RFID Based Attendance Monitoring System

Problem Statement

The existing system of attendance monitoring is a manual system which can lead to data redundancy. In the existing system, attendance is carried out in hand written registers. It is a very time consuming process and as well as the human effort is more here. The retrieval of the information is not easy as the records are maintained in the hand written registers.

Proposed System

To overcome the drawbacks of the existing system, the proposed system has been evolved. Our project aims to reduce manual effort and save time.

Objective

To design an updated and advanced RFID based attendance monitoring system for fast and efficient attendance monitoring.

Technologies involved and their working principles:

The complete system comprises and utilises many other technologies, either hardware or software, and each technology is based on its own set(s) of principles. The technologies that are an integral part of this system are listed below:

- Radio Frequency IDentification (RFID).
- Use of microcontrollers for carrying out logical operations.
- LoRa module and LoRaWAN protocol.
- Database and Database Management System.

Systematic overview:

RFID based attendance monitoring system comprising three basic units such as -
i) Entry Level Module.
ii) Master Control Unit(MCU).
iii) Student Control Unit.

Entry Level Module- This module basically looks like a credit card swipe machine having a LCD display panel at the top along with a keypad over its body. At the top part a RFID scanner is present along with a camera for facial recognition.

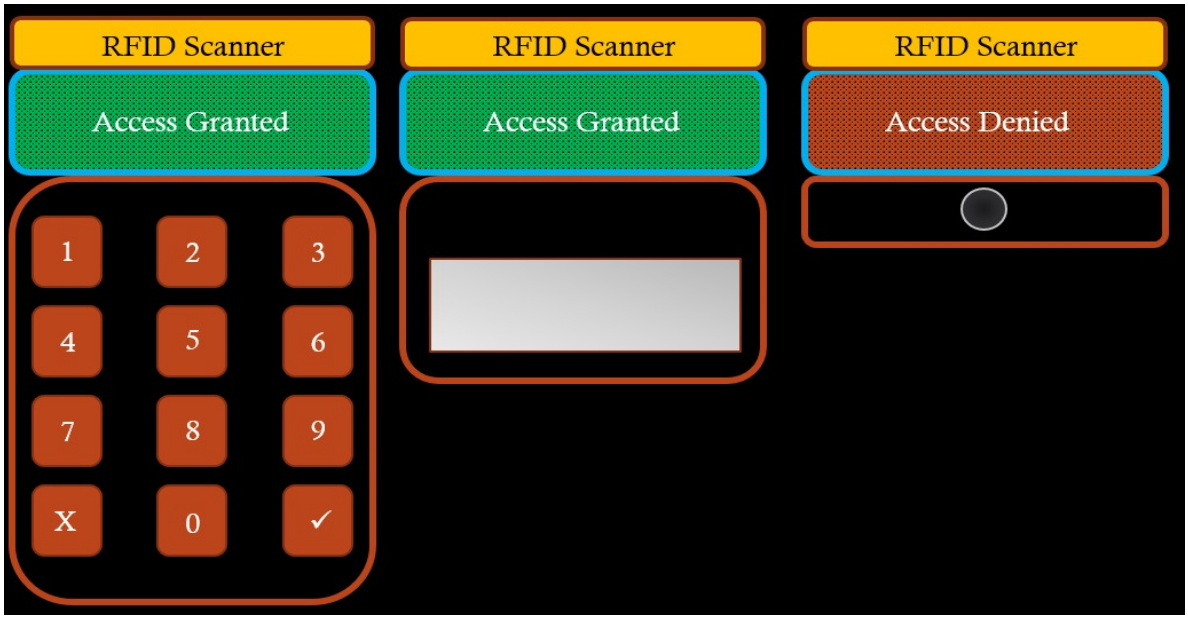


Fig:1.1 Different ways to implement Multiple-Factor Authentication
i. Number Pad based second-factor authentication
ii. Biometric scanner based second-factor authentication
iii. Facial recognition based second factor authentication

