Cybercrime Incident Management & Awareness System

Adithayan AS Adwin T Sunil Evaan Antony Philip

August 13, 2025

Index

Objective

- Provide a secure, centralized platform for reporting, tracking, and managing cybercrime incidents.
- Facilitate collaboration between victims, investigators, and administrators.
- Raise public awareness on safe online practices.

Frontend Features

- **Incident reporting with evidence upload:** Victims can file reports and attach documents, images, or videos for investigation.
- **Awareness Hub for educational content:** Provides articles, guides, and safety tips to promote digital literacy.
- **Role-based dashboards for different users:** Customized interfaces for victims, investigators, and admins to view relevant data and tasks.
- **Crime mapping and statistics:** Visualizes incident locations and trends for better situational awareness.
- **Notification system:** Sends real-time alerts to users when their case status changes or new awareness updates are published.
- **Responsive UI using React & JavaScript:** Ensures smooth, accessible, and visually appealing experience across all devices.

Backend Components

- **User authentication and role-based access control:** Ensures that only authorized users can access specific features based on their role.
- **PostgreSQL database with Django backend:** Provides a scalable and reliable database solution powered by a robust web framework.
- **Secure file handling & password hashing:** Protects sensitive user data and uploaded evidence using encryption and hashing algorithms.
- **Analytics for location-based crime trends:** Processes incident data to generate insights and highlight high-risk areas.

