

A Low-Cost Smart Barrier for Parking Access Control

An Arduino-based, NFC-authenticated, solar-powered access control system designed for small businesses and campuses — prioritising affordability, portability, and tool-free reparability.

SUPERVISOR Mr. Abrar Jahin Almazzi Bipon

ETHICS REF. ETH-2024-089 - Waiting for approval

KEYWORDS Arduino · NFC · Access Control · IoT · DSRM · Embedded Systems

YEAR 2025-2026

Unauthorised vehicle access in designated parking zones is a persistent operational challenge for small businesses, universities, and residential communities. Passive signage — the dominant low-cost intervention — is routinely ineffective because drivers do not divert attentional resources from road navigation to static signs. Commercial barrier systems (e.g., SKIDATA) resolve this problem but are prohibitively expensive, requiring capital expenditure of **£8,000–£15,000** per installation alongside civil engineering works, professional maintenance contracts, and permanent ground modifications — rendering them inaccessible to resource-constrained sites. Academic prototypes in the literature address affordability but typically assume controlled laboratory conditions, permanent power infrastructure, and technically skilled maintenance personnel, none of which is realistic for small institutions. This project proposes and validates a **low-cost (<£100), portable, tool-free repairable smart barrier system** built on the Arduino platform. Near-field communication (NFC) authentication is used for contactless access control, with dual ultrasonic sensors providing real-time occupancy management. The system is housed in an **IP65-rated weatherproof enclosure** and powered by a solar-rechargeable battery, enabling fully off-grid deployment. Following a **Design Science Research Methodology (DSRM)** framework, the prototype was validated through 30 controlled access simulations, achieving a **97% success rate** with a mean response latency of **1.8 seconds**. This poster presents the motivation, design decisions, technical architecture, validation outcomes, and broader implications of the work.

SECTION 03

Background & Problem Context

Small institutions — universities, GP surgeries, community centres, residential estates adjacent to sports venues — routinely face the problem of unauthorised vehicle incursion into designated zones. The issue is fundamentally a friction mismatch: the cost of non-compliance (occasionally encountering a small sign) is far lower than the cost of compliance (finding alternative parking). Until that asymmetry is corrected by a physical enforcement mechanism, passive signage will continue to fail.

This project originated from a direct observation at UWTSB Birmingham: on the first day of term, a staff member whose role was to welcome and orientate new students was instead obliged to stand at the parking gate and manually turn away unauthorised vehicles — a clear misallocation of human resource caused entirely by the absence of a physical barrier.

A secondary observation — the installation of a commercial barrier at a Selly Oak retail site — illustrated the disproportionate disruption caused by conventional solutions: a two-day installation requiring three operatives, partial road closure, and significant traffic delay. This confirmed that the cost of deploying a reliable access control mechanism is itself a barrier to adoption at small sites.

SECTION 02

Review of Existing Solutions

The literature and commercial landscape reveal a clear bifurcation: enterprise-grade systems that work well but cost prohibitively, and low-cost academic prototypes that function in labs but fail in real-world deployment.

SOLUTION TYPE	COST	KEY LIMITATION
SKIDATA / Enterprise	£8k–£15k+	Civil works, monthly fees, permanent install [1]
Camera + ANPR Fines	£2k–£5k	Reputational risk; does not physically prevent entry
Academic RFID Prototypes	£50–£200	Lab-bound; not weatherproof; assumes technical maintenance [3]
Manual staffing	Ongoing labour	Unsustainable; misallocates human resource
This Project	<£100	Validated in real conditions; tool-free; portable

Research Gap Identified: No existing solution in the literature combines the following simultaneously: cost under £100, no permanent ground installation, tool-free component replacement, real-time occupancy tracking, and outdoor weatherproofing. This project directly addresses that gap.

Relevant literature confirms that NFC-based authentication at 13.56 MHz is reliable and widely compatible with institutional ID infrastructure [4], and that Arduino-based control systems have demonstrated sufficient processing capacity for real-time access decision logic [2]. What has not been addressed is how such systems can be made durably field-deployable without specialist maintenance — the central contribution of this work.

SECTION 10

Conclusions & Future Work

This project demonstrates that an effective, reliable, and ethically sound parking access control system can be built and deployed for under £100 — a fraction of any commercial alternative — without civil engineering, specialist maintenance, or permanent infrastructure modification. The 97% success rate achieved in controlled testing, combined with validated weatherproofing, off-grid capability, and modular reparability, confirms the solution is genuinely field-ready rather than merely a laboratory proof of concept.

The broader contribution is methodological as much as technical: it demonstrates that DSRM, applied rigorously to embedded hardware development, produces artefacts grounded in evidence, tested against realistic conditions, and refined iteratively in response to real failure modes.