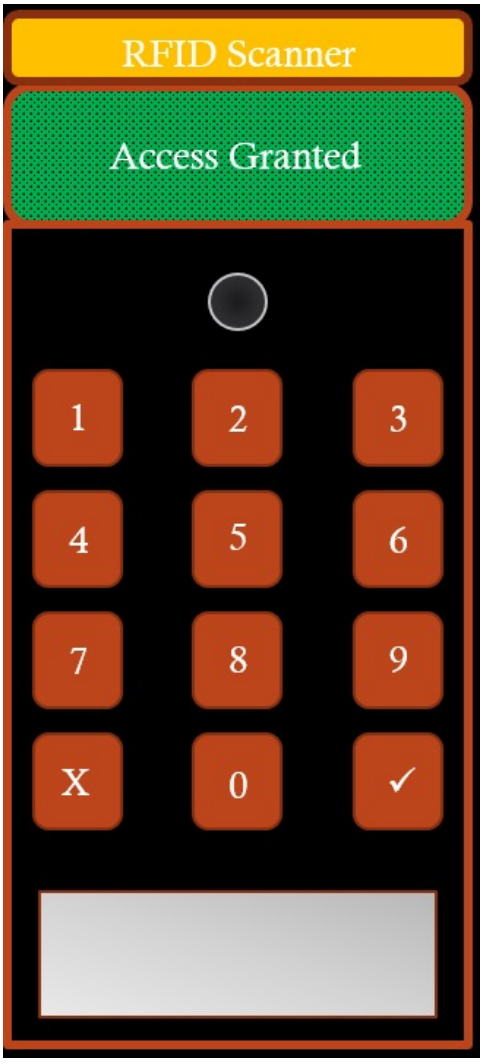


Fig 1.2 Different ways of second factor authentication can be integrated together to implement a Multiple-Factor authentication.
(In this diagram, Number pad, biometric scanning as well as Facial recognition is implemented)

