Smart Attendance – Technical Pack (Orange Pi 5)

1. Burning OS & Code on Orange Pi 5 (Ethernet-Only Set-up)

a) Download Orange Pi 5 Debian/Ubuntu image. Flash to microSD/NVMe with Balena Etcher.
b) First boot (HDMI+keyboard) → create user, set password, enable SSH.
c) Network: plug Ethernet. Disable Wi■Fi/Bluetooth: mask services, remove firmware.
d) Update packages:

```
sudo apt update && sudo apt -y upgrade sudo systemctl mask wpa_supplicant
bluetooth ModemManager || true echo "blacklist brcmfmac" | sudo tee
/etc/modprobe.d/nowifi.conf echo "blacklist btusb" | sudo tee
/etc/modprobe.d/nobt.conf sudo apt install -y python3-pip git
python3-opencv libopencv-dev python3-venv python3-numpy python3-smbus
i2c-tools spidev libnfc-bin libnfc-dev libpcsclite-dev pcscd
libatlas-base-dev cmake build-essential
```

Create project user + folder:

```
sudo adduser attend && sudo usermod -aG spi,i2c,gpio,dialout attend sudo
mkdir -p /opt/attend && sudo chown -R attend:attend /opt/attend
```

Python venv + dependencies:

```
python3 -m venv /opt/attend/venv source /opt/attend/venv/bin/activate pip
install --upgrade pip pip install opencv-python face-recognition numpy
pillow pyserial spidev RPi.GPIO pyfingerprint pn532py deactivate
```

Systemd service (auto-start at boot):

```
sudo tee /etc/systemd/system/attend.service &>/dev/null <<'EOF' [Unit]
Description=Smart Attendance Kiosk After=network-online.target
Wants=network-online.target [Service] User=attend Group=attend
WorkingDirectory=/opt/attend Environment=VIRTUAL_ENV=/opt/attend/venv
Environment=PATH=/opt/attend/venv/bin:/usr/bin
ExecStart=/opt/attend/venv/bin/python /opt/attend/main.py Restart=always
RestartSec=3 [Install] WantedBy=multi-user.target EOF sudo systemctl
daemon-reload sudo systemctl enable --now attend.service
```