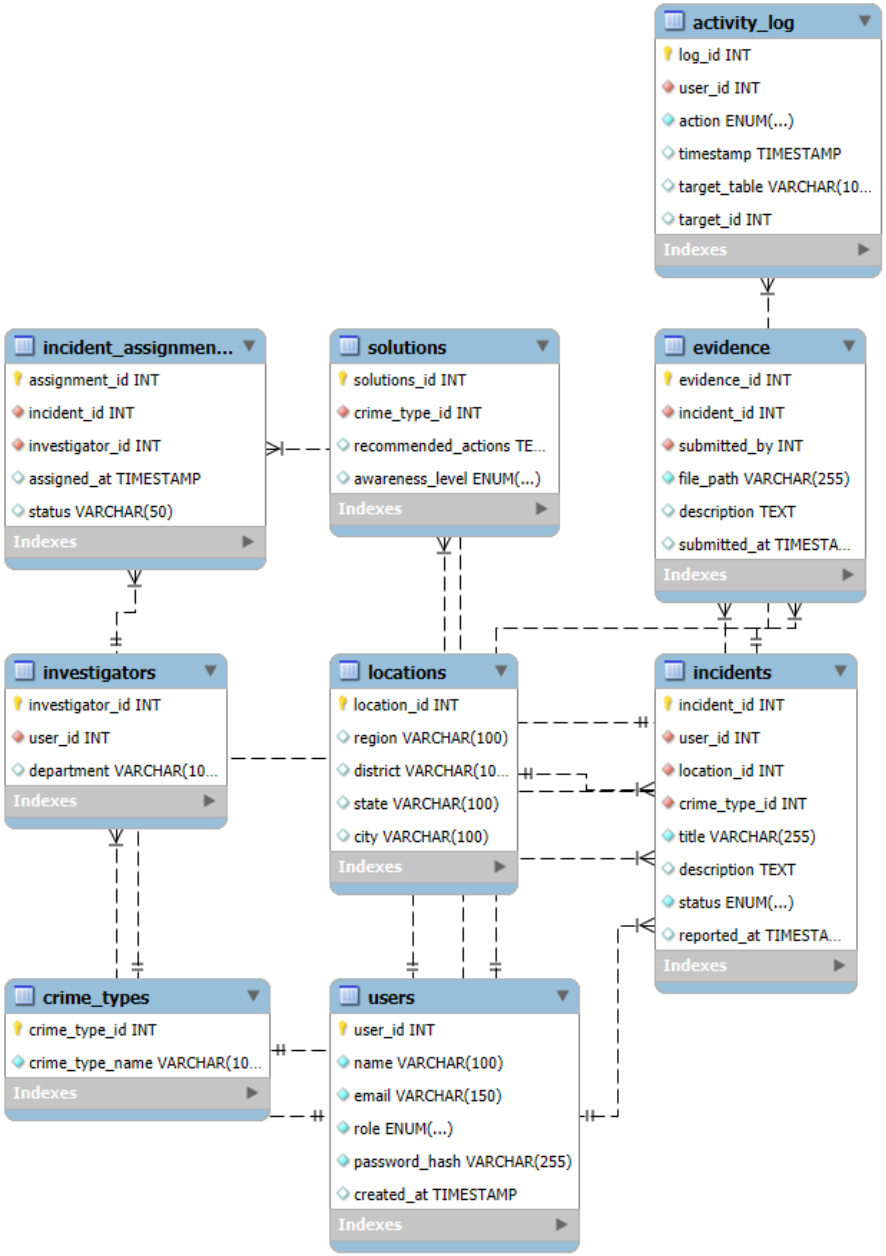
Abstract

The project aims to develop a secure and centralized platform for cybercrime incident management. CIMAS enables victims to submit complaints and evidence, while investigators can manage cases and track progress. It offers location-based analytics and an Awareness Hub for public guidance. Built with React, JavaScript, Django, and PostgreSQL, the system ensures security via password hashing, access control, and safe file handling. Core features include reporting, case tracking, crime mapping, and awareness content.

