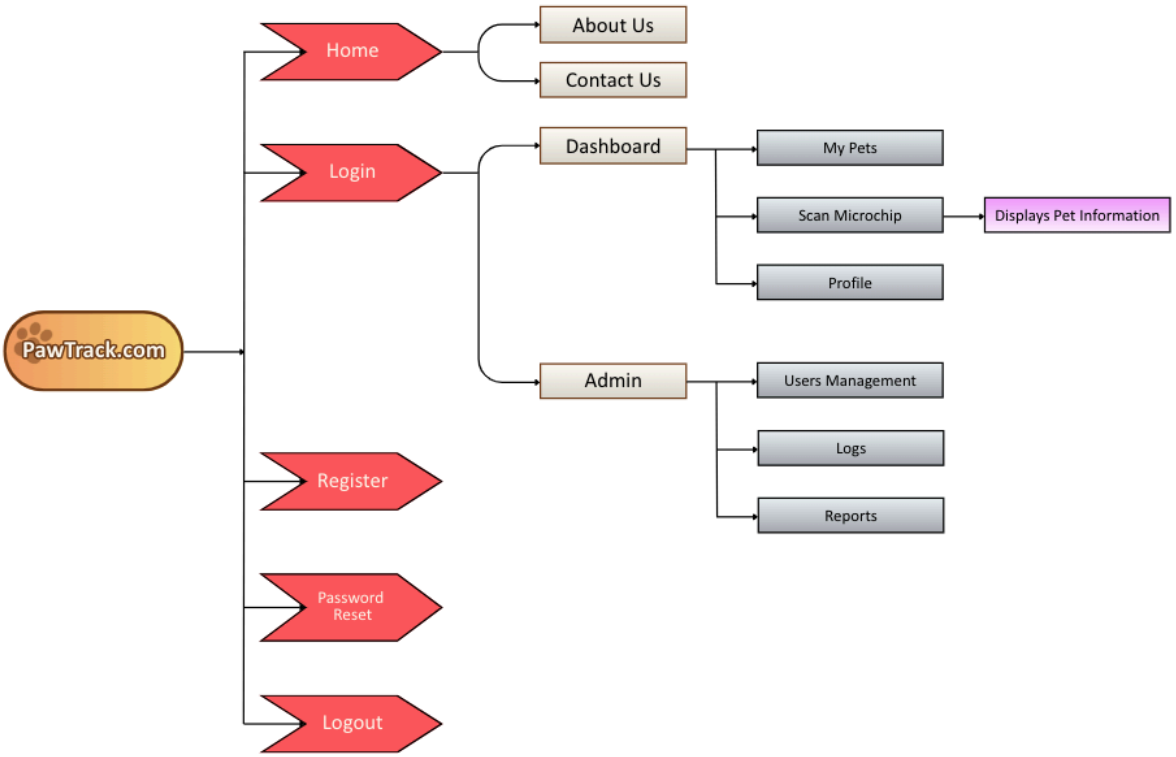
Activity 4 – Sitemap Diagram September 09, 2025
GROUP 10 BM2

BORRINAGA, Don Carlo C.
DENIÑA, Julia Abigail B.
ONA, Shanen Francesca B.
TAN, Paul Gabriel S.

PawTrack: IoT-Integrated Web-Based Pet Information Management System with Microchip Detection



Secure Site Map

This site map organizes the system's pages and features, highlighting key security considerations for each section.

- **Public Access Pages**
  - Home (/)
    - *Security Notes:* Simple landing page, no sensitive data.
  - About (/about)
    - *Security Notes:* Informational only.
  - Login (/login)
    - *Security Notes:* All form submissions **must** use POST requests and be transmitted over HTTPS. Passwords should be hashed on the server using a strong, one-way

algorithm (e.g., bcrypt).
    - Register (/register)
        - *Security Notes:* Similar to Login. Requires server-side validation for all fields. Email verification process is highly recommended to prevent fraudulent accounts.
    - Password Reset (/reset)
        - *Security Notes:* Implement a secure, token-based reset process to prevent unauthorized password changes.

- **Authenticated User Dashboard**
    - Dashboard (/dashboard)
        - *Security Notes:* All sub-pages on the dashboard require a valid, active session token. Access to this page is restricted to logged-in users.
    - My Pets (/dashboard/pets)
        - *Security Notes:* Only displays pets associated with the currently logged-in user.
        - View Pet (/dashboard/pets/:pet_id)
            - *Security Notes:* **Strict** access control. The system must verify that the user is authorized to view the specific pet ID (:pet_id) before retrieving and displaying the data.
        - Add New Pet (/dashboard/pets/new)
            - *Security Notes:* All form data (e.g., pet details, owner information) must be sanitized and validated on the server.
    - Scan Microchip (/dashboard/scan)
        - *Security Notes:* API endpoints for this function are heavily secured. They only accept requests from a verified IoT device with a valid API key, and the data payload must be encrypted.
    - Profile Settings (/dashboard/profile)
        - *Security Notes:* User can view/edit their own information. Changes to sensitive data (e.g., email, password) must be validated with the user's current password.

- **Administrator Pages**
    - Admin Panel (/admin)
        - *Security Notes:* Access is restricted to users with the Admin role. System must log all administrative actions, as these have a high impact on the system.
    - User Management (/admin/users)
        - *Security Notes:* Admin can view, add, or delete user accounts. All actions are logged.
    - Audit Logs (/admin/logs)
        - *Security Notes:* Read-only access for admins. This page provides a chronological, immutable record of all major system events, including failed login attempts, data modifications, and security alerts.

- **IoT API Endpoints**

- POST /api/scan-chip
  - *Security Notes:* This is the most critical endpoint. It must be protected by a unique API key, rate-limiting, and constant monitoring for suspicious activity. Data payloads (the chip ID) must be encrypted.