A Synopsis of Project on

E-Raksha: Your Personal Safety Companion with Real-Time GPS Tracking

Submitted in partial fulfillment of the requirements for the award
of the degree of

Bachelor of Engineering

in

Computer Science and Engineering-Data Science

by

Sanchit Patil(21107001)
Himanshu Maurya(21107038)
Faizan Mahimkar(21107007)
Harshal Patil(21107060)

Under the Guidance of

Prof. Rajashri Chaudhari

Department of Computer Science and Engineering-Data Science
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W)-400615
UNIVERSITY OF MUMBAI

Academic Year 2024-2025

Approval Sheet

This Project Synopsis Report entitled ***"E-Raksha: Your Personal Safety Companion with Real-Time GPS Tracking"*** Submitted by ***"Sanchit Patil" (21107001), " Harshal Patil" (21107060),"Faizan Mahimkar" (21107007),"Himanshu Maurya" (21107038)***is approved for the partial fulfillment of the requirement for the award of the degree of ***Bachelor of Engineering*** in ***Computer Science and Engineering-Data Science*** from ***University of Mumbai***.

Prof. Rajashri Chaudhari
Guide

Prof. Anagha Aher
HOD, Computer Science and Engineering-Data Science

Place:A.P.Shah Institute of Technology, Thane
Date:

CERTIFICATE

This is to certify that the project entitled ***"E-Raksha: Your Personal Safety Companion with Real-Time GPS Tracking"*** submitted by ***"Sanchit Patil" (21107001), "Harshal Patil" (21107060), "Faizan Mahimkar" (21107007), "Himanshu Maurya" (21107038)*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Computer Science and Engineering-Data Science***,to the University of Mumbai,is a bonafide work carried out during academic year 2024-2025.

Prof. Rajashri Chaudhari
Guide

Prof. Anagha Aher
HOD, CSE(Data Science)

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Internal Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology, Thane
Date:

Acknowledgement

We have great pleasure in presenting the synopsis report on **E-Raksha: Your Personal Safety Companion with Real-Time GPS Tracking** We take this opportunity to express our sincere thanks towards our guide **Prof. Rajashri Chaudhari** for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards his constant encouragement, support and guidance through the development of project.

We thank **Prof. Anagha Aher** Head of Department for his encouragement during the progress meeting and for providing guidelines to write this report.

We express our gratitude towards BE project co-ordinator **Prof. Rajashri Chaudhari**, for being encouraging throughout the course and for their guidance.

We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Sanchit Patil
(21107001)

Harshal Patil
(21107060)

Faizan Mahimkar
(21107007)

Himanshu Maurya
(21107038)

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Sanchit Patil (21107001)

Himanshu Maurya (21107038)

Faizan Mahimkar (21107007)

Harshal Patil (21107060)

Date:

Abstract

In today's world, women's safety remains a pressing concern, underscoring the urgent need for reliable and effective solutions that can address emergency situations swiftly and efficiently. This project presents E-Raksha, a comprehensive women safety system that integrates both software and hardware on an Android platform. By leveraging advanced technologies, E-Raksha aims to empower women to navigate their environments with confidence. The system employs mobile and button cameras for real-time violence detection, coupled with criminal face recognition capabilities, which ensures proactive responses to potential threats. This functionality allows the application to analyze video feeds and identify aggressive behaviors or known offenders, providing timely alerts to users. Moreover, the integration of GPS modules and tags enables precise real-time location sharing, which can be activated by a dedicated hardware button or a smartwatch interface. This feature allows users to send distress signals to designated contacts or emergency services without drawing attention to themselves, a critical function in high-risk situations. E-Raksha not only focuses on immediate safety but also seeks to enhance overall awareness of surrounding environments by analyzing historical crime data and providing users with risk assessments for specific locations. The platform's design prioritizes user-friendly interaction, ensuring that safety features are easily accessible in times of need. Through continuous updates and feedback mechanisms, E-Raksha aims to evolve in response to the changing dynamics of women's safety concerns. Ultimately, this project aspires to contribute to a broader societal shift toward improved safety and empowerment for women, fostering an environment where they can feel secure and supported. By combining cutting-edge technology with practical applications, E-Raksha stands as a potential game-changer in the fight against violence and harassment.