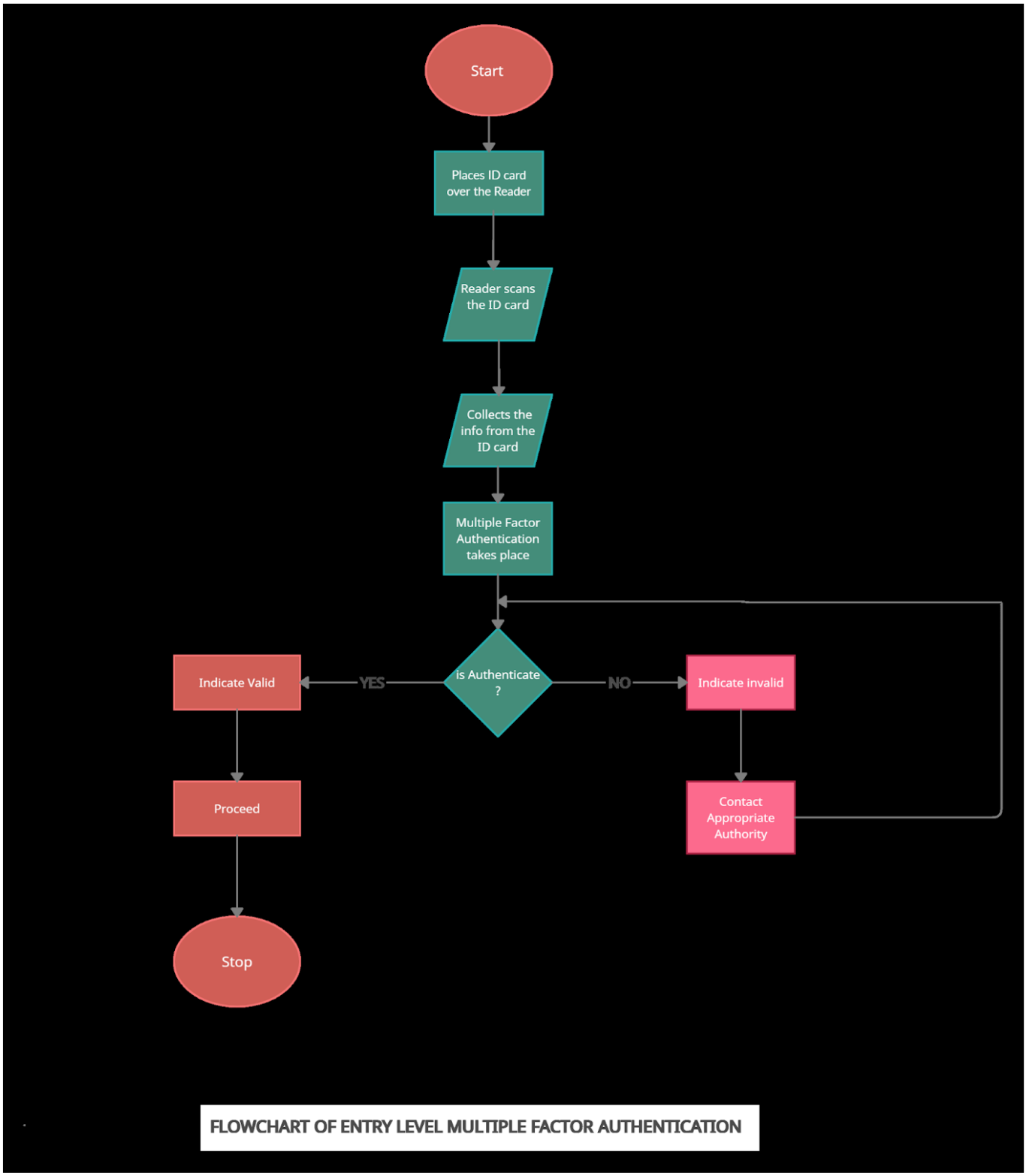
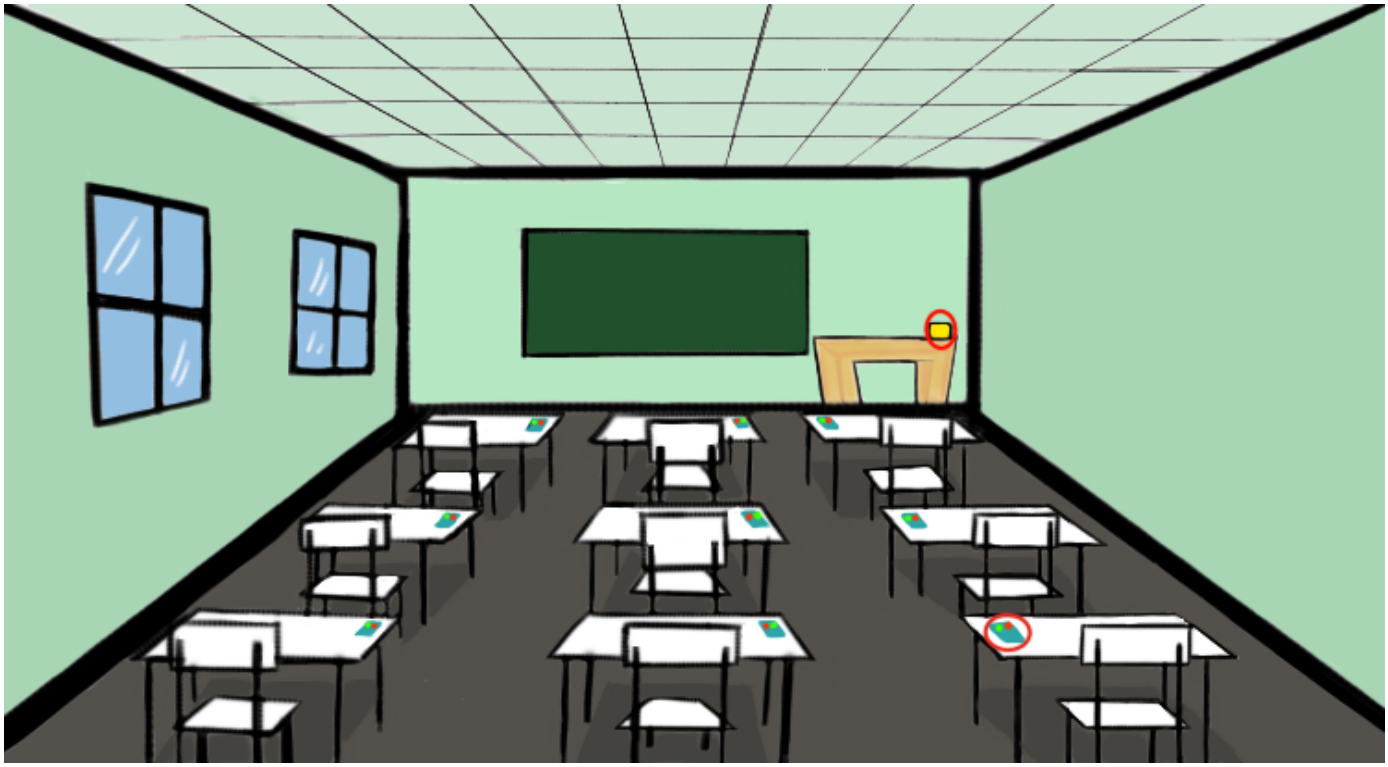


Fig 1.4 Flow chart of entry level multiple-factor authentication module



MasterControlUnit StudentControlUnit

Fig 2.1 3D view of a classroom with smart attendance monitoring system

Master Control Unit- This Unit consists of a RFID reader on the side, a display panel at the top along with a keypad below the display where teachers have to enter their authorized key for activating all student units inside the classroom.

