UNIVERSITY OF MAKATI

DEVELOPMENT OF BULLYPROOF: A MOBILE APPLICATION IN REPORTING CYBERBULLYING INCIDENTS FOR THE UNIVERSITY OF MAKATI USING LOGISTIC REGRESSION ALGORITHM

A CLOUD DOCUMENTATION SUBMITTED TO THE FACULTY OF COLLEGE OF COMPUTING AND INFORMATION SCIENCES IN CANDIDACY FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE
(APPLICATION DEVELOPMENT TRACK)

BY

BANTILO, JADE DANIELE M.

CORDA, RYAN P.

DERIGE, PAUL ANGELO

EUGENIO, SHILOH B.

MAKATI CITY, PHILIPPINES

DECEMBER 2024

The CLOUD DOCUMENTATION entitled:

DEVELOPMENT OF BULLYPROOF: A MOBILE APPLICATION IN REPORTING CYBERBULLYING INCIDENTS FOR THE UNIVERSITY OF MAKATI USING LOGISTIC REGRESSION ALGORITHM

prepared by Jade Daniele M. Bantilo, Ryan P. Corda, Paul Angelo Derige, Shiloh B. Eugenio and will be submitted to

____
PROF. ETHEL RAMOS
ELECTIVE 3 (CLOUD COMPUTING) ADVISER
College of Computing and Information Sciences

TABLE OF CONTENTS

LIST OF FIGURES

Definition of Terms

This section of the paper clarifies important terms used to enhance understanding of the different concepts within the overall project.

Social media websites and applications that enable users to create and share content or to participate in social networking.

Mobile Application software application developed specifically for use on small, wireless computing devices, such as smartphones and tablets, rather than desktop or laptop computers.

Bullying Refers to repetitive, intentional hurting of one person or group by another person or group, where the relationship involves an imbalance of power.

Cyberbullying Refers to bullying through digital technologies.

Complainant Refers to someone who makes a complaint in a legal action or proceeding.

Complainee Refers to the individual against whom the complaint is made.

University Refers to institutions of higher education that has the authority to award bachelor's and higher degrees, usually having research facilities.

Logistic Regression Algorithm Refers to the statistical method used to model the probability of a binary outcome given an input variable.

Datasets are collections of related sets of information that are composed of separate elements but can be manipulated as a unit by a computer.

Flutter Refers to Google's portable UI toolkit for crafting beautiful, natively compiled applications for mobile, web, and desktop from a single codebase.

Laravel is a free and open-source PHP framework that provides a set of tools and resources to build modern PHP applications.

Node.js is an open-source, cross-platform.

JavaScript runtime environment that executes JavaScript code outside of a web browser.

Python is the easiest and most useful programming language.

Accuracy is a metric that measures how often a machine learning model correctly predicts the outcome.

Summarizes the predictive performance of a model on a binary classification task.

Precision is a metric that tells us about the quality of positive predictions.

Recall in this context is defined as the number of true positives divided by the total number of elements that belong to the positive class

Classification is the action or process of classifying something according to shared qualities or characteristics.

Project Context

Social media today can be regarded as transformative, playing a crucial role in the daily lives of individuals. According to Valerie Forgeard, Social media is a big part of our lives. It has become how we sometimes communicate with others and even ourselves. We rely on social media to keep up with friends, family, and what's happening worldwide. Social Media impacts our lives in many ways, but it can also be detrimental if used incorrectly or too much. (Brilliantio, 2022) From the moment people wake up until they go to bed, platforms like Facebook, Twitter, and Instagram have become integral to their routines. However, this continuous engagement also introduces negative consequences, such as inappropriate use and the rise of bullying, commonly referred to as cyberbullying. The increasing prevalence of these incidents presents a valuable opportunity for in-depth research on cyberbullying cases at the University of Makati, highlighting the need for awareness and effective intervention strategies.

Despite the various types and cases of bullying, this study specifically focuses on the development of a mobile application that can be used by students, staff, and professors of the University of Makati to report incidents of cyberbullying they experience or witness. This research is solely focused on cases of cyberbullying; however, it will also emphasize testing an algorithm designed to classify incident reports and determine whether they can be classified as cyberbullying.

This research aims to address the core problem of cyberbullying by developing a mobile application called Bullyproof, which will be used for reporting incidents. The purpose of this application is to investigate and take action on each reported incident.

Through this, the researchers aim to empower cyberbullying complainants by giving them the courage and strength to reveal their experiences using Bullyproof.

According to Martina Ćorić and Ana Kaštelan Bullying is an aggressive, intentional act carried out by a group or an individual against a complainant who cannot easily defend himself or herself.(Psychiatr Danub, 2020) and indicates that people who are targets of cyberbullies can be adversely affected physically and mentally. However many people who experience cyberbullying may keep quiet out of embarrassment, fear, or shame. (Psych mental, 2020) According to these studies, cyberbullying has a significant impact on every complainant who experiences it, highlighting the need to take action for each complaint. Furthermore, the studies we have gathered Regarding this issue show that the Center for Student Formation and Discipline (CSFD) is interested in this study on cyberbullying occurring as to why cases of cyberbullying continue to rise. The impact on complainants is serious, as it can have various harmful consequences. As a result, the researchers' target, the University of Makati, may struggle to address or take action on every incident occurring within the university. To tackle this problem, the development of “Bullyproof” aims to assist complainants in reporting their experiences and help the University of Makati investigate and take action on each case reported by complainants.

Objective

The general objective of the study is to design and develop "Bullyproof," a mobile application aimed at helping complainants of cyberbullying at the University of Makati. The Logistic Regression Algorithm will be used to assist the Center for Student Formation and

Discipline in classifying whether cyberbullying has occurred based on the incident details submitted by complainants.

Specific Objectives

To fulfill the main objective of this project, the researchers constructed the following specific objectives:

1. Understand the capability of Bullyproof and how it can help complainants of cyberbullying at the University of Makati by investigating each report through the mobile application.

