Low	High
Fingerprint Systems	High	High	Medium
Facial Recognition Systems	High	High	High

Table 2.1: Comparison of Attendance Tracking Methods Using the CIA Triad

Our proposed system aims to leverage the security advantages of Facial Recognition Systems by adding an extra layer of user authentication that requires students to use their UP RFID which is personal and unique to each student.



## Chapter 3

# Research Methodology

This chapter lists and discusses the specific steps and activities that will be performed to accomplish the project. The discussion covers the activities from pre-proposal to Final SP Writing.

### 3.1 Research Activities

This project aimed to create an automated attendance system with the help of RFID together with facial recognition technology. This attendance system will replace and reduce the usage of manual attendance such as the written and oral and enhance its lacking optimized features such as security, reliability, authenticity, and integrity using the student's RFID and facial biometric.

The proposed system is expected to function by tapping the RFID of the students with real time facial capture through face recognition technology. The identity of the students will be verified through the unique serial number of their RFID that will match from the system database while the face recognition will serve as the two-factor authentication. The face recognition is expected to work by capturing the students face then will be matched also through the system database. The attendance will only be valid once both student's unique serial number in their RFID and their face has been verified.

To make the system functional, several data from the students need to be collected. Those are the student's name, student number, student's unique serial number of their RFID, and their facial biometrics. Those data will be gathered either online or face to face. Students are encouraged to download any of the RFID

360 card readers to know their RFID's serial number but in case they are incapable of  
361 doing that. Face to face to face will be an option where we can provide a physical  
362 RFID card reader. The facial recognition data will be gathered through capturing  
363 their image or video to be more accurate.

364 The hardware components will be using in this system are: RFID scanner:  
365 Which will be used to read the RFID given to the students. This will also be  
366 responsible for taking the students unique serial number on their RFID ensuring  
367 the integrity of the students. USB connector: This will be used to connect the  
368 RFID scanner to the Laptop or Raspberry Pi. Flex cable: This will be used to  
369 connect the Raspberry Pi Vision Camera to Raspberry Pi. Laptop / Raspberry  
370 Pi: This will serve as the main processing unit. The laptop or raspberry pi will be  
371 used for running the required algorithm to make the face recognition and read the  
372 RFID correctly. Overall, the laptop / raspberry pi will be in charge of handling  
373 the data. Raspberry Pi Vision Camera: In charge of capturing the student's facial  
374 image while scanning the RFID to the RFID scanner.

## 375 **3.2 RFID and Face Recognition**

376 We use the UP RFID for our system. This approach enhances security by com-  
377 bining something you have (the RFID token) with something you are (your face).

### 378 **3.2.1 RFID as a Token**

379 The RFID token (the UP RFID) provides a unique identifier (ID) for the user.  
380 The RFID reader scans the token and extracts the unique ID. This ID is used to  
381 retrieve the corresponding user profile from a database.

### 382 **3.2.2 Face Recognition as a Verifier**

383 Face recognition ensures that the person presenting the RFID token is the autho-  
384 rized user associated with that token.

### 3.3 Face Recognition

Face recognition pipeline can be simplified into 2 steps:

1. Face Detection: The process of finding the faces in a viewfinder and draw bounding boxes around the detected face. We will use a pretrained YOLOv8n model as the base model for face detection. We will feed the resulting cropped image into the face recognition model. It will run on the IMX500 chip in the Raspberry Pi AI Camera for inference, freeing the CPU for other task (Sony, 2023). As on now, only YoloV8 officially supports exporting their model to the Rasperberry Pi AI camera(Ultralytics, 2024). For this to work seamlessly, it is recommended to avoid low-light conditions. According to Zhou (2025), images captured in low-light conditions tend to be of poor quality, are easily disrupted by background noise, and suffer loss of detail, which lowers the accuracy of facial verification in the next step.
2. Face verification: The task of comparing 2 faces and checking if they are of the same identity. The model we chose for this is MobileFaceNet which is a face recognition model optimized for mobile and embedded devices like the Raspberry Pi(Chen, Liu, Gao, & Han, 2018).

#### 3.3.1 Face recognition model fine tuning

The pretrained MobileFaceNet we chose is under the Apache 2.0 license. The model size is about 800kb by user Jason Wong on Kaggle which was trained on MS1M-ArcFace with 85k unique identities and 5.7 million images.

### 3.4 Hardware Development Tools

Our current prototype uses hardware components that are commonly used in the industry to build an integrated system. All of the tools are readily available. These include but are not limited to:

- RFID Scanner - Used as a reader for the RFID. The RFID scanner allows us to have secured and efficient way of identifying the student's unique serial number.