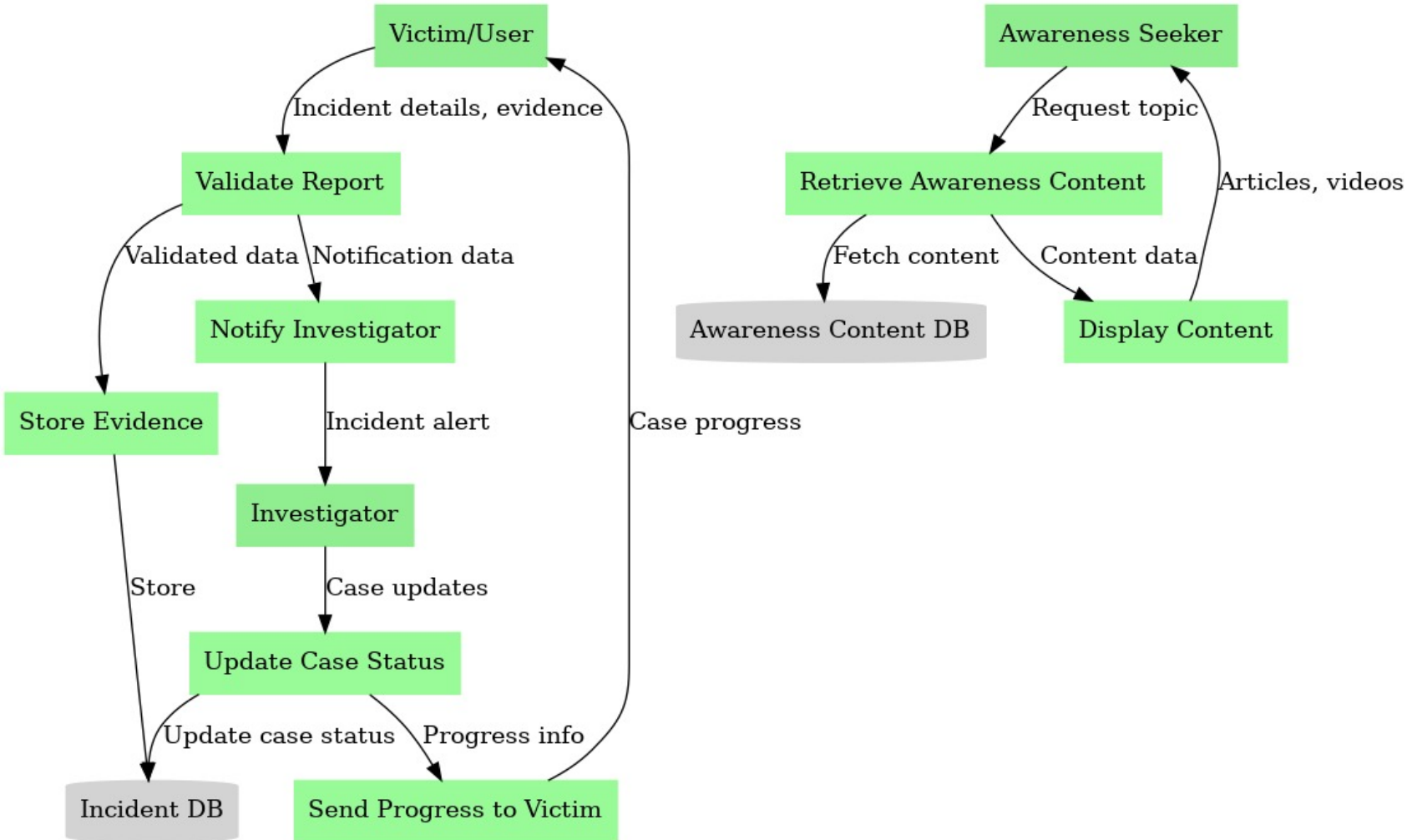
Module Description

1. **User Management Module:** Handles registration, authentication, and role-based access for system users.
2. **Incident Reporting Module:** Enables users to submit, track, and manage crime incident reports.
3. **Evidence Management Module:** Stores, organizes, and secures digital and physical evidence records.
4. **Case Assignment Module:** Assigns reported cases to investigators based on workload and expertise.
5. **Activity Logging Module:** Records all system activities for security, auditing, and accountability.
6. **Crime Analytics Module:** Analyzes incident data to identify patterns, trends, and hotspots.
7. **Awareness & Solutions Module:** Provides educational resources and preventive measures against crimes.

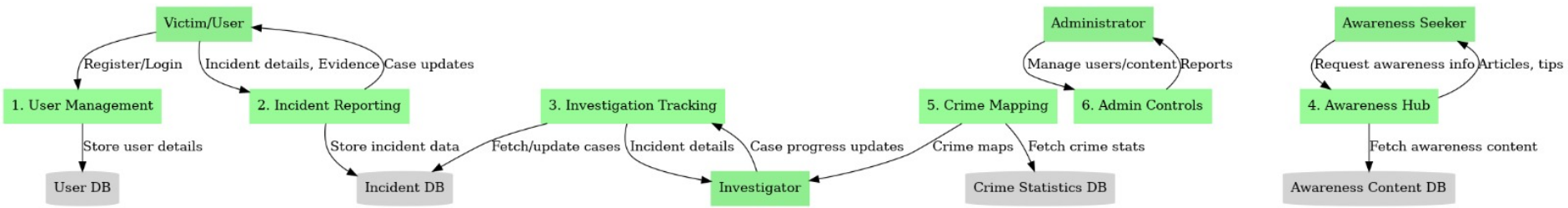
ER Diagram


activity_log
log_id INT
user_id INT
action ENUM(...)
timestamp TIMESTAMP
target_table VARCHAR(10...
target_id INT
Indexes
incident_assignmen...
assignment_id INT
incident_id INT
investigator_id INT
assigned_at TIMESTAMP
status VARCHAR(50)
Indexes
solutions
solutions_id INT
crime_type_id INT
recommended_actions TE...
awareness_level ENUM(...)
Indexes
evidence
evidence_id INT
incident_id INT
submitted_by INT
file_path VARCHAR(255)
description TEXT
submitted_at TIMESTA...
Indexes
investigators
investigator_id INT
user_id INT
department VARCHAR(10...
Indexes
locations
location_id INT
region VARCHAR(100)
district VARCHAR(10...
state VARCHAR(100)
city VARCHAR(100)
Indexes
incidents
incident_id INT
user_id INT
location_id INT
crime_type_id INT
title VARCHAR(255)
description TEXT
status ENUM(...)
reported_at TIMESTA...
Indexes
crime_types
crime_type_id INT
crime_type_name VARCHAR(10...
Indexes
users
user_id INT
name VARCHAR(100)
email VARCHAR(150)
role ENUM(...)
password_hash VARCHAR(255)
created_at TIMESTAMP
Indexes