2. Explore existing systems or applications that are relevant to reporting cyberbullying incidents.

3. Train and evaluate the Logistic Regression Algorithm using the Confusion Matrix Metric.

4. Train and evaluate the Logistic regression Algorithm using the following evaluation metrics

   a. Accuracy

   b. Precision

   c. Recall

   d. F1 Score

5. Design and develop a mobile application and website with the following key features:

Mobile Application

A. User Authentication - User Authentication ensures that only authorized users can access the system. Users must create an account by providing their full name, umak email, contact number, and password. This function protects user data and ensures that only verified users can report an incident.

B. Report Incident - The Report Incident feature allows users to report cyberbullying incidents through the mobile app. Complainants can give detailed information, such as the people involved, what happened, and any evidence like screenshots. This helps ensure accurate and thorough reporting.

C. Real-time Notification - With Real-time Notification, complainants are instantly notified about updates on their reports. They receive alerts when their report status changes, and they can delete or mark notifications as read. This ensures users stay updated on the progress of their cases.

D. History of Incident Reports - The History of Incident Reports function allows users to view all their submitted reports. They can see details such as submission dates, current statuses, and the evidence they provide. This feature helps users track the progress of each case over time.

E. Image-to-text - Image-to-text conversion simplifies the reporting process by allowing complainants to upload images containing text, such as screenshots of online messages, and convert them into readable text. This saves time and makes reporting more efficient.

F. Profile Management - With Profile Management, students, staff, professors, directors, and admin can update their account details, such as their name, contact information, and password. This ensures users have control over their information and can keep their profiles up to date.

Web Application

A. Incident management - Incident Management allows the director and admin to access and manage all submitted reports. Admins can filter reports by status, date, or people involved, view detailed information, update statuses, and export reports in CSV or XLSX formats. They can also review evidence such as uploaded screenshots.

B. Email Content Management - The director and admin can create custom email content for complainants and complainees. This includes notifications for scheduled, rescheduled, or canceled appointments, ensuring clear communication throughout the process.

C. Appointment management - The director and admin can schedule appointments between complainants and complainees to discuss incidents. They can set the start time, end time, and date, as well as monitor and update the status of these appointments.

D. Automated Appointment Email Notifications - Complainants and complainees automatically receive email notifications about scheduled, rescheduled, or canceled appointments, ensuring timely updates.

E. Dashboard - The Dashboard provides admins with key statistics, including the total number of users, incidents reported, reports under investigation, resolved cases, and reports awaiting confirmation. It also includes monthly reports and a bar chart showing incidents by platform.

F. Appointment History Tracking - The director and admin can view a complete history of all appointments. This feature allows filtering by date range or appointment status for easy reference.

G. Calendar Scheduler - The Calendar offers a monthly, weekly, or daily view of scheduled appointments. It provides detailed information about the involved parties and helps admins manage schedules efficiently.

H. Complainee Information Management - The director and admin can manage complainee information, including ID numbers and remarks. They can also view all incidents involving a particular complainee and track the number of incidents they've been associated with.

I. Users Management - The director has the ability to activate or deactivate user accounts, especially in cases where users misuse the application. This ensures a safe and secure environment.

J. Admin Account Management - The Director can create and manage staff accounts, ensuring proper access control and delegation of responsibilities.- Admins and users can update their details, including contact information and passwords. This feature ensures that user profiles are always up-to-date and secure.

K. Profile Management - The director, staff, and users can update their details, including contact information and passwords. This feature ensures that user profiles are always up-to-date and secure.

L. Audit Trail - The director can view who logged in and who logged out on the application.

6. Test the system using a set of metrics:

A. Functionality

B. Performance efficiency

C. Flexibility

D. Portability

7. Evaluate the Bullyproof using some of the criteria in ISO 25010:

A. Functional Suitability

B. Interaction Capability

C. Maintainability

D. Flexibility

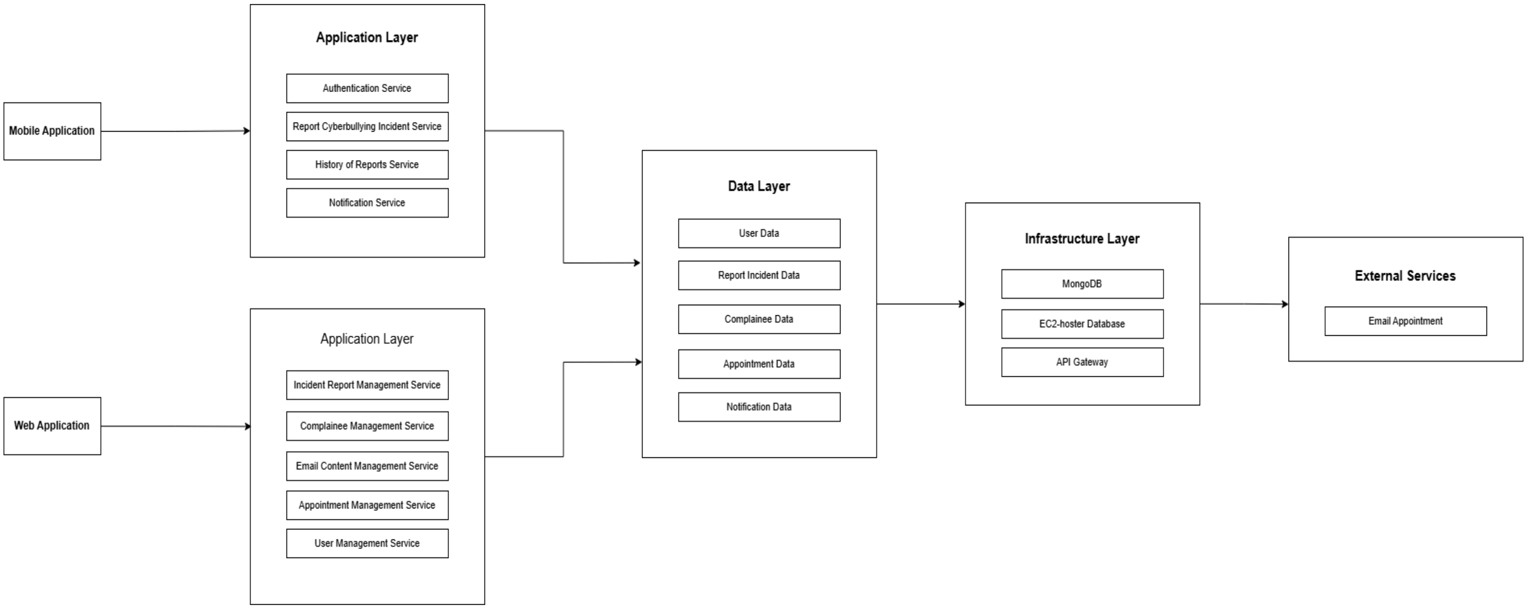
8. Implement and deploy the system.