- 413 • Raspberry Pi AI Camera - The newly released camera module for Rasp-  
414 berry Pi hardware that allows us to capture the student's facial image while  
415 scanning the RFID with the use of RFID scanner. It uses an embedded AI  
416 accelerator for efficient processing of face data.
- 417 • Raspberry Pi - Serves as the main processing unit which allows us to inte-  
418 grate the other hardware together with the necessary software.
- 419 • USB Connector - Serves as connector for the RFID scanner and Raspberry  
420 Pi.
- 421 • Flex Cable - Serves as connector for the Raspberry Pi Vision Camera and  
422 Raspberry Pi.

## 423 3.5 Software Development Tools

424 Our current prototype include these frameworks and tools that are heavily used  
425 in the industry for rapid development and deployment of web applications. All of  
426 the tools used are open source. These include but are not limited to:

- 427 • Django - The web framework for perfectionists with deadlines. Django,  
428 which serves as the backend server, allows us to interface with the database  
429 server to do queries in the Python using Django's Object Relational Mapping  
430 tool(ORM). We can easily integrate popular pretrained facial recognition  
431 models as they are typically written in Python.
- 432 • Django Ninja - Creates the REST API on top of our Django backend to  
433 allow the frontend to consume the backend content.
- 434 • NuxtJS - The frontend JavaScript framework used to build our web interface.  
435 Includes all the tools for routing, quering, and security. By default, it renders  
436 our web interface in Server Side Rendering(SSR) mode. Most of the work  
437 happens in the server and no authentication tokens are stored in the client  
438 browser. This increases security since authentication tokens are only added  
439 in the server side per request.

## Chapter 4

# System Architecture and Model Evaluation

## 4.1 System Architecture

Using the tools mentioned in Section 3.5, our system can be visualized as shown in Figure 4.1:

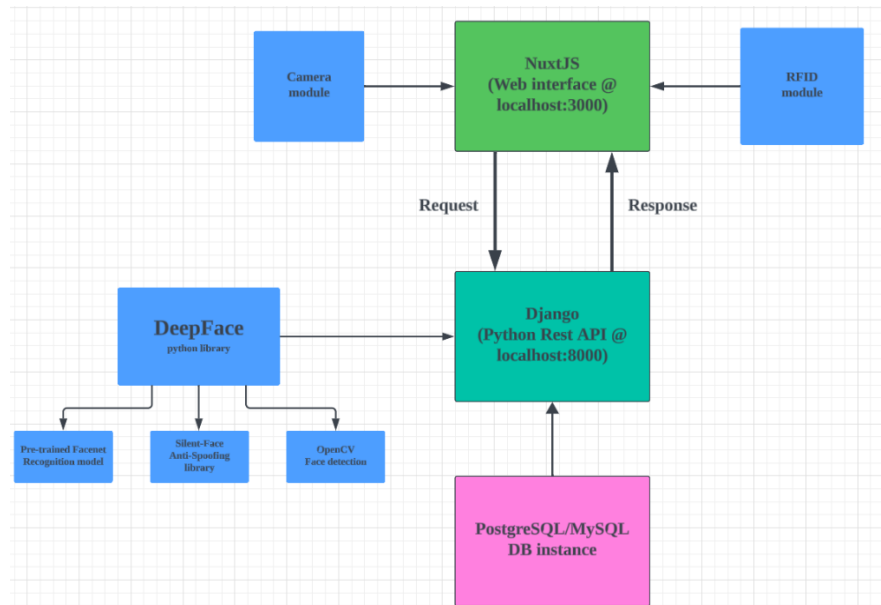


Figure 4.1: System Architecture

446 Currently, we use the DeepFace library for face recognition as a temporary  
 447 measure to test our system while our own face recognition model is in the works.

## 448 4.2 Process Diagrams

### 449 4.2.1 Faculty CSV Import Process

450 To make the registration of the students much easier for the faculty, the faculty  
 451 members can upload a CSV file containing the students' required details. The  
 452 system parses the CSV file and stores the extracted data in the database. The  
 453 data uploaded is validated to avoid any duplicate or wrong entries.

### 454 4.2.2 Student Registration Process

455 Students must register their facial ID to enable attendance verification. This reg-  
 456 istration process only captures one facial image, which will be used to iden-  
 457 tify the student during attendance tracking.

### 458 4.2.3 Time In Process

459 Time in process includes a check if the student already has time in records. First  
 460 step in this is the student tapping the ID to the RFID sensor and trigger the  
 photo capture to check the face.