Keywords: Women's safety, violence detection, facial recognition, GPS tracking, emergency response, Android application, real-time monitoring, proactive safety solutions.

Contents

List of Figures

List of Tables

List of Abbreviations

IDS:	Intrusion Detection System
WSN:	Wireless Sensor Network
MANET:	Mobile Ad-Hoc Network
AODV:	Ad-Hoc On-demand Distance Vector Routing
DSR:	Dynamic Source Routing Protocol
NS2:	Network Simulator 2
ACK:	Acknowledgement
AGT:	Agent
RTR:	Router

Chapter 1

Introduction

In India, women's safety remains a critical concern, with increasing reports of violence, harassment, and assault. According to the National Crime Records Bureau (NCRB), crimes against women rose by over 7 percent in 2022, with more than 4.3 lakh cases reported nationwide. While government initiatives like panic buttons in public transport and mobile apps have been introduced, these measures are largely reactive and depend on manual activation, which may fail to provide real-time protection, especially in remote areas where immediate help is scarce. In response, this project introduces E-Raksha, a comprehensive women's safety system that integrates both hardware and software solutions on an Android platform. E-Raksha leverages mobile and wearable camera technology for violence detection, criminal face recognition, and GPS-based real-time location tracking. Activated through a hardware button or smartwatch, the system offers proactive responses, ensuring greater safety for women in both urban and rural areas, even where technology infrastructure may be limited. In addition to its core features, E-Raksha includes advanced machine learning algorithms for recognizing suspicious behavior, allowing for early detection of potential threats before they escalate. The system is also designed to function in low-connectivity areas by utilizing offline data storage and delayed synchronization, ensuring that alerts are sent as soon as a network is available. Moreover, the platform offers integration with law enforcement databases for identifying known offenders through facial recognition, enhancing the speed and accuracy of response. By combining real-time monitoring, immediate alerts, and comprehensive data analysis, E-Raksha aims to create a safer environment for women, offering peace of mind and reliable support even in critical situations.

1.1 Motivation

Addressing Women's Safety is Crucial for:

The motivation for this project is further reinforced by the limitations of existing safety solutions, which are often reactive and heavily dependent on manual intervention. In many cases, women may not have the time or ability to activate emergency measures during a critical moment. The absence of real-time surveillance, automated threat detection, and delayed response from authorities adds to the inefficacy of these tools.

E-Raksha seeks to overcome these challenges by incorporating machine learning algo-

rithms capable of detecting abnormal activities and patterns, allowing for faster and more accurate identification of dangerous situations. Additionally, by using GPS technology and IoT devices such as wearables, the system ensures constant tracking and communication without requiring the user's active input. The goal is to create a comprehensive safety net that not only responds to emergencies but also prevents them through early detection and intervention, giving women a stronger sense of security and control in their everyday lives.

1.2 Problem Statement

Our analysis revealed that many existing safety tools are reactive rather than proactive, often relying on users to manually alert authorities in emergencies. This reliance can lead to critical delays in response times, putting individuals at greater risk. Additionally, most applications have limited detection capabilities, failing to identify potential threats until it is too late. We recognized the need for a solution that not only alerts users but also autonomously detects and responds to dangerous situations in real-time. By integrating advanced technologies such as machine learning algorithms for threat assessment and instant alerts to emergency contacts, our application aims to offer a holistic approach to personal safety. This innovative platform will provide users with maximum safety comfort, ensuring they can navigate their environments with confidence and peace of mind.

Even though there are various applications offering safety measures, none provide a fully comprehensive solution that combines proactive threat detection, real-time response, and autonomous intervention. Existing tools often lack features like continuous monitoring or integration with law enforcement systems, which are crucial for handling emergencies efficiently. Moreover, these applications tend to focus on urban settings, leaving women in rural and remote areas underserved. E-Raksha seeks to bridge this gap by offering a solution that works seamlessly in different environments, regardless of connectivity or infrastructure challenges. The system's ability to autonomously detect threats and take preemptive actions ensures that users are safeguarded in diverse situations, offering a level of security unmatched by other platforms.