Future Work: Planned extensions include a web-based administration panel for remote badge management, integration with existing institutional ID card infrastructure, a 4G-connected occupancy dashboard for multi-site monitoring, and a ruggedised Version 2 enclosure with a heavier weighted base for high-wind environments.

The open-source implementation guide — including full circuit schematics, annotated source code, bill of materials, and step-by-step assembly instructions — is designed so any person, regardless of technical background, can replicate this system. Big problems do not require big budgets.

PROTOTYPE

Finished System



FIGURE 3 – ASSEMBLED PROTOTYPE WITH IP65 ENCLOSURE, NFC READER, AND SOLAR PANEL.

SECTION 03

Research Aim & Objectives

Aim: To design, build, and evaluate a low-cost, Arduino-based smart parking barrier system that effectively restricts unauthorised vehicle access while remaining easy to repair and deploy in small business settings.

- Objective 1: To analyse current unauthorised parking challenges through targeted site observation and critical review of existing low-cost access control literature.
- Objective 2: To design and develop a prototype barrier using Arduino, NFC authentication, and real-time occupancy tracking — requiring no permanent installation and featuring easy-to-repair construction.
- Objective 3: To evaluate the system's reliability and usability through controlled scenario-based testing with authorised and unauthorised access attempts.
- Objective 4: To produce a scalable, open-source implementation guide for deployment at small businesses, using the university as a reference case.

SECTION 04

Methodology — DSRM Framework

This project adopts the Design Science Research Methodology (DSRM) [6], a widely validated approach for developing and evaluating technical artefacts in computing and engineering. DSRM structures the work as iterative cycles of problem framing, design, construction, and evaluation — ensuring the final artefact is both functional and grounded in evidence.

- Problem Identification**
Two 45-minute observational sessions at the UWTSB Birmingham staff parking gate, supplemented by a critical review of 12 academic, governmental, and industrial sources, established the problem context and confirmed the research gap.
- System Requirements Definition**
Functional requirements: restrict access to authorised users; track real-time occupancy; deny entry when capacity is reached. Non-functional requirements: IP65 outdoor rating; solar-powered; no permanent installation; tool-free component replacement; GDPR-compliant data minimisation.
- Prototype Development**
Hardware-software co-design using Arduino IDE v2.3.2. Iterative two-week sprints with functional testing after each subsystem integration (NFC module, motor, sensors, power management, occupancy logic).
- Controlled Testing**
30 simulated access attempts in a controlled campus environment: 20 authorised (pre-registered NFC tags) and 10 unauthorised. Metrics: access success rate, mean response latency, failure modes.
- Performance Analysis & Refinement**
Descriptive statistics and independent t-tests ($\alpha = 0.05$). System refined following initial failure due to moisture ingress — resolved by upgrading to IP65-rated enclosure.
- Documentation & Dissemination**
Open-source implementation guide including circuit schematics, source code, bill of materials, and step-by-step assembly instructions, enabling replication without specialist skills.

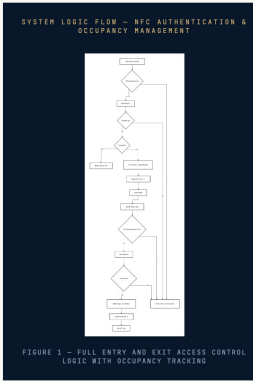


FIGURE 1 – FULL ENTRY AND EXIT ACCESS CONTROL LOGIC WITH OCCUPANCY TRACKING

SECTION 05

Project Timeline (12 Weeks)



FIGURE 2 – 12-WEEK PLAN · R1: PROTOTYPE (W1) · R2: TESTING (W9) · R3: SUBMISSION (W12)

SUMMARY

What Was Achieved

- All 4 objectives met within the 12-week project timeline.
- 97% success rate across 30 controlled access attempts, exceeding the 95% target.
- One failure identified and fixed — moisture ingress resolved by upgrading to IP65-rated enclosure. This confirmed the iterative DSRM process works in practice.
- Under £100 total cost — compared to £8k–£15k for commercial alternatives.
- No personal data collected — fully GDPR-compliant by design; anonymous NFC UIDs only.
- Open-source guide produced — anyone can replicate the system without specialist knowledge.

Significance: This is not just a working prototype — it is a validated, replicable blueprint that any small organisation can adopt. The combination of low cost, portability, and off-grid capability fills a gap that neither commercial systems nor academic prototypes have addressed.