2. Peripherals – Wiring & Drivers

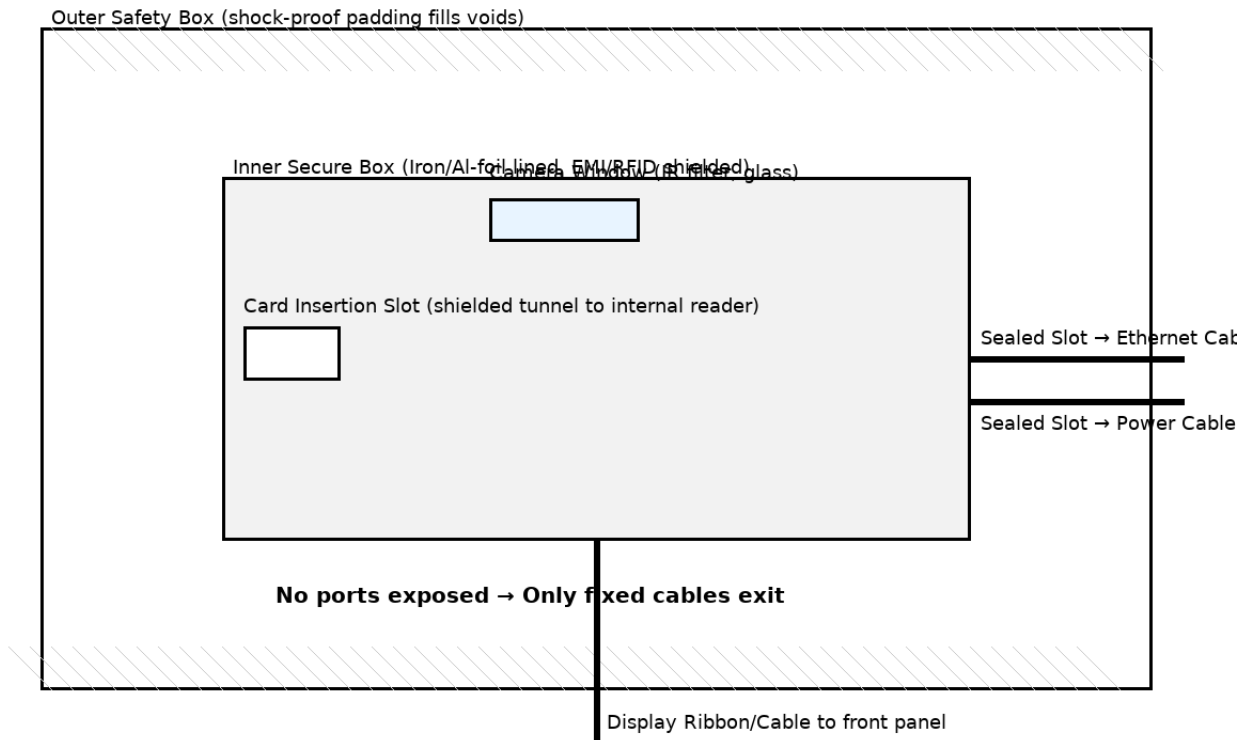|	Interface	Pins/Port	Driver/Lib	Notes
MX219/OV5647)	MIPI CSI	CSI port	opencv, v4l2	Enable camera kernel modules; IR varian
t (R307/GT511C3)	UART/USB	GPIO14/15 or USB	pyfingerprint	3.3V/5V as per module; common GND.
32) or RFID (RC522)	I2C/SPI	I2C: SDA/SCL; SPI: CE0,MOSI,MISO,SCK	nfcpy, pn532py or spidev	Read-only UID mode; custom encoding c
3.5–4")	HDMI/SPI	HDMI out / SPI pins	fbcp, vendor driver	Mirror GUI or show status page only.
LEDs	GPIO	Any free GPIO + resistor	RPi.GPIO (OPi.GPIO)	Tone/LED feedback for pass/fail.
	RJ45	LAN	systemd-networkd	Static/DHCP as per IT policy.
+ 5000mAh	5V power	GPIO header	vendor	Graceful shutdown signals optional.

NFC Policy (Read-Only UID, No Master Cards)

• Reader accepts only UID reads; APDU/writable sectors ignored.
• UID must pair with biometric (face/fingerprint).
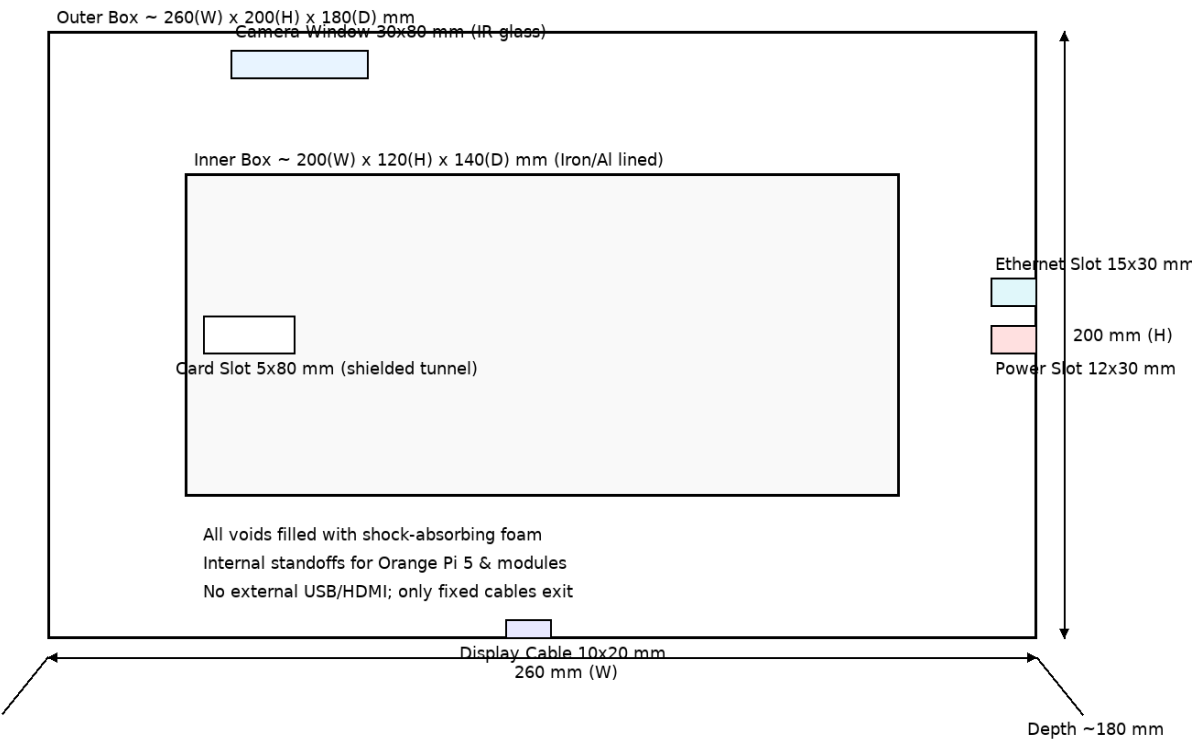• Custom scramble/whitelist check in backend; clones auto-flag & lockout.