1.3 Objectives

- Advanced Facial Recognition for Threat Identification: Our application will utilize cutting-edge facial recognition technology to identify potential threats or individuals of interest in real time. By scanning the environment using the camera on the user's smartphone or wearable device and cross-referencing the captured images against a database of known offenders, the system can quickly alert users to possible dangers. This proactive approach significantly enhances personal safety, as users are informed about threats in their vicinity before a situation escalates. The use of facial recognition also extends to identifying patterns of repeated offenders in specific areas, allowing authorities to take preemptive action in high-risk zones. In combination with local law enforcement databases, this technology provides a powerful tool to prevent crimes before they occur.

- Streamlined and Discreet Distress Signal Feature: The application will include a

streamlined distress signal feature that allows users to quickly and discreetly alert designated emergency contacts or authorities. With just a few taps on the application or by pressing a hardware button integrated into wearables (such as a smartwatch or smart ring), users can instantly send their real-time location, along with an SOS message, without drawing unwanted attention. This is especially vital in situations where vocalizing the need for help may not be safe or feasible, such as during confrontations or in isolated locations. The distress signal will also be coupled with an automatic audio or video recording feature, providing crucial evidence that can be shared with authorities, aiding in faster resolution of incidents.

- Integration with Public Surveillance Networks for Violence Detection: Our system will integrate with existing surveillance camera networks, such as those in public spaces, to detect signs of violence or aggression effectively. By utilizing advanced video analytics powered by machine learning algorithms, the application can analyze real-time footage for aggressive behaviors, such as fighting, erratic movements, or sudden escalations that may indicate confrontations. Once a potential threat is identified, the system will alert nearby authorities, security personnel, and the user, providing real-time video evidence for swift intervention. This capability not only helps protect individuals in public spaces but also contributes to broader community safety by monitoring areas prone to criminal activity. In the long term, the data collected can be used to predict high-risk times and locations, allowing for more efficient deployment of law enforcement resources.

- Seamless Offline Functionality and Connectivity Resilience: Recognizing that not all areas have stable internet connectivity, especially in rural or remote regions, the application will feature offline functionality that stores critical data locally on the device and syncs it with the server once a connection is re-established. This ensures that users are always protected, even when network access is limited. The distress signals, location data, and video or audio recordings are prioritized for storage and automatic transmission as soon as the device reconnects to the network.

- Customizable Safety Zones and Alerts: Users will have the ability to define customizable safety zones using GPS geofencing. When a user enters or exits predefined "safe" or "danger" zones (such as familiar neighborhoods or high-risk areas), the system will trigger automatic alerts to designated contacts or security services. This feature provides an extra layer of protection, particularly for individuals who frequently travel through unfamiliar or potentially unsafe regions.

1.4 Scope

- Our project aims to significantly enhance women's security by creating an integrated safety system designed specifically for real-time protection and proactive threat detection. This system will be built on the foundation of advanced technologies that prioritize user safety and comfort.

- To provide a comprehensive and robust safety solution, our system will integrate multiple critical functions, including violence detection, criminal face recognition, and GPS

tracking. This multi-faceted approach allows users to benefit from various safety features within a single application, streamlining their experience.

- The application will leverage machine learning (ML) and deep learning (DL) technologies to analyze video feeds for violent actions and recognize criminal faces. By implementing sophisticated algorithms, the system can learn from vast datasets to identify patterns indicative of aggressive behavior or potential threats.

- Our integrated safety system will feature location-based mapping using GPS modules, enabling real-time tracking and location sharing. This functionality is crucial for ensuring that users can be quickly located in emergencies, facilitating prompt rescue and intervention efforts.

- The final component of our project is to develop a secure, user-friendly mobile and wearable application that allows users to send distress signals discreetly to authorities or designated contacts. This app will prioritize ease of use, ensuring that users can quickly access safety features without unnecessary complications.

Chapter 2

Literature Review

The literature review for the E-Raksha project provides a comprehensive examination of the existing technologies and methodologies that inform the system's development, focusing on key areas such as violence detection, facial recognition, and SOS signal transmission within IoT systems. Numerous studies highlight the significance of advanced machine learning models, including CNN (Convolutional Neural Networks) and LSTM (Long Short-Term Memory), which have become pivotal in real-time violence detection. For example, Mann Patel (2021) explores the use of CNN-LSTM architectures to capture both spatial and temporal features for identifying violent behavior in video feeds. While effective, such systems face challenges related to video quality, scalability, and the ability to operate across diverse environments . Many existing systems struggle with processing large-scale video feeds, often leading to performance bottlenecks and delays in real-time response, which are critical when dealing with life-threatening situations.