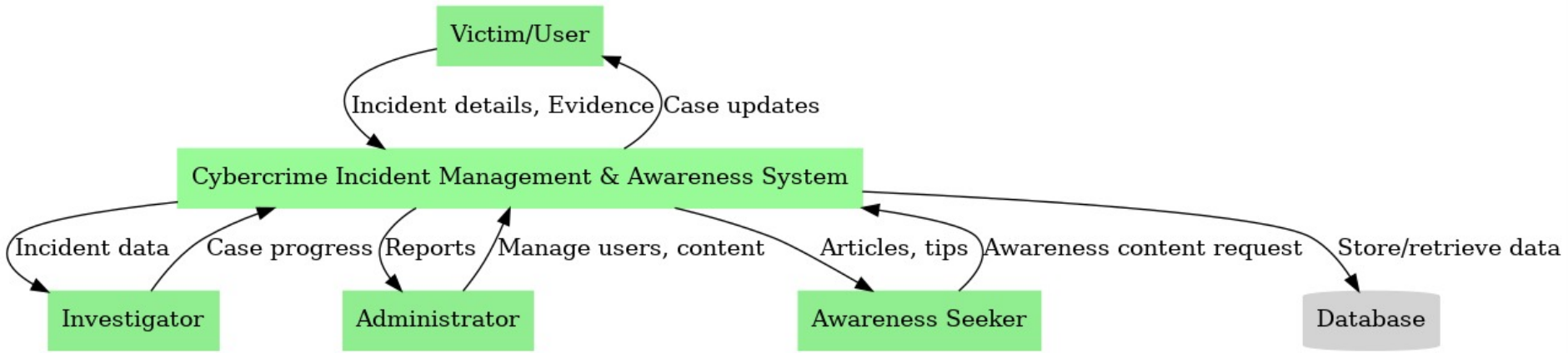
DFD Level 0


Victim/User
Incident details, evidence
Validate Report
Validated data
Notification data
Notify Investigator
Store Evidence
Incident alert
Investigator
Store
Case updates
Update Case Status
Update case status
Progress info
Incident DB
Send Progress to Victim
Case progress
Awareness Seeker
Request topic
Retrieve Awareness Content
Articles, videos
Fetch content
Content data
Awareness Content DB
Display Content

DFD Level 1


Victim/User
Register/Login
Incident details, Evidence
Case updates
1. User Management
2. Incident Reporting
Store user details
Store incident data
User DB
Incident DB
3. Investigation Tracking
Fetch/update cases
Incident details
Case progress updates
Investigator
Administrator
Manage users/content
Reports
5. Crime Mapping
6. Admin Controls
Crime maps
Fetch crime stats
Crime Statistics DB
Awareness Seeker
Request awareness info
Articles, tips
4. Awareness Hub
Fetch awareness content
Awareness Content DB

DFD Level 2


Victim/User
Incident details, Evidence
Case updates
Cybercrime Incident Management & Awareness System
Incident data
Case progress
Reports
Manage users, content
Articles, tips
Awareness content request
Store/retrieve data
Investigator
Administrator
Awareness Seeker
Database

Conclusion

- CIMAS improves cybercrime reporting, investigation, and awareness.
- Strong security and role-based workflows enhance trust.
- Future: AI crime detection, blockchain evidence verification, mobile app.