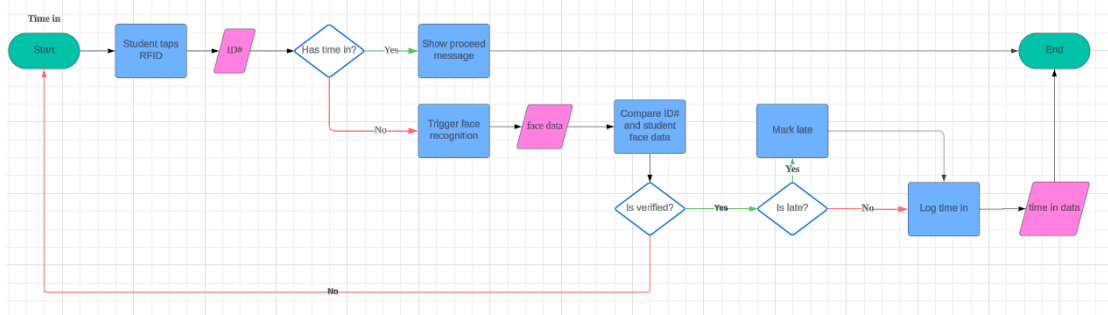


Figure 4.2: Time in

#### 4.2.4 Time Out Process

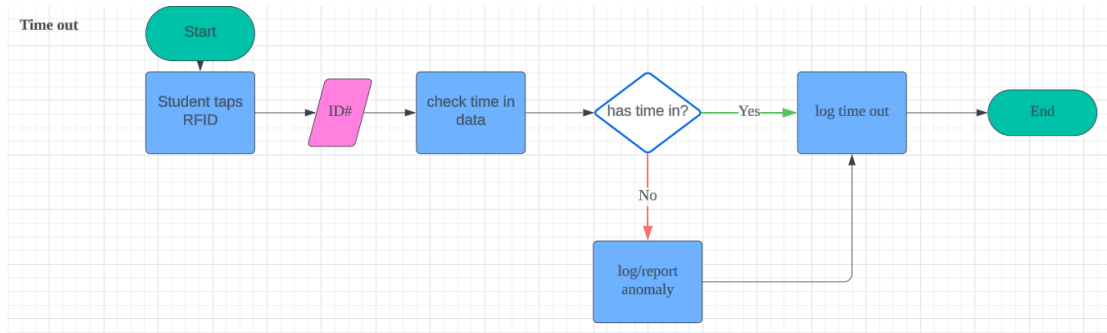


Figure 4.3: Time Out

#### 4.2.5 Attendance Record Export Process

The faculty members are allowed to export their attendance records into a CSV file in order to have better access and record keeping. In addition to that, this feature can be useful for further analysis, for data backup purposes, or if they want to integrate it into another academic system.

#### 4.2.6 Reports Module

The system includes a Reports Module that allows faculty to generate attendance reports in PDF or CSV file.

### 4.3 Django Backend

#### 4.3.1 Models

Django Model class maps to SQL tables. For example, a Student table will have the following columns which maps to Student Model class' attributes like in Figure 4.4:

SQL equivalent would be:

```

class Student(models.Model):
    student_id = models.IntegerField(primary_key=True)
    first_name = models.CharField(max_length=100, default='')
    last_name = models.CharField(max_length=100, default='')
    email = models.EmailField(null=True)
    face_data = models.TextField(null=True)

    Codeium: Refactor | Explain | Generate Docstring | ✕
    def full_name(self):
        | return f'{self.first_name} {self.last_name}'
    Codeium: Refactor | Explain | Generate Docstring | ✕
    def __str__(self):
        | return self.full_name()

```

Figure 4.4: Student model

```

477 CREATE TABLE Student (
478     student_id INTEGER PRIMARY KEY,
479     first_name VARCHAR(100) NOT NULL DEFAULT '',
480     last_name VARCHAR(100) NOT NULL DEFAULT '',
481     email VARCHAR(254),
482     face_data TEXT,
483     CONSTRAINT unique_email UNIQUE (email)
484 );
485

```

### 4.3.2 Database Tables

Our database tables that can be accessed by Django's ORM. This includes the tables for Teachers, Subjects and tables for relationships. See Figure 4.5

### 4.3.3 REST API by Django Ninja

Figure 4.6 is the automatic OpenAPI compliant documentation provided by Django Ninja. It contains all endpoints we can use to query data from the database. All endpoints are protected using HTTP Bearer token authentication.



