During my industrial attachment , i was privileged to secure a slot at Center of Development of Electronic Devices at DEDAN KIMATHI UNIVERSITY OF TECHNOLOGY (DeKUT)

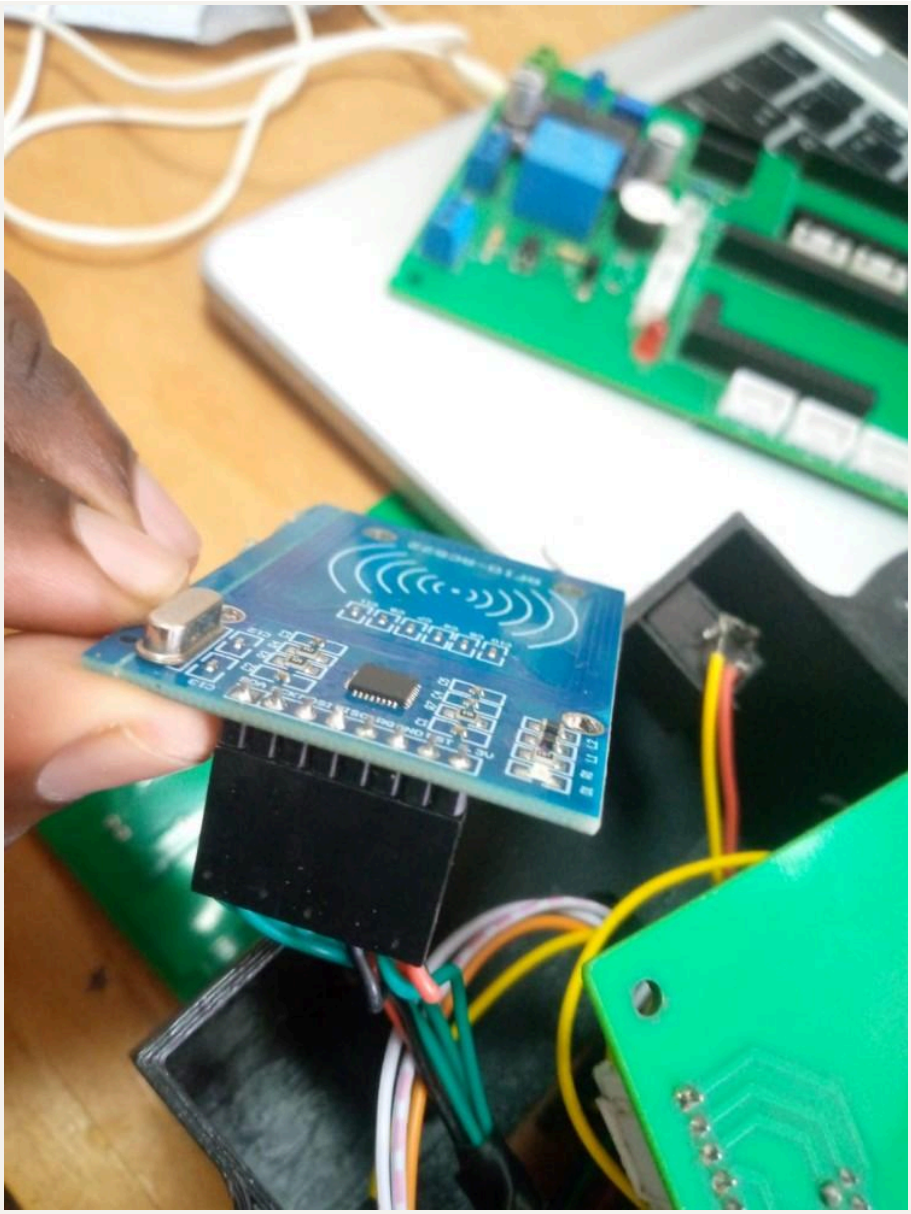
The attachment was centered on developing a clocking device and door access system that selectively grants entry to authorized users while denying access to unauthorized individuals. This device is also designed to communicate with a server database to record clocking-in and clocking-out times. The core component of this device is a card reader module known as Radio Frequency Identification (RFID) MFRC522, which operates using the Serial Peripheral Interface (SPI) communication protocol. The RFID card reader scans RFID tags to obtain their unique identification (UID) numbers, which are then stored in the EEPROM of an Arduino Pro Mini ATmega 2560 microcontroller. The system interacts with a 2.8-inch TFT display.

and a keypad interface to guide users through the process.