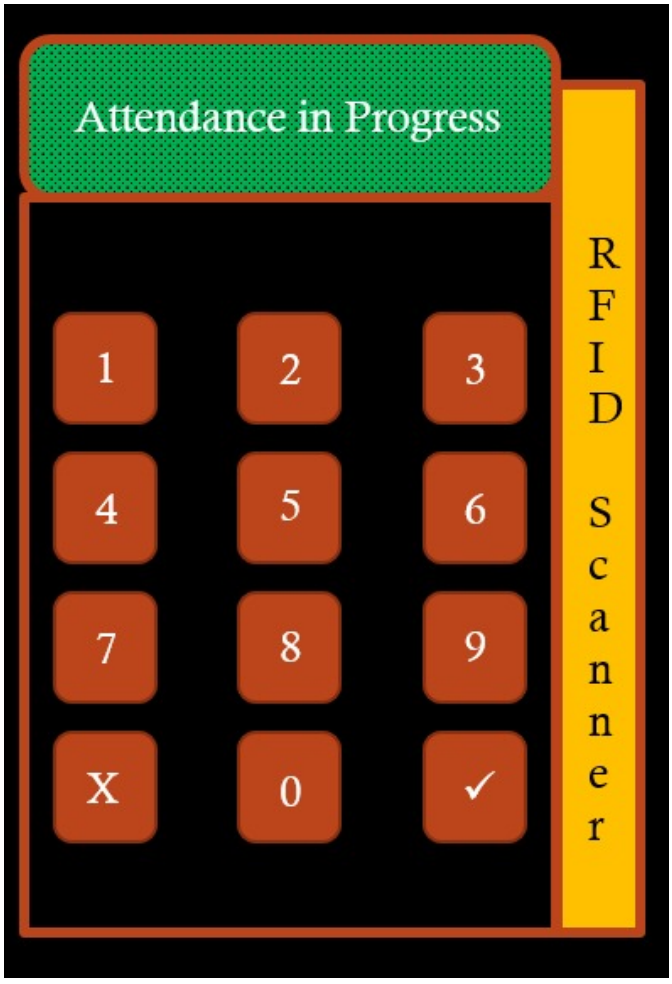


Fig 2.2 Master Control Unit capable of registering attendance and monitoring.

Student Control Unit- This unit consist of three layers and an outer covering:

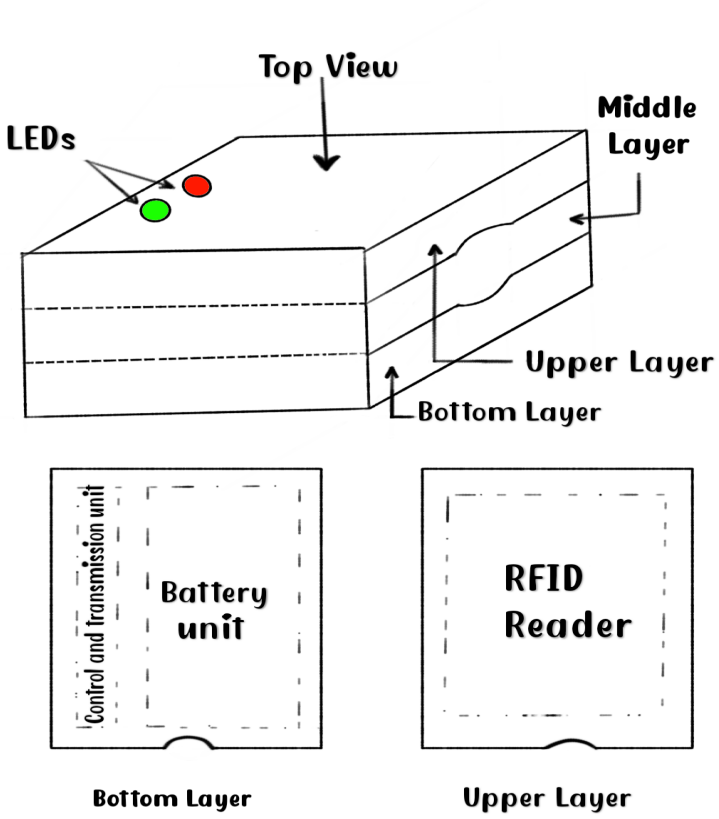


Fig:2.3 Diagram of student control unit

Upper Layer – This layer contains a RFID reader which is used to read the data sent from the Identity card. This data is then processed by the control unit.

Middle layer- In this layer a gap is made where students have to insert their RFID tag for attendance which basically contains an unique ID and other relevent data like student name, roll, dept, class/semester, etc.

Bottom Layer- This layer contains a battery unit which provides power to the CAT unit and the reader to read data from the RFID tag. It also contains a Control and Transmission Unit (CAT Unit). This unit retrieves the data from the RFID reader and sends this data to the MCU through LoRa.

Casing- The casing is the outer cover of the Student unit which holds all the three layers together and contains two indicative LEDs (one red and one Green LED) on topside.

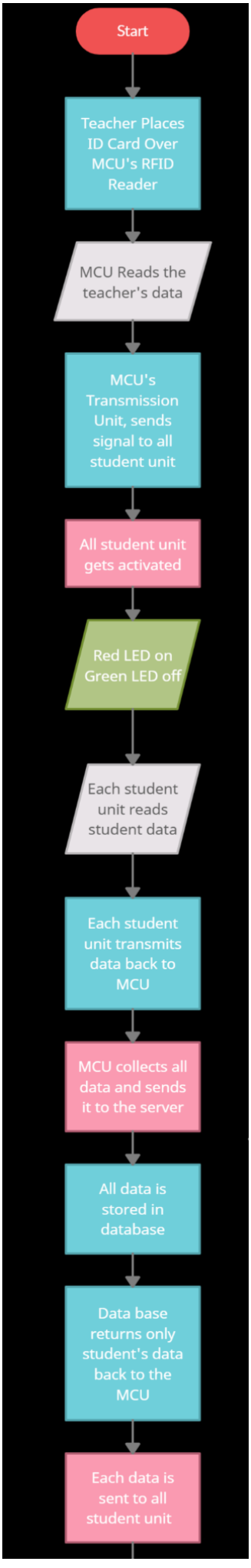
Fig 2.4 (i) Outer appearance of Student ID card (ii) Internal representation of RFID tag inside the ID Card

Systematic process flow inside the classroom:

- It is assumed that students are already inside the classroom and seated in their seats before the teacher enters the classroom.
- Once the teacher enters the classroom, the teacher places his/her ID card over the MCU's RFID reader.
- The MCU reads the teacher's ID card and temporarily stores the data inside the MCU.
- Then the MCU sends a signal to all the Student units present in the class.
- Upon receiving the signal, all the Student units get activated and the RED indicative LED glows for all student units irrespective of whether a student is seated on that table or not.
- Each and every student is now advised to provide their attendance. Now the students place their ID cards inside the provided slot.
- The RFID reader on the student unit scans the Identity card of that student and if an ID card is present, it temporarily stores the data in the Student unit.
- This data is then transmitted to the MCU by each student unit.
- The MCU combines the teacher's and the student's data and sends it to the server.
- The server stores all the necessary data.
- The server then sends back only the student data back from the database (The student data in the server is kept intact).
- The MCU receives the student data back from the server and sends this data to all student units.
- If a student unit receives a signal,
    - It checks if the value is equal to the stored value.
        - If it is equal, then the GREEN indicative LED glows and the RED indicative LED turns off.

- If a student unit does not receive a signal from the MCU, it waits for a definite period of time (say 30 sec) to get a signal from the MCU.
    - If it still does not receive a signal in that specified period of time, then the student unit shuts down.

The attendance taking process is then completed.