Structure of the System

The system structure of BullyProof encompasses the complete process of reporting and managing cyberbullying incidents. It integrates key components such as user interaction through the mobile app, data processing via a machine learning algorithm, real-time classification of reports, and seamless data storage and retrieval using MongoDB. The admin web platform allows university administrators to manage incidents efficiently, all hosted on a scalable AWS EC2 instance to ensure reliable system performance.

Figure 1.

System Structure



The software architecture consists of three main components: the Mobile Application, the Web Application, and the underlying Infrastructure Layer.

1. **Mobile Application**

- This is the front-end application that users (students, professors, staff) will interact with on their mobile devices.
- It provides the following services:
  - Authentication Service: Handles user authentication and authorization.
  - Report Cyberbullying Incident Service: Allows users to report cyberbullying incidents.
  - History of Reports Service: Provides a history of reported incidents.
  - Notification Service: Sends notifications to users regarding their reported incidents or related updates.

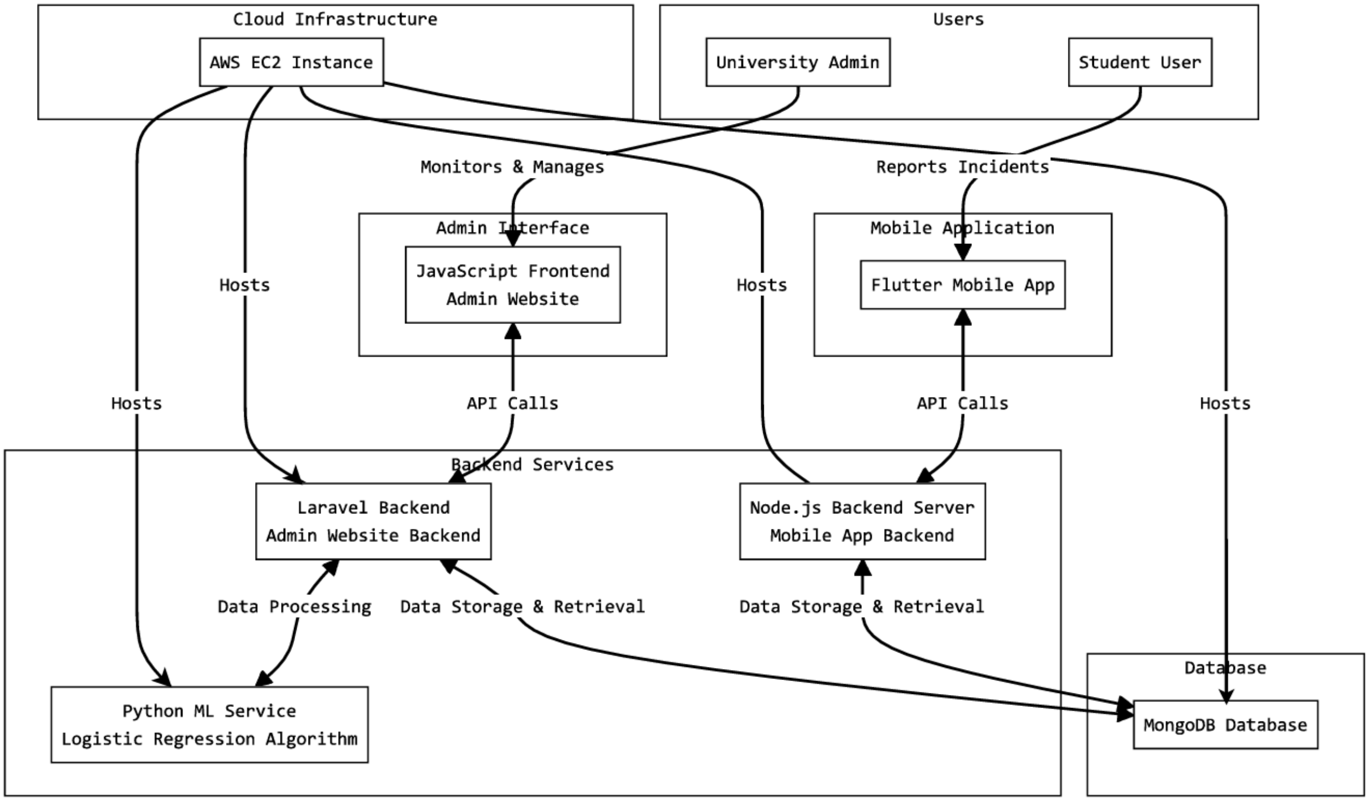
2. **Web Application:**
   - This is the admin-facing application that allows authorized personnel to manage the system.
   - It provides the following services:
     - **Incident Report Management Service** - Allows administrators to view, manage, and update status reported cyberbullying incidents.
     - **Complainee Management Service** - Enables administrators to manage complainee-related data and actions.
     - **Email Content Management Service** - Allows administrators to create and manage email content for appointment-related notifications.

        - **Appointment Management Service** - Facilitates the scheduling and management of appointments between complainants, complainees, and the relevant departments.
        - **User Management Service** - Allows director to create an account for the other admin and manage user accounts, including enabling and disabling them.

3. **Infrastructure Layer**
    - This layer provides the underlying data storage and communication services for the application.
    - It includes the following components:
        - **MongoDB** - A NoSQL database used to store the application's data, such as user information, incident reports, appointment details, and notification data.
        - **EC2 (Elastic Compute Cloud) -** A cloud-based computing service that hosts the web application and API gateway.
        - **API Gateway** - Provides a unified entry point for the web application to access the various services and data sources.

Figure 2.

Software Architecture



Frontend

The front end of BullyProof is developed using **Flutter**, a framework powered by **Dart**, which enables a smooth and responsive user experience for both Android and iOS users. The mobile app allows students to report bullying incidents efficiently and interact with key features of the system.