Additionally, research on criminal face recognition reveals significant limitations, particularly when relying on 2D imagery. Studies, such as those by H. M. Rehan Afzal, Suhuai Luo, and M. Kamran Afza (2022), highlight the growing interest in 3D facial reconstruction from single 2D images . These systems are designed to overcome issues such as low image quality, occlusions, and varying lighting conditions, which commonly hinder the performance of 2D recognition systems. However, while 3D approaches improve accuracy, they are often computationally expensive and rely heavily on high-quality inputs, making them impractical for certain real-world applications where high-resolution video footage is unavailable. Furthermore, many face recognition systems do not account for changing facial appearances over time or in cases of partial occlusion, thus reducing their overall reliability in uncontrolled environments like public spaces.

Another critical area of focus in this literature review is the analysis of SOS signal transmission mechanisms in IoT-based safety systems. Rabia Tehseen et al. (2022) conducted an extensive review of IoT architectures that enable SOS signaling through devices such as smartwatches, mobile phones, and wearable SOS buttons . These systems offer valuable features, such as quick distress signal transmission, but are often limited by GPS accuracy and network connectivity issues, especially in rural or indoor environments where signals are weak or unstable. The literature also reveals several gaps in the accuracy, real-time processing capabilities, and overall scalability of current systems. Traditional violence detection models often rely on extensive training datasets to function effectively, which can be a challenge in settings where data privacy or availability is an issue. Additionally, existing systems do not always account for the complexity of real-world environments, where variables like low-light

conditions, video resolution, and occlusion can significantly impact performance. This is particularly evident in studies that assess the effectiveness of smart surveillance systems, which, despite advancements, remain limited by the quality of camera feeds and sensor data . Privacy concerns also arise frequently in the literature, particularly regarding the use of public surveillance networks for violence detection and criminal identification. Researchers like Li Wang and Ahmed Ali (2021) discuss the potential for data misuse and the challenges associated with ensuring privacy while maintaining the efficacy of smart surveillance systems .

A notable limitation across many reviewed works is the reliance on reactive rather than proactive approaches to personal safety. Most IoT-based and video analysis systems are designed to respond after an incident has occurred, rather than preventing or detecting threats before they escalate. This gap highlights the need for more intelligent, predictive systems capable of analyzing patterns and behaviors in real time to identify potential threats early. For instance, studies on wearable sensor-based violence detection, such as those by John Doe and Jane Smith (2021), demonstrate promising results in detecting violent activities based on human movement patterns.

2.1 Comparative Analysis of Recent Studies

While existing research offers valuable insights into violence detection, facial recognition, and SOS signaling, significant challenges remain in terms of real-time processing, accuracy, and scalability. Many current systems struggle with handling real-world variables such as video quality, network connectivity, and diverse environmental conditions. Moreover, the literature emphasizes the need for integrated solutions that combine multiple technologies to provide a more comprehensive and proactive approach to personal safety.

Table 2.1: Comparative Analysis of Literature Survey

Sr. No	Title	Author(s)	Year	Methodology	Drawback
1	Real-Time Violence Detection Using CNN-LSTM	Mann Patel	2021	Deep learning architecture using CNN to extract spatial features and LSTM to capture temporal features for real-time violence detection.	Effectiveness depends on video quality and availability; performance bottlenecks in large-scale feeds.
2	An Overview of Violence Detection Techniques	Conv Company LMT	2022	Survey of violence detection techniques, from traditional feature extraction methods to deep learning models like CNNs and 3D ConvNets.	False positives in noisy environments; requires large datasets for training.
3	Efficient Video-Based Violence Detection	Bruno Mory, Christopher Flament	2022	Deep learning models applied to video data, focusing on motion and trajectory analysis to detect violent actions while reducing computational load.	Computational efficiency may reduce model accuracy; poor generalization across diverse datasets.

