☑ 4.3.10 Security Issues – EcoSweep Cleaning Robot

☑ ▶ 1. Data Transmission Security

Issue:

- Data (commands) are sent from the **Mobile App to Raspberry Pi** using Classic Bluetooth (SPP).
- Bluetooth SPP is not highly secure by default — vulnerable to eavesdropping, spoofing, and man-in-the-middle (MITM) attacks.

Mitigation Strategies:

- Implement **Bluetooth Pairing with PIN Authentication** to reduce unauthorized connection risks.
- Use **data encryption (AES)** in the app and Raspberry Pi communication layer.
- Avoid transmitting sensitive information (e.g., passwords) in plain text.
- Ensure a limited connection window — allow Bluetooth connections only when explicitly initiated.

☑ ▶ 2. Unauthorized Access

Issue:

- Without proper authentication, any nearby device could potentially send commands to EcoSweep.

Mitigation Strategies:

- Implement an authentication mechanism between the Mobile App and Raspberry Pi (e.g., passcode or token-based).
- Whitelist allowed Bluetooth MAC addresses to restrict access to only the user's device.
- Disable discoverability after pairing is complete.

☑ ▶ 3. Command Injection

- ***Issue:***

  - Malicious commands sent by unauthorized users or malformed data can cause unexpected behavior.

- ***Mitigation Strategies:***

  - Validate and sanitize all incoming command data at the Raspberry Pi before forwarding to Arduino Mega.
  - Use a strict command structure with a checksum or hash to verify integrity.
  - Reject invalid or corrupted command packets.

☑ ▶ 4. Sensor Data Integrity

- ***Issue:***

  - Sensor data (Ultrasonic, GPS, IMU, Compass) can be tampered with or falsely injected by hardware faults or attacks.

- ***Mitigation Strategies:***

  - Implement sanity checks (e.g., acceptable value ranges).
  - Cross-check data from multiple sensors to detect anomalies.
  - Log sensor data for audit purposes and post-event analysis.

☑ ▶ 5. Physical Security

- ***Issue:***

  - Physical access to Raspberry Pi and Arduino Mega could allow attackers to tamper with the system.

◇ *Mitigation Strategies:*

- Use tamper-proof casing for the EcoSweep hardware system.
- Avoid exposing debug ports during normal operation.
- Implement a secure boot process for Raspberry Pi to prevent unauthorized firmware changes.

☑ ▶ 6. Data Privacy

◇ *Issue:*

- GPS location data and sensor logs could expose private information (e.g., home location).

◇ *Mitigation Strategies:*

- Store data locally on Raspberry Pi and avoid uploading to cloud unless encrypted and secured.
- Provide users the option to enable/disable GPS logging.
- Inform the user about data collection in privacy policy.

☑ Summary to Add in Documentation

➤ Key Security Issues and Their Mitigation

Security Issue	Mitigation Strategy
Data Transmission Security	Use encrypted Bluetooth communication + PIN authentication
Unauthorized Access	MAC address whitelisting + authentication tokens
Command Injection	Strict input validation + checksum verification
Sensor Data Integrity	Sanity checks + Cross-sensor validation
Physical Security	Tamper-proof casing + Disable debug ports
Data Privacy	Local storage of GPS logs + User consent prompt

☑ Final Note to Add in Documentation

Security is a critical aspect of the EcoSweep system because it ensures safe operation, prevents unauthorized control, and protects sensitive user and sensor data. These measures help guarantee that EcoSweep functions reliably in home environments without privacy or safety risks.