When a user places their RFID card near the reader, the system scans the card and retrieves its UID. If the UID matches an entry stored in the EEPROM, the user is granted access to clock in or out or to enter or exit through a door. This process ensures that only authorized personnel can use the system. The system also leverages a server database that allows administrators to input and save the UID, name, and other details of users. By using an ESP32 Dev Kit, the system can send requests to the server to check if the scanned card's details are present in the database. If the details are found, the server returns a positive response to the system, triggering a relay that deactivates a door lock and grants access.

The system's capability to enroll and delete users is essential for maintaining up-to-date access control. During enrollment, the user's UID is scanned and stored in both the EEPROM and the server database. When a user wishes to be deleted from

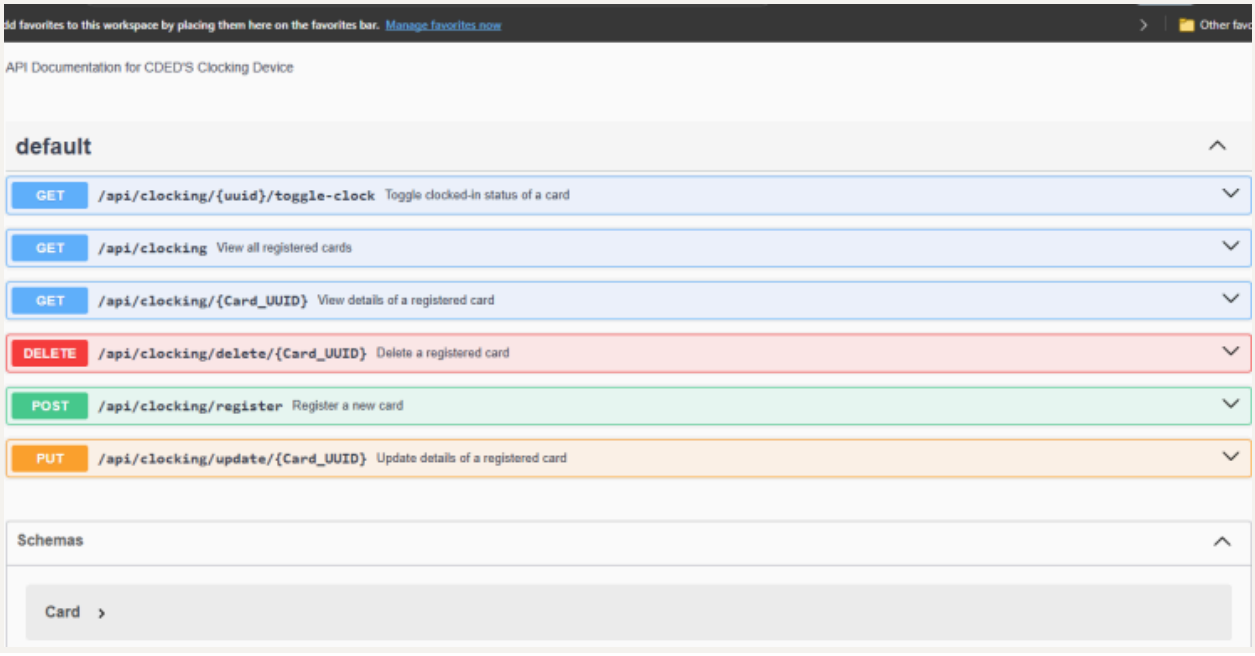
the system, their UID is removed from both storage locations. This dual storage approach ensures redundancy and reliability in access control. Additionally, the system's communication with the server database provides a robust way to manage user information and track access logs.



In practice, the device operates as follows: a user approaches the RFID card reader and presents their card. The card reader scans the UID and sends it to the Arduino

microcontroller, which checks the EEPROM for a match. If the UID is found in the EEPROM, the microcontroller sends a signal to allow access. Simultaneously, the ESP32 Dev Kit sends a request to the server database to verify the UID. If the server confirms the UID, the system triggers the relay to unlock the door. This multi-layer verification process enhances security by ensuring that only valid UIDs stored in both the EEPROM and the server database can grant access. The use of the SPI communication protocol between the RFID reader and the microcontroller ensures fast and reliable data transfer. This is crucial for the real-time operation of the system, especially during peak usage times when multiple users may be clocking in or out simultaneously. The TFT display and keypad interface provide an intuitive user experience, guiding users through the process of scanning their cards and confirming their access status.

Moreover, the system's ability to communicate with a server



database extends its functionality beyond simple access control. By logging access times and user details, the system can generate reports and analytics for administrative purposes. This data can be used to monitor employee attendance, identify access patterns, and enhance security protocols. The server database also allows for remote management of user information, making it easier for administrators to update access permissions and maintain the system.