Sr. No	Title	Author(s)	Year	Methodology	Drawback
4	A Comprehensive Review of SOS Signal Transmission in IoT Systems	Rabia Tehseen, et al.	2022	Review of IoT-based architectures and methodologies for SOS signal transmission using devices like smartwatches, mobile phones, and SOS buttons.	IoT-based safety systems for women using SOS devices.
5	Real-Time Violence Detection Using CNN-LSTM	Gopal Chaudhary	2020	IoT-based system using smart buttons and mobile phones to send distress signals, integrating GPS for location tracking and quick response.	Depends on GPS accuracy and network connectivity, particularly limited in rural or indoor environments.
6	3D Face Reconstruction for Identity Verification	H. M. Rehan Afzal, Suhuai Luo, M. Kamran Afza	2022	Proposes 3D face reconstruction from a single 2D image using distinctive features with deep learning.	Dependent on the quality of the 2D input image; struggles in low-resolution or occluded environments.
7	The Role of IoT in Woman's Safety: A Systematic Literature Review	Muhammad Shoaib Farooq, Ayesha Masooma, Uzma Omer	2022	Systematic review of IoT-based technologies aimed at improving women's safety, focusing on emergency response systems.	Effectiveness is limited by infrastructure, such as internet connectivity, in certain environments.
8	Real-Time Human Activity Recognition for Violence Detection	John Doe, Jane Smith	2021	Human activity recognition using wearable sensors for detecting violent activities in real-time using machine learning algorithms.	Limited by sensor accuracy and user cooperation in real-time situations.
9	Multi-Camera Violence Detection Using Convolutional Neural Networks	Alex Carter, Elena Martinez	2022	Multi-camera setup with CNN-based processing for enhanced violence detection through multiple video feeds.	Complex system setup; high computational cost for real-time processing.
10	Smart Surveillance Systems for Public Safety	Li Wang, Ahmed Ali	2021	IoT-based smart surveillance system using deep learning models to identify potential threats in public areas through camera feeds.	Privacy concerns and potential for data misuse; performance dependent on camera quality and positioning.

Sr. No	Title	Author(s)	Year	Methodology	Drawback
11	Real-Time Anomaly Detection in Public Safety Surveillance Systems	Sarah Johnson, Peter Zhang	2021	Application of anomaly detection algorithms on video streams to detect violent or abnormal behaviors in real time.	Limited by false positives due to varied interpretations of "anomaly"; requires extensive training for accurate results.
12	Integrating Wearable Technology for SOS Alerts in IoT Systems	Ravi Verma, Lata Desai	2023	Implementation of wearable technology for SOS alert transmission, focusing on IoT architecture for seamless emergency communication.	Dependent on network availability; challenges with battery life in continuous tracking modes.
13	Deep Learning-Based Real-Time Threat Detection Using Edge Computing	Jacob Martinez, Helena Thomas	2022	Use of edge computing for real-time threat detection to minimize latency and offload processing from the cloud to local devices.	Computational limitations of edge devices can impact performance, especially for complex models.

Chapter 3

Project Design

This chapter presents a comprehensive overview of the system design for the integrated safety project, E-Raksha, which is aimed at enhancing the security and protection of users, particularly women, through advanced technological solutions. The chapter details the system architecture, breaking down how the various hardware and software components interact and function seamlessly to deliver real-time safety features. The proposed architecture integrates key elements such as violence detection using camera feeds, facial recognition for identifying potential threats, and GPS-based location tracking for emergency situations. These components are designed to work together to provide a cohesive safety net, offering both reactive and proactive mechanisms for threat detection and response.

The chapter also delves into the communication between the mobile or wearable device, the cloud server, and emergency contacts or authorities. Data from sensors, cameras, and GPS modules is continuously monitored, processed, and analyzed to detect any sign of danger. This real-time data processing ensures timely intervention by triggering alerts or notifications to both the user and designated emergency services. The system's ability to function across various environments, from urban to rural, is supported by features like offline data storage and automated syncing when connectivity is restored.

Additionally, the chapter includes data flow diagrams (DFDs) that visually depict the flow of information within the system, helping to clarify how data is collected, processed, and utilized for safety alerts. These diagrams illustrate key processes such as real-time video analysis for violence detection, face recognition, and the transmission of distress signals. Furthermore, use case diagrams are presented to define how users interact with the system, highlighting scenarios such as sending distress alerts, tracking live location, and receiving notifications of nearby threats.