3. Casing Design — Dimensions & Shielding

- Inner secure box (EMI/RFID shielded): ~200(W) x 120(H) x 140(D) mm, iron or Al-foil lined.
- Outer safety box: ~260(W) x 200(H) x 180(D) mm; voids filled with shock-absorbing foam.
- Only three sealed slots: Ethernet (15x30 mm), Power (12x30 mm), Display (10x20 mm).
- Flush card slot (5x80 mm) with shielded tunnel; IR glass camera window (30x80 mm).
- No external ports; service via internal header after unlocking lid.

Simplified Casing Diagram (Not to Scale) — Inner Secure Box inside Outer Safety Box

Outer Safety Box (shock-proof padding fills voids)

Inner Secure Box (Iron/Al-foil lined, EMI/RFID shielded)
Camera Window (IR filter glass)

Card Insertion Slot (shielded tunnel to internal reader)

Sealed Slot → Ethernet Cable

Sealed Slot → Power Cable

No ports exposed → Only fixed cables exit

Display Ribbon/Cable to front panel

Engineering Sketch (Approximate Dimensions, mm) — Cuboidal Casing

Outer Box ~ 260(W) x 200(H) x 180(D) mm
Camera Window 30x80 mm (IR glass)

Inner Box ~ 200(W) x 120(H) x 140(D) mm (Iron/Al lined)

Ethernet Slot 15x30 mm

200 mm (H)

Power Slot 12x30 mm

Card Slot 5x80 mm (shielded tunnel)

All voids filled with shock-absorbing foam
Internal standoffs for Orange Pi 5 & modules
No external USB/HDMI; only fixed cables exit

Display Cable 10x20 mm
260 mm (W)

Depth ~180 mm

4. Why Judges Should Select This Project (Keywords)

• Tamper-proof enclosure; EMI/RFID shielding; no exposed ports; only fixed cables.

• Two-factor attendance: biometric (face/fingerprint) + card (NFC/RFID).

• Ethernet-only: eliminates Wi■Fi/Bluetooth attack surface; secure, deterministic networking.

• Anti-cloning NFC: read-only UID, custom encoding, backend pair with biometrics.

• Rural-ready: low power, shockproof, offline queue with auto-sync, easy IT maintenance.

• Transparent UX: 3.5–4" display shows live face feed and clear verification status.

• Scalable & affordable: Orange Pi 5 platform, open-source libs, modular peripherals.

• Auditability: local logs, centralized LAN sync, lockout on tamper or clone attempts.