Key Features of the Frontend:

- **Cross-Platform Compatibility:**

  The single codebase developed in Flutter ensures seamless operation across Android

- and iOS devices, reducing development time and maintaining consistent design and performance.

- **User-Friendly UI/UX Design:**
  The app employs modular, reusable widgets, allowing for highly customizable interfaces. It incorporates intuitive navigation through bottom navigation bars, forms, and incident submission workflows to enhance usability.
- **State Management:**
  The app utilizes state management solutions like **Provider**, **Riverpod**, or **Bloc** to efficiently handle real-time state changes such as new incident submissions, user profile updates, and notifications.

Backend

The backend for BullyProof is developed using **Node.js**, handling the core logic, incident processing, and API interactions. It facilitates data management, algorithm execution, and communication between the front end and the database.

Key Features of the Backend:

- **Incident Classification via Machine Learning:**
  The **Python ML Service** integrates a **Logistic Regression Algorithm**, hosted on **AWS EC2**, to classify reports into various levels of severity, ensuring that high-priority cases receive prompt attention.
- **Data Processing and Storage:**
  The backend processes incident data validates reports, and interacts with the **MongoDB database** for data storage and retrieval.
- **API Endpoints for Mobile App Integration:**
  The Node.js backend provides RESTful API endpoints to manage user authentication, incident reporting, and real-time notifications.

Database

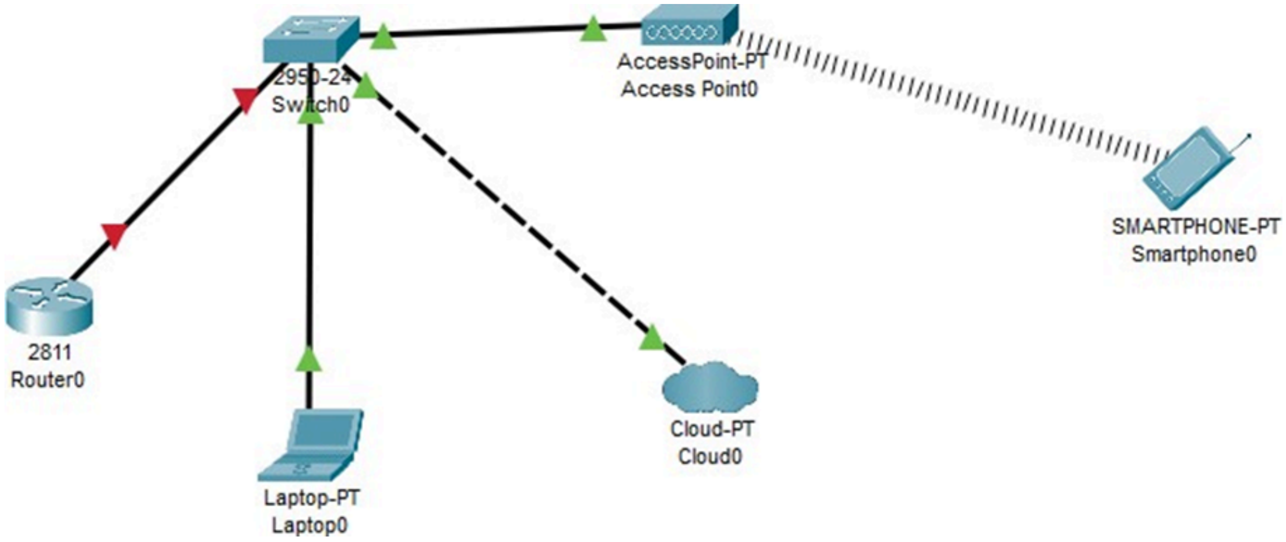
The **MongoDB Database** serves as BullyProof's core storage system. It is optimized for handling structured data related to users, incident reports, and system logs.

Key Features of the Database:

- **NoSQL Data Storage:**
  MongoDB stores structured and semi-structured data such as user profiles, incident details, and historical records of bullying incidents.
- **Scalability and Reliability:**
  MongoDB offers high scalability and ensures real-time synchronization between the mobile application, administrative website, and backend processes.

Figure 3.

Network Architecture



The network diagram represents the infrastructure for the BullyProof

The key components are:

1. **Router** - This is the main router that connects the various devices and services in the network.
2. **Access Point** - This wireless access point provides network connectivity, allowing mobile devices like smartphones to access the system.
3. **Cloud** - This represents a cloud-based service, likely a MongoDB database, that is used to store and manage the data collected by the BullyProof mobile application.
4. **Laptop** - This is a laptop computer, potentially used by developers or administrators to access and manage the system.

5. **Smartphone** - This is a smartphone or mobile device running the BullyProof mobile application, which allows users to report cyberbullying incidents.