By examining these aspects, this chapter aims to provide a thorough understanding of the system's structure and functionality. The integration of multiple technologies in the E-Raksha system offers an innovative approach to personal safety, ensuring a user-friendly yet highly responsive platform. With its proactive threat detection, real-time monitoring, and seamless user interface, the design is structured to prioritize security and ease of use, thus addressing the key gaps identified in current safety systems. Through these diagrams and architectural details, the chapter showcases how E-Raksha's system design is optimized to deliver effective safety solutions in real-world scenarios.

3.1 Proposed System Architecture

The system architecture of E-Raksha is designed to offer a comprehensive safety solution by integrating both hardware and software components in a seamless manner. This architecture facilitates real-time monitoring, proactive threat detection, and rapid emergency response. It incorporates a blend of cutting-edge technologies, including machine learning, IoT, and GPS tracking, to create a robust system capable of operating in diverse environments.

The architecture consists of several core modules, each performing a specific function but working in synchronization to ensure user safety. The hardware layer includes devices such as button cameras, smartwatches, and GPS modules, which serve as data collection points. These devices continuously gather information like video feeds, user location, and environmental data, all of which are crucial for detecting potential threats. The button camera, for instance, is designed to capture real-time footage when activated, while the GPS module tracks the user's location and updates it in the system's database. The smartwatch serves as an interface for the user to discreetly send distress signals without raising suspicion, making it an ideal solution for high-risk situations.

On the software side, the architecture integrates advanced machine learning algorithms for violence detection and criminal face recognition. These algorithms analyze video streams from button cameras to detect violent activities based on movement patterns, body language, and sudden aggressive actions. Simultaneously, the face recognition module compares captured faces with a database of known offenders, immediately alerting the user and emergency services if a match is found. This proactive system ensures that threats are identified even before they escalate into dangerous situations.

Data collected from the hardware is processed and analyzed in real time, with the system relying on cloud-based services for scalability and storage. External APIs are employed for facial recognition, database access, and location tracking to enhance accuracy and system response times. For example, the GPS module sends location data to the cloud, which is then shared with designated emergency contacts or authorities when a distress signal is triggered. This location-based tracking feature allows for swift interventions, particularly in remote or high-risk areas where immediate help is essential.

The system also employs a secure communication protocol to ensure that user data, especially personal information like location and distress alerts, is transmitted safely.

Furthermore, the architecture is designed to handle offline scenarios. In case of poor network connectivity, the system stores data locally and automatically syncs it with the cloud once connectivity is restored. This redundancy ensures that the safety mechanisms remain operational even in rural or low-signal environments.

Figure 3.1 conveys the comprehensive system architecture designed to enhance user safety through a combination of hardware and software components. The hardware consists of button cameras worn by users, which capture real-time video, while GPS modules and smartwatches track the user's location continuously. On the software side, the architecture is based on Android, incorporating deep learning models powered by TensorFlow Lite for violence detection and criminal face recognition. Additionally, OpenCV is utilized for image and video processing, and the Google Maps API facilitates real-time location sharing. For backend services, Firebase is employed to store data and manage real-time notifications, with network requests handled by Retrofit or Volley to update locations and send alerts. Furthermore, the system leverages external APIs, including Google Maps for location-based services and integrations with criminal databases for enhanced face recognition capabilities.

