

PROJECT ABSTRACT

Keypad and RFID Door Lock with Web Access Log

A dual-credential smart door lock — keypad PIN plus RFID on ESP32 with servo latch and a live web access-log dashboard — delivered as a built-to-order hybrid student project with firmware, working demo, report, PPT and viva kit.

01. Title

Keypad and RFID Door Lock with Web Access Log

02. Introduction / Background

Access control answers two questions: who may enter, and who actually did. Credentials — something you know (a PIN) or something you carry (a card) — solve the first; an audit log solves the second. Single-credential systems fail gracefully: a forgotten PIN or a lost card becomes a lockout. Combining a matrix keypad with 13.56 MHz RFID gives users two independent ways in, and the ESP32 adds the modern half of the product — an embedded web server that renders the access log as a filterable dashboard, so the audit trail is visible from any browser on the network.

03. Problem Statement

Basic electronic locks grant or deny entry and then forget everything: no record of who entered, when, or how many times a wrong credential was tried. Commercial access systems keep logs but are closed boxes — useless as student projects. A defensible hybrid project must demonstrate credential management, a physical locking mechanism, anti-tamper behaviour (lockout after repeated failures) and a genuinely useful web dashboard with search, filter and export. The log is what makes this hybrid rather than just hardware.

04. Objectives

- Authenticate users by 4–6-digit PIN on a 4x4 keypad and by MIFARE UID on an RC522 reader.
- Drive a servo latch with configurable unlock duration and auto-relock.
- Enforce a 3-strike lockout with cooldown, counting strikes across both credential types.
- Record every attempt — granted and denied — with timestamp, credential type and identity.

- Serve a live dashboard with search, credential filter and CSV export of the log.
- Support on-device enrollment of PINs and cards without a PC.
- Provide a tamper/duress input hook for future hardware.

05. Proposed Methodology

The keypad is scanned by row-column matrix driving with debounce; the RC522 is brought up over SPI with UID reads validated first. Credential records (PIN hashes/PINs and UIDs with names) persist in ESP32 flash through an enrollment mode. The firmware implements a state machine — idle, verifying, unlocked, lockout — driving the SG90 latch and a buzzer for feedback. The web server renders the log dashboard from the flash ring buffer with server-side filtering parameters, plus CSV export. Testing covers valid and invalid credentials for both types, the 3-strike lockout, power-cycle log retention and concurrent lock/web operation.

06. System Architecture / Working

Keypad entries are accumulated and compared against stored PINs; card taps yield UIDs compared against the enrolled roster. A match drives the servo to the unlock angle, starts the auto-relock timer and logs a GRANTED event with timestamp, type and identity; a miss logs DENIED and increments the strike counter, which triggers lockout at three. The dashboard — served by the ESP32 over WiFi — reads the same event ring: search by name, filter by credential type, sort by time and export CSV. Enrollment mode, entered by a master credential, adds new PINs and cards on-device.

07. Hardware / Software Requirements

- ESP32 DevKit (credential store, web server).
- 4x4 matrix membrane keypad.
- RC522 RFID reader + MIFARE cards (13.56 MHz).
- SG90 servo as the demonstration latch.
- Buzzer for entry feedback; tamper-switch input header.
- Web dashboard: embedded HTML/CSS/JS served by the ESP32.
- Software: Arduino IDE (C/C++ firmware).

08. Expected Outcomes

A working lock that opens on either correct credential, denies and counts wrong attempts, locks out after three strikes and auto-relocks. The dashboard shows the full event history with working search, filter and CSV export, and survives power cycles. The demo exercises enrollment, dual-credential entry, lockout and log inspection — the complete access-control loop.

09. Applications

- Laboratory and project-room access control.
- Hostel and PG-room doors.
- Small-office and storage-room security.
- Teaching platform for embedded access control.
- Exhibition demo of credential + audit architecture.

10. Future Scope

Cloud backup of the log, MQTT push alerts on denied attempts and a fingerprint-module third credential are the natural extensions. A real electric strike or solenoid would replace the demonstration servo, and a battery-backed RTC would harden timestamps.