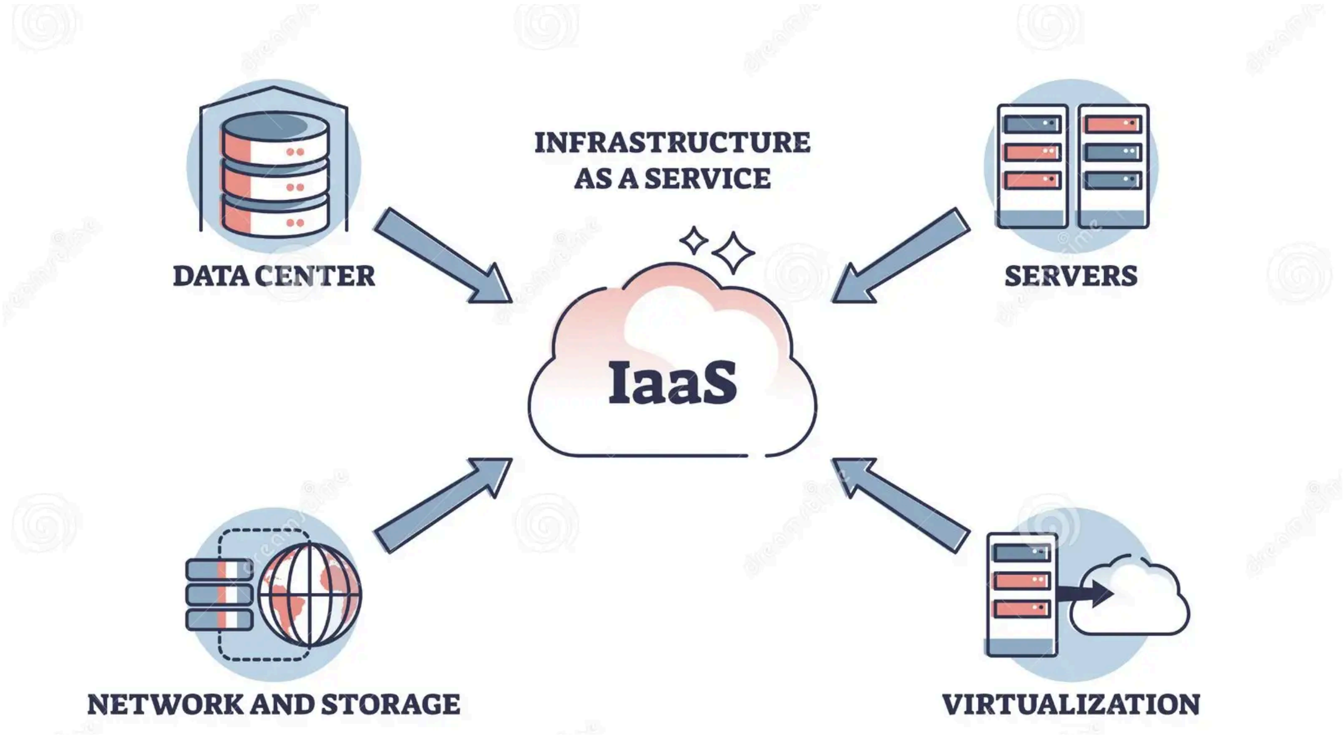
The network setup enables the mobile application to securely communicate with the MongoDB database hosted in the cloud, facilitating the reporting and storage of incidents. This architecture supports the overall project by providing the necessary infrastructure for the mobile application to function and integrate with the backend database system.

Integration of Cloud Computing

IaaS (Infrastructure as a Service) is a cloud computing model where the infrastructure, including virtual machines, networking, storage, and databases, is provided over the internet by a cloud provider. For BullyProof, this model enables the platform to run its backend infrastructure, host its database, and manage cloud storage without investing in or maintaining physical servers. This ensures scalability, flexibility, and cost-efficiency.

Figure 4.

Infrastructure as a Service



IaaS Components for BullyProof

1. Amazon EC2 (Elastic Compute Cloud)

a. Hosts the app's backend services, ensuring reliable performance and scalability for handling user reports and incident data.

b. It provides computing power to run the logistic regression algorithm for analyzing cyberbullying reports and incidents.

c. Enables dynamic scaling, adapting to changes in traffic as more users report incidents or administrators manage data.

2. MongoDB on EC2

a. Hosts the app’s NoSQL database, ensuring quick access to cyberbullying report data, user profiles, and related metadata.

b. Supports complex data storage for unstructured data such as user-generated reports, appointments, and media files.

c. Offers high availability by replicating data across multiple EC2 instances, ensuring uninterrupted access to critical data.

3. Amazon S3 (Simple Storage Service)

a. Provides scalable cloud storage for user-uploaded media, such as screenshots submitted alongside cyberbullying reports.

b. Guarantees durability and availability of media files by storing them across multiple availability zones, ensuring they are safe and easily accessible by both users and administrators.

Use Cases for BullyProof

- **Backend Hosting**
    1. Ensures continuous availability of the app’s core functionalities, including incident submission, report management, and logistic regression analysis for classifying incidents.
    2. Enables easy access for both mobile app users and administrators, ensuring seamless operation across platforms.
- **Data Redundancy**
    1. Maintains backups to protect user-generated reports and media from data loss or corruption.
    2. Replicates data across multiple regions to prevent loss due to hardware failure and ensure data availability at all times.
- **Elastic Scalability**
    1. Accommodates traffic spikes during peak usage times, such as when many users are submitting reports or when administrators are reviewing incidents.
    2. Dynamically scales compute resources to handle increased server demand, ensuring optimal app performance and user experience.

Deployment Models

Deployment models describe how cloud services are implemented and accessed based on organizational needs. For BullyProof, these models ensure that both the mobile app and admin website remain accessible, secure, and cost-effective while providing the necessary infrastructure to report and manage cyberbullying incidents.

1. Public Cloud

a. BullyProof leverages the public cloud for its infrastructure, using services like Amazon EC2, MongoDB, and Amazon S3. These cloud resources are hosted and managed by Amazon Web Services (AWS) and are shared with other organizations.

b. This model ensures cost-effectiveness by utilizing shared resources, offering scalability and flexibility to handle fluctuating workloads, especially during peak times when multiple reports are submitted from both the mobile app and the admin website.

2. Private Cloud

a. For sensitive data, such as personal user information and incident reports, BullyProof utilizes a private cloud environment, where the backend infrastructure is isolated and controlled by the organization.

b. This model ensures data security and compliance with privacy regulations, allowing for a higher level of control over the data storage and processing infrastructure while still taking advantage of cloud scalability.

c. The admin website, which handles the management and review of cyberbullying reports, benefits from the private cloud, ensuring secure access and controlled data handling.

3. Hybrid Cloud

a. BullyProof could use a hybrid cloud model, combining the benefits of both public and private clouds. For example, user data and incident reports could be stored in the private cloud to ensure security, while the computational processes for logistic regression analysis and media storage are handled in the public cloud for better scalability and cost efficiency.
b. This model allows for greater flexibility by enabling BullyProof to scale resources for computing tasks, such as running algorithms while keeping sensitive data secure on the private cloud. Both the mobile app and the admin website can seamlessly work across these environments, ensuring optimal performance and security.

Integration of Multi-Level Cloud Computing

The integration of multi-level cloud computing is a strategic approach that uses Infrastructure as a Service (IaaS) to create a comprehensive, effective, and scalable solution for the development and operation of Bullyproof. This model contributes uniquely to the app's functionality, performance, and reliability.