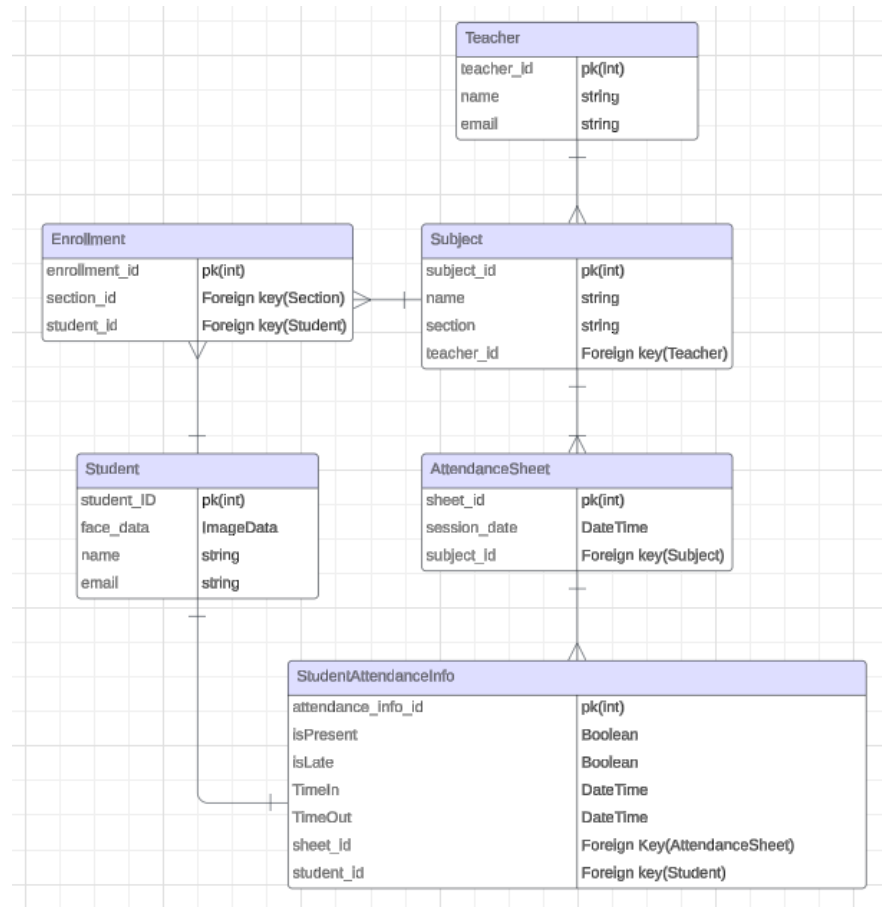


Figure 4.5: Database Tables

#### 4.3.4 Admin panel by Django

Figure 4.7 is the Django administration page only accessible to a superuser account. This is where most of the backend maintenance work happens. It contains all the data inside the database allow full control over them. It also contains every authentication tokens used by each teacher account.

## 4.4 Nuxt Frontend

With the backend handling most of the heavy work, the frontend only needs to capture images from the camera and sending them to the backend to verify student identity. The localhost:3000/dashboard/time-in-out page handles the time in and time out process. The RFID input is automatically highlighted upon opening

Authorize

Teachers API			^
GET	/api/teachers/subjects	Get Subjects	🔒
Attendance API			^
POST	/api/attendance/time-in	Save Time In	🔒
POST	/api/attendance/time-out	Save Time Out	🔒
GET	/api/attendance/recent	Get Recent Attendance	🔒
Student API			^
POST	/api/student/register	Register Student	🔒
GET	/api/student/all	Get All Students	🔒
DELETE	/api/student/{student_id}	Delete Student	🔒

Figure 4.6: API Documentation

503 the page so it will be immediately ready to take in input from the RFID scanner.  
504 When the proper number length is inputted, it will immediately start to verify the  
505 identity. It will then notify the student for the time in/time out time and status.  
506 It will also notify for any errors like spoof image or no face detected. From our  
507 testing, the response time is currently at most 2.3 seconds, most of the delay  
508 comes from the fake delay we used to allow the student to read the notification  
509 after verification.

