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

Group 10

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

Business Objectives

The "PawTrack" system, an IoT-integrated web-based pet information management system with microchip detection, aims to benefit its client, Bethlehem Animal Clinic, in several key ways.

- **Improve efficiency and security**: The system will replace manual record-keeping, which is prone to human error and data loss, with a secure, automated process. By using microchip detection, it will provide a faster, more reliable way to identify pets and retrieve their information.

- **Centralize and synchronize data**: The project will address the issue of delays and inconsistencies that occur when a pet is transferred between branches. The IoT technology will ensure real-time data synchronization across multiple locations, providing a single, consistent source of truth for pet records.

- **Enhance data security**: The system will protect sensitive pet and owner data from unauthorized access, a significant risk with traditional methods. It will implement security measures like encrypted data transmission and role-based access control to build customer trust.

User Requirements

Here are the user requirements for the "PawTrack" system based on the different types of users and their interactions.

- The **vet clinic staff** shall **scan a pet's microchip** in order to **retrieve the pet's profile from a secure database and display essential details**.

- The **vet clinic staff** shall **access the web-based platform** in order to **manage and update pet information**.

- The **vet clinic staff** shall **view a pet's complete records** (including vaccination history and medical records) in order to **provide prompt and informed care**.

- The **system administrator** shall **set up role-based access control** in order to **protect sensitive data from unauthorized access**.

- The **system administrator** shall **view audit logs** in order to **monitor all major system events and security alerts**.

Functional Requirements

Functional requirements specify what the system should do, the behavior of the system, and what the user and system should accomplish.

- **User Authentication and Authorization**: The system must provide secure login and registration processes. For public-facing pages like Login and Register, all form submissions must use
  - **Creating New Users**
    - This function allows the system administrator to create new users.
    - User will provide the following details:
      - E-mail
      - Password
      - Confirmed Password
      - First Name
      - Last Name
      - Contact Number
      - Address
    - The system administrator has to input the new user's information with additional details:
      - Customer ID/Employee ID
      - Starting Date
      - Role/ Access

  - **Login for Users**
    - This function allows the authorized users of the system to login. The system automatically detects if the user is a customer, employee or as a system administrator.
  - **Editing User Information**
    - This function allows the user to edit the user information such as Mobile Number, Email address, and saved address in case the user chooses to have them changed.

    - **HTTPS** and **POST requests**, with passwords hashed using a strong, one-way algorithm like **bcrypt**. Access to authenticated user dashboards and administrator pages requires a valid session token and is restricted based on the user's role.

- **Microchip Detection and Data Retrieval**: The system must utilize an **IoT-compatible microchip scanner** to read a pet's RFID-enabled microchip. The scanner will transmit the pet's unique ID to the web platform, which will then retrieve and display the corresponding pet profile from a secure database. The API endpoint for this is the most critical, requiring protection with a unique API key, rate-limiting, and encryption for data payloads.

- **Centralized Database Management**: The system must provide a secure, centralized database to store pet and owner information:
        - Pet Name
        - Pet IDnum
        - Vaccination History
        - Medical Records

  Authorized users must be able to view, add, edit, and delete pet profiles.

- **Real-time Data Synchronization**: The system shall ensure data is synchronized in real-time across all clinic branches. This prevents data inconsistencies and delays in accessing vital information.

- **Secure Data Handling**: All form data submitted must be sanitized and validated on the server. For sensitive actions, like changing a password, the system must validate the user with their current password. The system must also log all administrative actions due to their high impact.

- **Audit Logging**: The system must provide an **Audit Logs** page that is read-only for administrators. This page will provide a chronological, immutable record of all major system events, including failed login attempts, data modifications, and security alerts. The system must also log all administrative actions due to their high impact on the system.

- **Report Generation**: The system must allow administrators to generate reports. This function should enable the administrator to create reports based on the current users list and all system transactions for monitoring purposes.