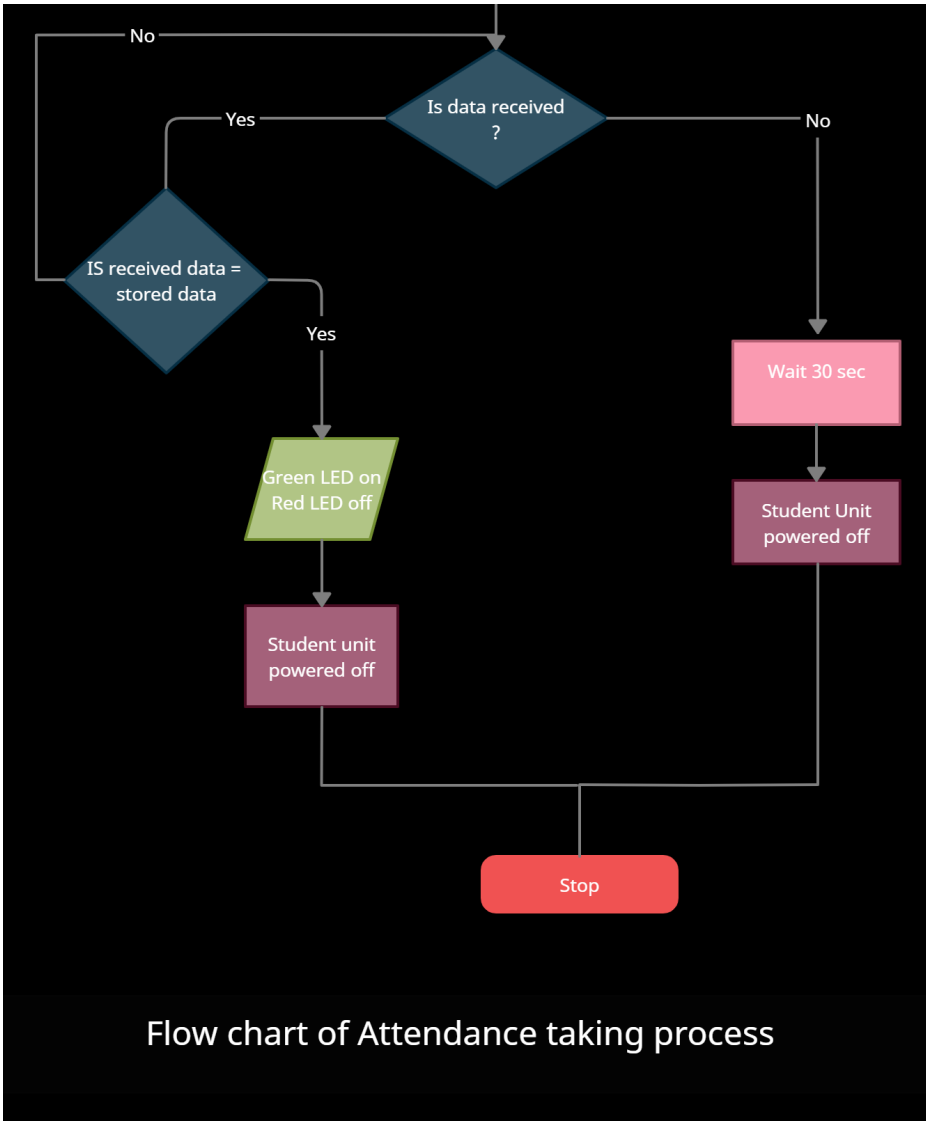


Fig 2.5 Flowchart of Attendance taking process (Click for full image)

Advantages

1. It saves time as compared to the traditional method of attendance registering process.
2. Easy to operate and efficient.
3. The communication network and protocol used, LoRa, is very robust, immune to interference, secure, provides long battery life and suits the requirements for this process.
4. Since the system is designed to be active only when required as well as it consists of a power saving communication system, the system maintenance required is very low and it is speculated to have a long lifetime.
5. It helps minimize human induced error(s).
6. The data is stored in an organised manner which helps to resolve any conflict that may arise.
7. The system is reliable and secure, hence protecting the date of any ID card holder.

Limitations(if any)

Although steps have been taken to ensure that chances of fake attendances are reduced, it can not be guaranteed that it can be completely eliminated. Even though a student needs to be present in the institutional/organisational premises, at the time of attendance it may happen that a student poses as another student to fake an attendance.

During the attendance registering process, the system is not aware if the ID Card holder is using his/her ID card for registering that particular attendance. The system, currently, is not able to check this.

This problem can also be tackled but requires more sophistication and complex designing as well as some manual effort.