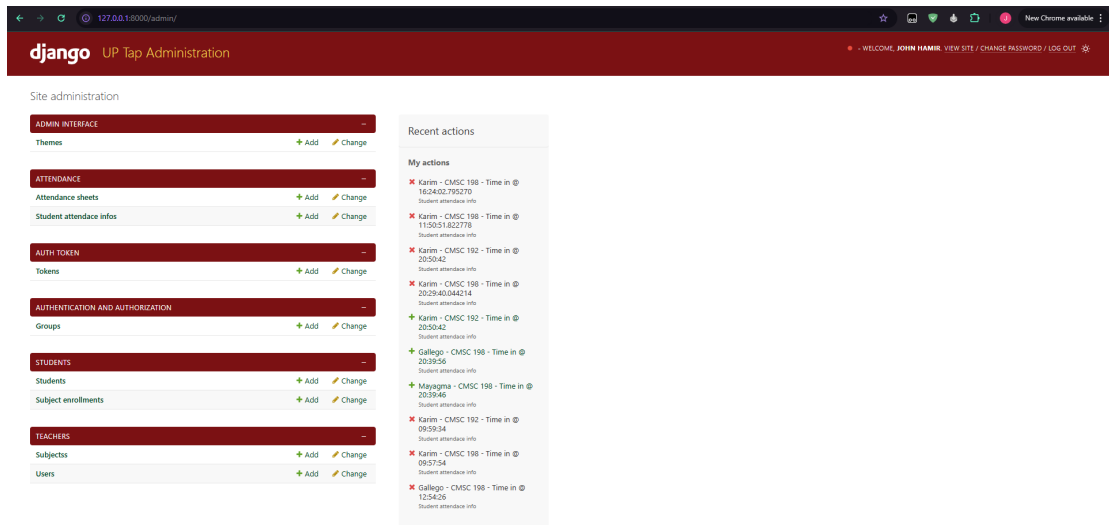


Figure 4.7: Django Administration

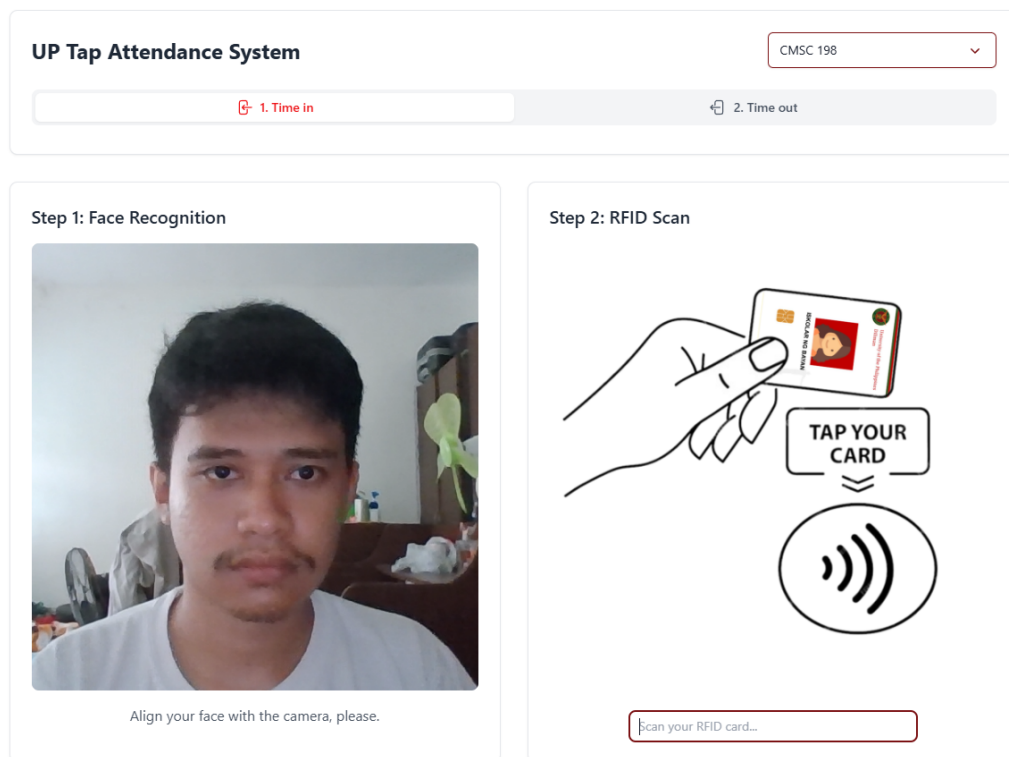


Figure 4.8: Time in and Time out Page

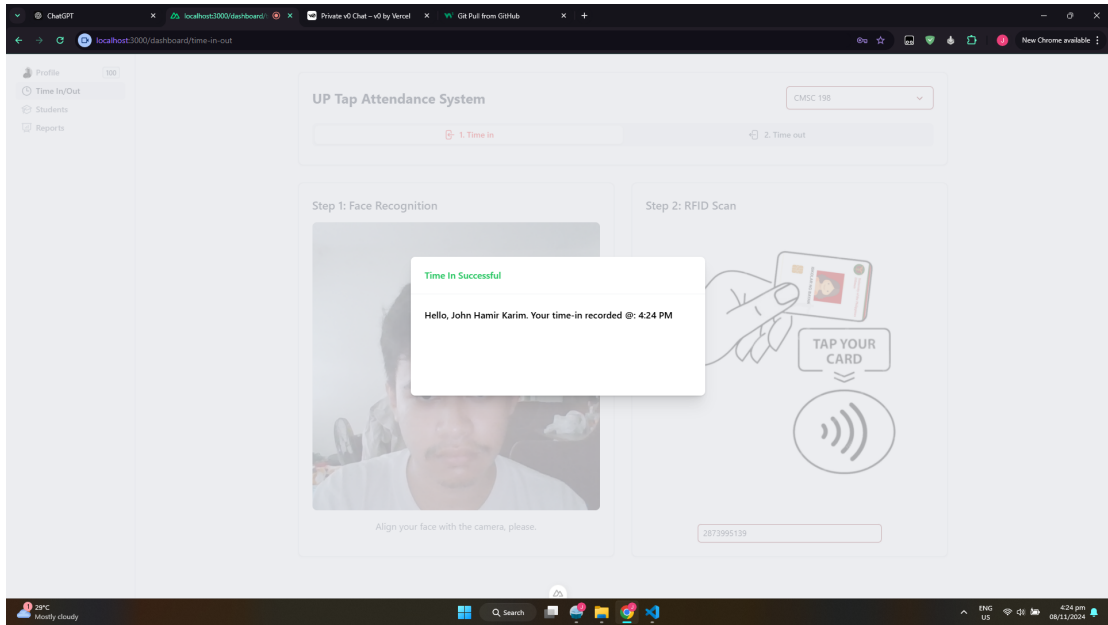


Figure 4.9: Successful Time In

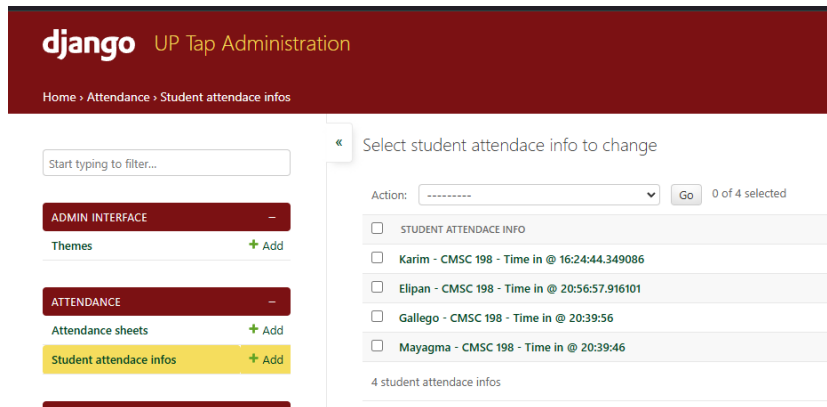


Figure 4.10: Django saving the attendance time instance in 24-hr format

```

if(time_in){
  openModal(time_in)
  // 2 second countdown
  setTimeout(() => {
    closeModal()
  }, 2000);
  setTimeout(() => {
    rfidRef.value.$refs.input.focus()
  }, 2300)
}

```

Figure 4.11: Fake Delay

## 4.5 MobileFacenet in detail

The MobileFacenet model for was used face verification. The model takes in a 112x112x3 image and outputs an embedding(a mathematical representation of face). We then use Cosine similarity with a certain threshold to compute if two embeddings are similar, therefore concluding that both identities are the same. The model was converted to a Tensorflowlite model to run faster on the Raspberry Pi 5 hardware. The final size of the model is 863Kb.