Infrastructure as a Service (IaaS)

- This model provides the infrastructure, including virtual machines, networking, storage, and databases, to host and manage the app.

Core Components

1. **Amazon EC2**

- **Functionality:** Hosts backend services for the application, ensuring reliable performance and scalability.
- **Role:** Runs algorithms, such as logistic regression, to analyze cyberbullying reports and incidents.
- **Scalability**: Allows dynamic scaling to accommodate varying traffic levels as user reports increase or as administrators manage data.

2. **MongoDB on EC2**

- **Functionality:** Acts as a NoSQL database for storing and accessing cyberbullying report data, user profiles, and related metadata.
- **Data Handling:** Supports complex storage needs for unstructured data, including user-generated content and media files.
- **Availability:** Ensures high availability through data replication across multiple EC2 instances, maintaining uninterrupted access to critical information.

3. **Amazon S3 (Simple Storage Service)**

- **Functionality:** Provides scalable cloud storage for user-uploaded media, such as screenshots related to cyberbullying reports.

- **Data Safety:** Guarantees durability and availability of media files by storing them across multiple availability zones, allowing easy access for users and administrators.

CORS policy

Cross-Origin Resource Sharing (CORS) ensures secure communication between the Bullyproof app and external resources. It defines how resources (such as APIs and data services) hosted on one domain can be accessed from another domain, particularly in web and mobile applications.

For Bullyproof:

- Configuration for Flutter and MongoDB:
    - Cors is configured to allow Flutter (frontend) to securely interact with MongoDB (backend) over HTTPS.
    - Guarantees that requests from the Bullyproof app are verified and valid before being processed by MongoDB.
- Unauthorized Access Prevention:
    - Verifying incoming requests and responses blocks cross-site scripting (XSS) attacks, where harmful scripts try to exploit security flaws.
- User Data Protection:
    - Protects sensitive user data (Reports) by enforcing strict rules during data transfers.
- Error Management:

- Automatically blocks suspicious or unverified requests, reducing potential security threats.

Authentication scheme

Bullyproof uses strong authentication methods to make sure that only authorized users can access its services, safeguarding user accounts and data.

Email/Password Authentication:

- Allows users to register and log in securely using MongoDB Authentication.
- Credentials are encrypted and stored safely to avoid security breaches.

Personal info ng users:

- Allows users to input their personal information securely using MongoDB Authentication.

Reports:

- Allows users to input the incident report securely using MongoDB Authentication.

Token-Based Authentication:

- Tokens expire if there is no activity in the app after 10 minutes.

Security

User Authentication:

- Function: Ensures that only authorized users can access the application.
- Data Security Role: This function protects against unauthorized access by requiring users to create an account with personal information and ensuring that only verified individuals can report incidents.

Report Incident:

- Function: Allows users to report incidents such as cyberbullying.
- Data Security Role: This feature collects detailed information about incidents, including the individuals involved and evidence By documenting incidents accurately, it helps maintain a secure environment where users can safely report issues without fear of retaliation.

Profile Management:

- Function: Allows users to manage their account details.
- Data Security Role: Users can update their names, contact information, and passwords. This control over personal data is essential for maintaining privacy and security within the application, ensuring that users can protect their information from unauthorized access.

Requirements:

Product Requirements

The product requirements outline the key features and functionalities that Bullyproof must incorporate to meet user expectations and deliver a smooth experience.

- **Core Features**
  - **BullyProof App**
    - **User Authentication:** Users can create an account by providing their full name, UMAK email, contact number, and password.
    - **Report Incident:** Allows users to report cyberbullying incidents through the mobile app.
    - **Real-time Notification:** Complainants are instantly notified about updates on their reports.
    - **History of Incident Reports:** allows users to view all their submitted reports.
    - **Image to Text:** Allowing complainants to upload images containing text, such as screenshots of online messages, and convert them into readable text.
    - **Profile Management:** Allow students, staff, professors, director, and admin can update their account details, such as their name, contact information, and password.

- **Admin Website**

  - **Incident management:** allows the director and admin to access and manage all submitted reports.

  - **Email Content Management:** Allow the director and admin to create custom email content for complainants and complainees.

  - **Appointment management:** Allow the director and admin schedule appointments between complainants and complainees to discuss incidents.

  - **Automated Appointment Email Notifications:** Complainants and complainees automatically receive email notifications about scheduled, rescheduled, or canceled appointments, ensuring timely updates.

  - **Appointment History Tracking:** Allow the director and admin view a complete history of all appointments.

  - **Complainee Information Management:** Allows director and admin to manage complainee information, including ID numbers and remarks.

  - **Users Management:** Allow directors to activate or deactivate user accounts, especially in cases where users misuse the application.

        - **Admin Account Management:** Allows the Director to create and manage staff accounts.

        - **Profile Management:** Allow director, staff and users to update their personal details, including contact information and passwords.

        - **Audit Trail:** Allow the director to view who logged in and logged out on the application.

- **Performance**
    - Real-time updates for Incidents, status changes, and notifications.
- **Usability**:
    - Create a simple and easy-to-navigate interface that is suitable for both beginners and experienced users.
    - Make sure the design is responsive and compatible across both iOS and Android platforms.

Organizational Requirements

The organizational requirements focus on ensuring the app aligns with business and operational needs.

- **Team Management**:
    - ○ Provide administrative tools for overseeing user activities, such as task audits, user registrations, and issue resolution.
    - ○ Allow admins to generate reports and monitor system performance.

- **Data Compliance**:
    - Adhere to relevant data protection regulations:
        - Philippine Data Privacy Act for local compliance.
    - Include features for data privacy, such as user data anonymization and consent management.
- **Scalability**:
    - Build an infrastructure that supports the app's growth, allowing it to handle an increasing number of users.
    - Ensure the app can integrate new features without affecting existing functionalities.

External Requirements

external requirements focus on third-party dependencies, legal considerations, and integration capabilities to ensure functionality, compliance, and user safety.

Third-Party Services

1. **Database and Backend Services**:
    - Utilize **MongoDB** for managing core backend functionalities such as incident reporting, user authentication, and secure data storage.
    - Enable real-time data handling for reporting and notification features.
2. **Cloud Services**:
    - Integrate cloud solutions to provide scalable storage for multimedia evidence (e.g., screenshots).
    - Leverage cloud hosting for reliable app performance and availability.