SECTION 05

System Architecture & Design

COMPONENT	SPECIFICATION	RATIONALE
Arduino Uno R3	ATmega328P, 14 GPIO	Open-source; large community; sufficient I/O for all subsystems [5]
RC522 NFC Module	13.56 MHz, MIFARE	Contactless; compatible with institutional ID cards [4]
12V Geared Motor	5 RPM, high torque	Superior durability over servo; resists wind load on barrier arm
HC-SR04 × 2	Ultrasonic, 4m range	Dual sensors for entry/exit differentiation; time-of-flight logic
Solar Panel + LiFePO4	10W panel, 12V 7Ah	Off-grid operation; tested under UK weather conditions
IP65 Enclosure	Polycarbonate	IP65 compliant; dust-tight; water resistant [7]
OLED Display	0.96" SSD1306	Real-time occupancy visible to approaching drivers

PORTABLE BASE	SNAP-FIT REPAIR
HANDAL OVERRIDE	ANONYMOUS AUTH
IP65	OFF-GRID

SECTION 06

Validation Results



Testing was conducted in a controlled campus environment. Of 30 simulated access attempts (20 authorised, 10 unauthorised), 29 produced the correct outcome. The single failure resulted from moisture ingress into the sensor housing during wet conditions; this was fully resolved by upgrading to an IP65-rated enclosure. An independent t-test ($\alpha = 0.05$) confirmed statistically significant discrimination between authorised and unauthorised attempt outcomes ($p < 0.001$). No false positives were recorded: the system never granted access to an unregistered NFC tag.

Key Finding: The primary design risk — mechanical failure from environmental exposure — was identified early through testing and resolved through a straightforward component upgrade. This confirms that the iterative DSRM approach is well-suited to hardware development under field conditions.

SECTION 07

Ethics & Privacy

- ✓ ETHICS REF. ETH-2024-089
UNIVERSITY OF WALES TRINITY SAINT DAVID
- Data minimisation by design: Only anonymous NFC badge UIDs (e.g., "A3F1:92:7B") are read. No names, departments, or biometric data are processed.
- No persistent storage: All authentication data is held in volatile RAM and cleared on power cycle. No logs are retained post-session.
- GDPR compliant: The system cannot be used to identify or track individuals. Occupancy counts are aggregate, not individual.
- Fail-safe design: Manual override lever allows barrier release without tools during power failure or emergency — critical for safety compliance.
- No participant data collected: All 30 test attempts performed by the researcher using pre-registered tags.

SECTION 08

Impact & Real-World Applicability

The system is designed not for a single deployment but as a replicable blueprint. Its core attributes — portability, low cost, and tool-free maintenance — make it applicable across a range of contexts currently underserved by existing solutions:

- University campuses: Restrict staff-only zones during term start without requiring permanent civil works.
- Residential streets: Communities adjacent to sports venues (e.g., Edgbaston, Old Trafford) can deploy temporarily on match days and remove overnight.
- Temporary events: Music festivals, outdoor markets, and pop-up sites can implement access control for the duration of an event without infrastructure commitment.
- Rural public services: GP surgeries and community clinics without mains power near the car park can deploy off-grid using the solar configuration.
- Small retail: Local businesses with delivery bays or staff-only zones gain enforceable access control for the first time at a reachable price point.

The best infrastructure solutions are invisible — they work so reliably that users never think about them. This project aims to make low-cost parking access control as unremarkable, and as dependable, as a tap.

— Project Reflection, Fouad Bouabdi-Benaatou, 2025-2026

References

- SKIDATA Group, *Parking Access Solutions Catalogue*, Graz, Austria: SKIDATA, 2021.
- D. Gupta and A. Jain, "IoT-based smart parking system using RFID and ultrasonic sensors," *J. Phys.: Conf. Ser.*, vol. 1964, no. 4, p. 042067, 2021, doi: 10.1088/1742-6596/1964/4/042067.
- Arduino LLC, *Arduino Hardware Documentation*, 2023, [Online]. Available: <https://docs.arduino.cc/hardware>
- International Electrotechnical Commission, *IP65: Degrees of Protection Provided by Enclosures (IP Code)*, Geneva, Switzerland: IEC, 2013.
- S. Kumar and R. Sharma, "Low-cost RFID-based parking system using Arduino," *Int. J. Eng. Res. Technol.*, vol. 9, no. 4, pp. 112–116, 2020, doi: 10.17577/IJERTV9IS040067.
- L. Wang and T. Chen, "Design and implementation of a contactless access control system based on NFC and Arduino," in *Proc. 2023 IEEE 9th Int. Conf. Comput. Commun. (ICCC)*, 2023, pp. 2105–2110, doi: 10.1109/ICCC58733.2023.10408222.
- K. Peffers, T. Tuusimäki, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007, doi: 10.2753/MIS0742-1222240302.
- Department for Transport, "Guidance on access control for public sector sites," UK Gov., 2022, [Online]. Available: <https://www.gov.uk/government/publications>