### 4.5.1 Model Architecture

Figure 4.12 Shows the general architecture of the model as defined in the MobileFacenet paper (Chen et al., 2018).

Input	Operator	$t$	$c$	$n$	$s$
$112^2 \times 3$	conv3x3	-	64	1	2
$56^2 \times 64$	depthwise conv3x3	-	64	1	1
$56^2 \times 64$	bottleneck	2	64	5	2
$28^2 \times 64$	bottleneck	4	128	1	2
$14^2 \times 128$	bottleneck	2	128	6	1
$14^2 \times 128$	bottleneck	4	128	1	2
$7^2 \times 128$	bottleneck	2	128	2	1
$7^2 \times 128$	conv1x1	-	512	1	1
$7^2 \times 512$	linear GDConv7x7	-	512	1	1
$1^2 \times 512$	linear conv1x1	-	128	1	1

Figure 4.12: MobileFaceNet

## 4.5.2 Metrics

We tested the accuracy of the model using the Labeled Faces in the Wild (LFW) Dataset via sklearn. The dataset includes 13,233 images of 5,749 people. The sklearn package provides a 300 pairs of same + 300 pairs of different people per fold. We tested the model in 10 folds. Compared to models of hundreds of MB in size, the performance of the model is good but can be better. An AUC of 0.77 means that if we pick one genuine (same-person) pair and one impostor (different-person) pair at random, there's a 77% chance the model will score the genuine pair higher.