3. **Notification System**:
   - Use third-party notification services (e.g., MongoDB) to alert users about updates on their reports.

Legal Compliance

1. **Licensing**:
   - Ensure all frameworks, libraries, and third-party services used in the app development are properly licensed and adhere to their usage terms.
2. **Privacy and Security**:
   - Develop robust **terms of use** and **privacy policies** that comply with international laws such as the **General Data Protection Regulation (GDPR)** and local regulations like the **Philippine Data Privacy Act (DPA)**.
   - Protect user data by implementing strong encryption and secure access controls.
3. **Accessibility Compliance**:
   - Ensure the app meets accessibility standards (e.g., WCAG) to provide equal usability for all users, including individuals with disabilities.

By adhering to these external requirements, BullyProof will deliver a secure, scalable, and compliant mobile application that effectively addresses UMak's need to manage and mitigate cyberbullying incidents. This ensures that the solution is both user-centric and aligned with organizational and legal standards.

User Manual

Getting Started

BullyProof is a mobile app designed to empower students and faculty of the University of Makati (UMak) by enabling them to report and manage cyberbullying incidents. With user-friendly interfaces and secure backend integration, BullyProof ensures incident reporting is efficient, confidential, and impactful.

System Requirements

- Operating System: Android 8.0+ / iOS 12.0+
- Storage Space: At least 500MB free
- Internet Connection: Required for incident reporting, real-time notifications, and syncing features

Installation Process

1. Download the App

- For Android: Visit the Google Play Store and search for "BullyProof."
- For iOS: Visit the Apple App Store and search for "BullyProof."

2. Install

- Tap Install and wait for the app to download and install on your device.

3. Open

- Launch the app by tapping the BullyProof icon (a shield symbol with a light blue and white theme).

Mobile App

Account Registration

1. Click the **Create account** text on the login screen.
2. Fill in the required details, including full name, email, contact, password and account type.
3. Log in with your new account.

Signing In

1. Enter your registered email and password on the login screen.
2. Click **Login** to access your dashboard.

Features Guide:

Incident Reporting

- Submitting a Report:
  - Go to the Report screen.
  - Agree the data privacy policy.
  - Fill up incident details:
    - Relationship to Complainant

        - Complainant’s Name
        - Complainant’s Role
        - Complainant’s Year Level or Position
        - Complainee’s Name
        - Complainee’s Role
        - Complainee’s Year Level or Position
        - Platform Used for Cyberbullying
        - Any Witnesses
        - Incident Detail
        - Incident Evidence
        - Have you reported the Incident
        - Type of support
    - Agree the above statements are true.
    - Submit the report.
- Image to Text:
    - Click the converted image to text in the report.
    - Select an image to convert.
    - Wait for the process and it will display incident details.

Report History

- Monitor submitted report status.
- View past resolved incident reports.

Real-Time Notification

- Receive notification about status changes in your submitted report.
- Mark as read, delete or mark all as read a notification by tapping or sliding.

Profile Management

- Update profile details, including your name, contact and profile picture.
- Update your password if needed.

Troubleshooting

Common Issues and Solutions

1. **Cannot Log In**:
   - Ensure your email and password are correct.
   - Reset your password if necessary.
2. **History Not Syncing**:
   - Check your internet connection.
   - Ensure you're logged into the correct account.
3. **App Crashes**:
   - Restart the app.
   - Update to the latest version via the app store.

System Requirements for Admin Website

1. Hardware Requirements

- **Processor:**
  - Minimum: 2.0 GHz dual-core processor.
  - Recommended: 3.0 GHz quad-core processor or better for improved performance.
- **RAM:**
  - Minimum: 4 GB RAM.
  - Recommended: 8 GB RAM or higher for handling multiple users and heavy operations.
- **Storage:**
  - Minimum: 10 GB of free disk space (for the website's base and database).
  - Recommended: 20 GB of free disk space or more, depending on the number of records and files stored in MongoDB.
- **Network:**
  - Stable internet connection (required for accessing the web app and connecting to external services like email).

Website Access Process for Admins

1. Open the Browser

- Action: Open your preferred web browser (e.g., Google Chrome, Mozilla Firefox, Safari).
- System Response: The browser is ready to navigate to any website.

2. Visit the Website URL

- Action: Enter the Admin Website URL http://ec2-43-207-119-154.ap-northeast-1.compute.amazonaws.com/ in the browser's address bar.
- System Response: The browser loads the Admin Login Page

Web Application

Signing In

1. Enter your registered email and password on the login screen.
2. Click **Login** to access your dashboard.

Dashboard

- Total Users - The total number of users in the system.
- Total Incidents Reported - The total number of cyberbullying incidents that have been reported.
- Total Resolved Incidents - The number of reported incidents that have been resolved.
- Waiting for Confirmation - The number of incidents that are pending confirmation.

- Total Review Report - The number of review reports that have been submitted.
  - You can filter the data shown on the dashboard by clicking the "Filters" button in the top right. This allows you to set a start and end date range to view data for a specific time period.
  - Number of Reports - This section displays a line chart showing the number of reported incidents over time. This can help you identify trends and patterns in the data.
  - Cyberbullying Platforms The dashboard also shows a bar chart that breaks down the number of incidents reported by the platform (e.g., social media, messaging apps) where cyberbullying occurred.

Incidents Report

1. Incident Report List - The Incidents Report section displays a list of all reported incidents, showing key details such as the date filed, complainant name, complainee name, and status of the incident.
2. Incident Report Details - Click view on a specific incident report allows you to view all the details of that report, including the complainant's information, the complainee's information, and a description of the incident.
3. Incident Report Form - The Incident Report form allows you to see the submitted new cyberbullying incidents, capturing details like the date/time, complainant info, complainee info, incident description, and any actions taken.
4. Incident Evidence - For certain incidents, you can review evidence submitted by complainants, such as screenshots or chat logs, to help document the cyberbullying case.

5. Cyberbullying Analysis - The platform can analyze the incident details and provide a cyberbullying detection result, along with the probability that the incident is a genuine case of cyberbullying.