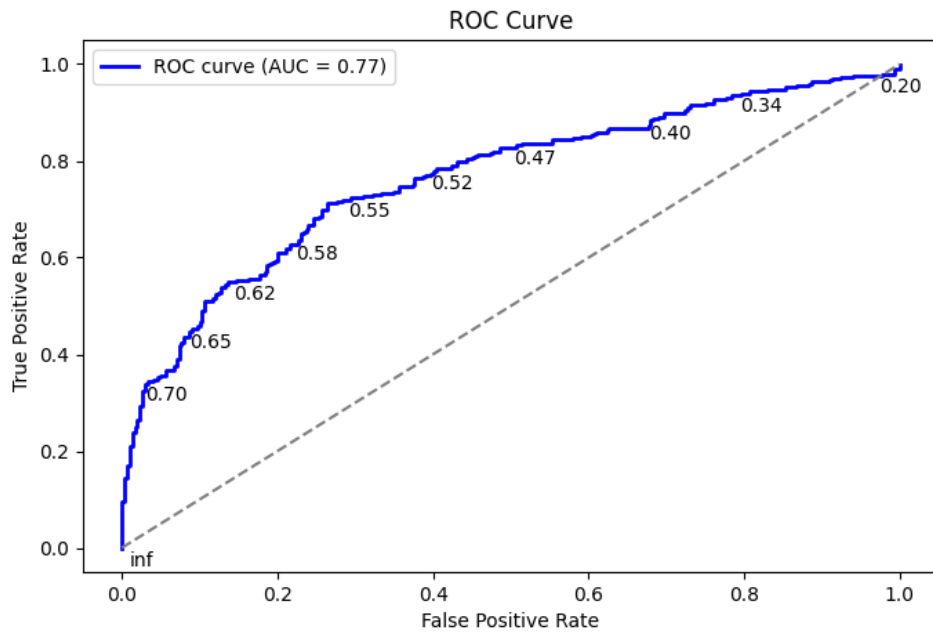


Figure 4.13: ROC AUC

529      Next we check the overall accuracy at the chosen threshold. We chose the 0.6  
 530 as threshold for a good balance of security and reliability. The threshold posted  
 531 an average accuracy score of 68.6% on all ten folds. While not impressive, note  
 532 that the model we test here is a TensorFlow Lite version which was compressed  
 for faster inference on RPI 5.

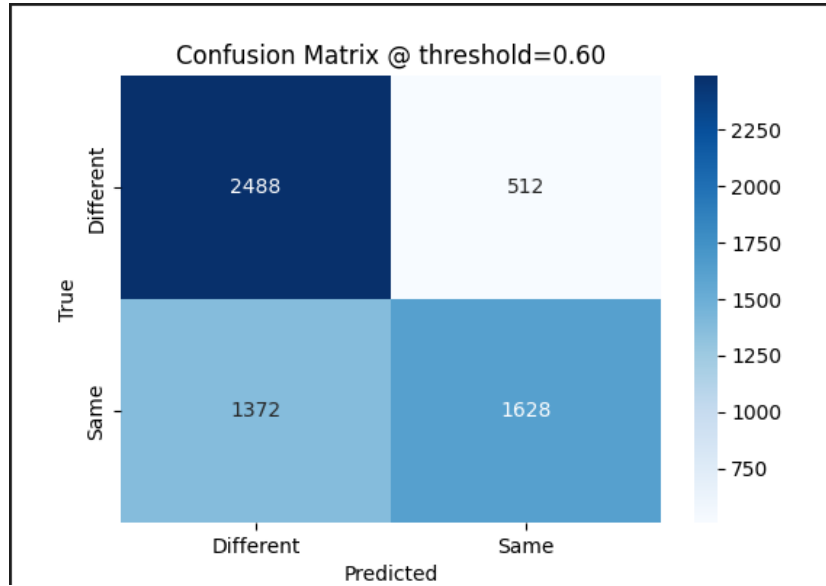


Figure 4.14: ROC AUC

533

## 534    4.6    YoloV8n for Face Detection

535    We used a pretrained YoloV8n model for face detection by Arnab Dhar on Hug-  
 536 gingface. The main motivation was because Yolo models were the first to officially  
 537 support exporting and deploying a model to the Raspberry Pi AI Camera. The  
 538 Ultralytics team abstracted the process of model quantization and compression  
 539 using Sony’s Model Compression Toolkit into their Python library. Compression  
 540 and quantization was required as the IMX500 chip has a limited memory for infer-  
 541 ence at approximately 8mb only. The original pickle file is around 6.0mb which is  
 542 compressed down to around 3mb per Ultralytics documentation. It can be further  
 543 finetuned using personal dataset for better accuracy.

## 544 Chapter 5

# 545 Summary, Conclusions, and 546 Recommendations

## 547 5.1 Summary

548 The created system is an automated attendance checker with the use of an RFID  
549 together with facial authentication to eliminate inefficiencies in conventional prac-  
550 tices at UP Visayas. The system integrated the UP RFID's exclusive identifica-  
551 tion with real-time facial identification using pretrained YOLOv8 and Mobile-  
552 FaceNet models with 1-2 second processing times per student. Major features  
553 were a Django-Nuxt web interface, hardware integration with Raspberry Pi, and  
554 two-factor authentication to maintain the CIA Triad principles (confidentiality,  
555 integrity, availability). Testing validated its superiority to manual roll calls and  
556 spreadsheet monitoring in terms of speed, accuracy, and fraud prevention, al-  
557 though light conditions and RFID reliance presented limitations.

## 558 5.2 Conclusion

## 559 5.3 Recommendation

560 For future development and improvement of the system, the following recommen-  
561 dation are proposed:



- 562     **1. Additional Biometric Authentication**
- 563         For the future enhancement of the system, it is recommended to consider
- 564         the addition of other biometrics such as voice recognition for security en-
- 565         hancement.
- 566     **2. Support for Virtual Classes**
- 567         Expand the range of the system that supports virtual classes with the use
- 568         of secure webcam verification.
- 569     **3. Technical Upgrades**
- 570         Replace Raspberry Pi with better computing devices such as NVIDIA Jetson
- 571         for better and faster processing.

## References

- Ancheta, R. F., Daniel, D., & Ahmad, R. (2021). Effect of class attendance on academic performance. *European Journal of Education Studies*, 8(9). Retrieved from <https://oapub.org/edu/index.php/ejes/article/view/3887> doi: 10.46827/ejes.v8i9.3887
- Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., Townsend, A., & Corporation, T. M. (2020, December). *Data integrity: Detecting and responding to ransomware and other destructive events*. <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>. (Retrieved December 4, 2024)
- Chen, S., Liu, Y., Gao, X., & Han, Z. (2018). *Mobilefacenets: Efficient cnns for accurate real-time face verification on mobile devices*. Retrieved from <https://arxiv.org/abs/1804.07573>
- Dewa, M., & Nyanga, L. (2020). Development of an online attendance register system (oars) using barcode technology: Going green in class. *SAIIE31 Proceedings, 5th-7th, Virtual Event*.
- Fruhlinger, J. (2024, 07). What is the cia triad? a principled framework for defining infosec policies. *CSO*. Retrieved from <https://www.csoononline.com/article/568917/the-cia-triad-definition-components-and-examples.html>
- Romero, M., & Lee, Y.-S. (2007, October). *A national portrait of chronic absenteeism in the early grades*. Retrieved from <https://www.attendanceworks.org/wp-content/uploads/2017/09/A-National-Portrait-of-Chronic-Absenteeism-in-the-Early-Grades-Oct-2007.pdf> (Accessed: 2025-01-28)
- Shoewu, E. D. O., Mekanjuola, N., & Olatinwo, S. (2014, 01). Biometric-based attendance system: Lasu epe campus as case study. , 8-14. doi: 10.12691/ajcrr-2-1-2
- Sony. (2023). imx500 key specifications [Computer software manual]. Retrieved from <https://developer.sony.com/imx500/imx500-key-specifications> (Accessed: 2025-01-28)
- Ultralytics. (2024). *Sony imx500 export for ultralytics yolov8*. Retrieved from

604 <https://docs.ultralytics.com/integrations/sony-imx500/> (Ac-  
605 cessed: 2025-01-31)  
606 Zhi, T. J., Ibrahim, Z., & Aris, H. (2014). Effective and efficient attendance  
607 tracking system using secret code. In *Proceedings of the 6th international*  
608 *conference on information technology and multimedia* (p. 108-112). doi:  
609 10.1109/ICIMU.2014.7066613

<sup>610</sup> **Appendix A**

<sup>611</sup> **Appendix Title**

## <sup>612</sup> **Appendix B**

## <sup>613</sup> **Resource Persons**