Using the Incident Reporting Management

1. **Viewing the Incident Report List**
    - Access the "Incidents Report" section from the left-hand menu.
    - This will display a table showing all the reported cyberbullying incidents.
    - You can filter the list by status (All, Under Investigation, Resolved) using the dropdown.
    - To view details of a specific incident, click on the corresponding row.
2. **Reporting a New Incident**
    - From the left-hand menu, select "Incidents Report".
    - Click the "New Incident" button to access the incident report form.
    - Fill out the complainant's information, complainee's information, and details about the incident.
    - Optionally, you can upload any relevant evidence files.
    - Click "Save" to submit the new incident report.
3. **Viewing Incident Report Details**
    - From the Incidents Report list, click on a specific row to view the details of that incident.
    - This will show you the complainant's information, the complainee's information, and all the details about the reported incident.

- Review the "Actions Taken" and "Incident Evidence" sections to see the progress and status of the case.

4. **Analyzing Cyberbullying Evidence**
    - If the incident report includes uploaded evidence files, the platform will analyze the content and provide a cyberbullying detection result.
    - This analysis includes the probability that the incident is a genuine case of cyberbullying.
    - Use this information to help assess the validity of the reported incident and determine the appropriate next steps.

Using the Email Content Management

This page allows you to compose email content for various scenarios related to appointment management.

The key user actions and flows observed are:

1. **Composing Email Content**
    - You can enter and format the email content using the rich text editor provided on the page.
    - The editor supports basic formatting options like bold, italic, bulleted lists, etc.
2. **Handling Appointment Scenarios**
    - The page has sections for different appointment-related scenarios, such as Complainants, Complainee, Cancelled Appointment, and Reschedule Appointment.

- You can compose email content specific to each of these scenarios.

3. **Saving Email Content**
    - After composing the email content, you can save it by clicking the "Save Content" button at the bottom of the page.
4. **Navigating Between Scenarios**
    - You can switch between the different appointment-related scenarios using the tabs or links at the top of the page.

Using the Appointment Management

1. **Viewing the Appointment Calendar**
    - You can access the "Appointment" section of the application.
    - This section displays a calendar view of the appointments for the month
    - The calendar shows the daily schedule, including time slots for appointments.
    - The calendar also displays various status badges for the appointments, such as Waiting for Confirmation, Approved, Rescheduled, Cancelled, Missed, and Done.
2. **Scheduling a New Appointment**
    - You click the “New Appointment" button to create a new appointment.
    - This opens a modal window where you can enter the details of the new appointment.
    - You must provide the Complainee Name, Complainee Email, Complainant Name, Complainant Email, Department of the Complainee and Complainant, Appointment Date, Start Time, and End Time.

- After filling out the required information, the user can click the "Submit Appointment" button to save the new appointment.

3. **Viewing Appointment Details**
    - You can access the appointment calendar view, which shows the scheduled appointments for the month.
    - When you click on a specific appointment block in the calendar, a modal window appears displaying the details of that appointment.
4. **Accessing Appointment Information**
    - The modal provides key information about the appointment, such as the complainant, complainee, their email addresses, the appointment status, and the date and time.
    - This allows the user to quickly view the relevant details of the scheduled appointment.
5. **Closing the Details View**
    - You can close the appointment details modal by clicking the "Close" button.
    - This returns the user to the main appointment calendar view.

Using the Appointments Summary

The Appointment Summary table displays a list of scheduled appointments over a specific date range. Each appointment has several details associated with it, including the appointment date and time, the respondent's name and email, the complainant's name and email, and the current status of the appointment.

You can filter the appointments by status (e.g., All, Missed, Cancelled, Approved, Waiting for Confirmation) and view the appointments within a specific date range. You can also search for appointments using the search bar.

The key interactions and functionality for the user would include:

1. Viewing the list of scheduled appointments and their details.
2. Filtering the appointments by status to quickly identify the appointments with specific statuses (e.g., Missed, Cancelled, Approved).
3. Searching for specific appointments using the search bar.
4. Updating the status of an appointment (e.g., marking as Approved, Cancelled, or Rescheduled).
5. Navigate to additional pages of appointments if there are more than 10 entries displayed.

Troubleshooting

1. Login Issues

Issue - Cannot login with valid credentials.

- **Possible Causes:**
    - Incorrect username or password.
    - Session issues (session expired or corrupted cookies).
- **Solutions:**
    - Double-check the credentials and try logging in again.
    - Clear browser cookies and cache, then try again.

Source code

Github BullyProof App Link: https://github.com/yenashiloh/bully_proof_umak

Github BullyProof Backend Link: https://github.com/yenashiloh/bully_proof_backend

Github BullyProof Admin Link: https://github.com/yenashiloh/BullyProofWebsite

BullyProof APK Link:

https://drive.google.com/file/d/1QrSgKCSLPham7R0OhWOShI6GX56rz5yI/view

Admin and Director Credentials on the Website

Admin

- Email - discipline-account@gmail.com
- Password - adminpassword

Director

- Email **-** super-admin@gmail.com
- Password - adminpassword

Developers Profile

Shiloh B. Eugenio
Project Manager/Lead Programmer

Paul Angelo Derige
Cloud Specialist/Programmer

Jade Daniele M. Bantilo
UI&UX Designer

Ryan P. Corda
Document Specialist/Researcher

Project Manager: Oversees the entire project, ensuring that timelines, resources, and deliverables are met.

Programmer: Responsible for coding the app, ensuring it runs smoothly, and implementing the required algorithms.

Cloud Specialist: Manages the cloud services used in the app, ensuring that data is securely stored, backed up, and that the app runs smoothly on the cloud infrastructure.

Document Specialist: Responsible for preparing documentation for the project, ensuring that both technical and non-technical stakeholders have the necessary information.

Researcher: Gathers relevant information, conducts studies, and provides insights to improve the app's functionalities and algorithms.

UI/UX: Focuses on creating an intuitive and aesthetically pleasing user interface and ensuring a smooth user experience.

Contact Information:

Email:

paulangelo.derige@gmail.com

shiloheugenio21@gmail.com

ryancorda123@gmail.com

jadedanbantilo15@gmail.com

Github:

https://github.com/yenashiloh

https://github.com/CodeAce36