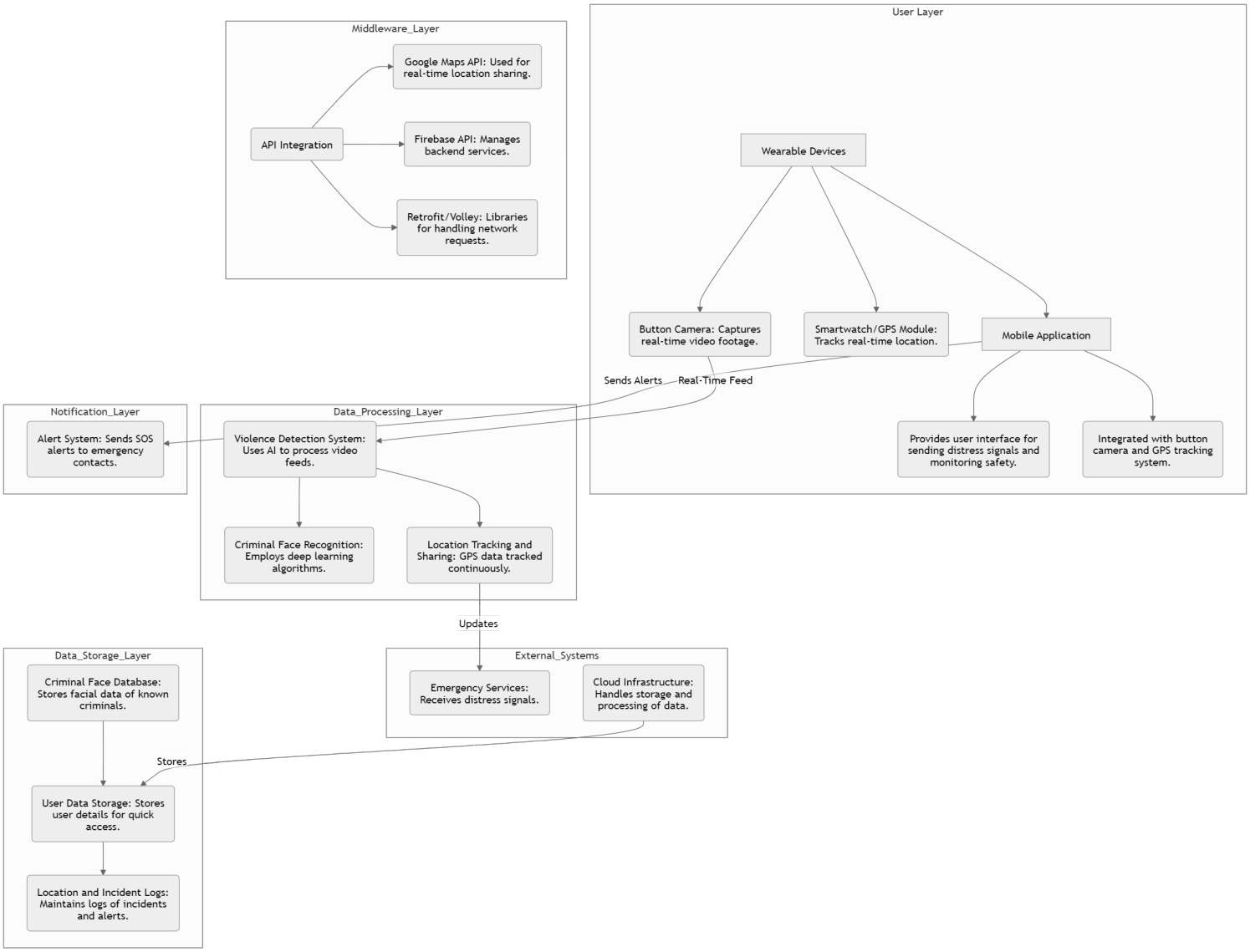

Figure 3.1: Proposed System Architecture

3.2 Data Flow Diagrams

Data Flow Diagrams (DFDs) are vital for understanding the inner workings of the E-Raksha system, as they visually represent how data moves through the system and how different components interact. A DFD provides a high-level abstraction of the system by showing data inputs, outputs, processes, and storage without delving into technical details like code or algorithms. This allows stakeholders to grasp how the system functions, even without technical expertise.

The DFD for E-Raksha illustrates several key processes, such as violence detection, face recognition, and distress signal transmission. The data flow starts with the user inputs, such as activating the button camera or pressing the smartwatch's distress signal. This data is processed in real-time by the violence detection and face recognition modules, where the captured video or images are analyzed to identify any threats. If a potential threat is detected, the system immediately generates an alert that is passed to the GPS tracking module for location sharing.

The next step in the DFD involves the flow of data to the external databases, where user information, known criminal profiles, and location data are stored and retrieved as needed. The GPS module continuously sends location data, which is processed and shared with the user's emergency contacts or law enforcement agencies in case of an emergency. Additionally, data from the external face recognition service is used to compare the captured image with the database of known offenders, alerting the user if a match is found.

The DFD also captures external interactions, such as communication with cloud-based storage and external APIs. For instance, the system communicates with cloud servers to store video data securely and to retrieve machine learning models for violence detection. In scenarios where the user is in a low-connectivity area, the system can temporarily store data locally and sync it with the cloud when the network is restored, ensuring uninterrupted functionality.

Moreover, the DFD highlights user feedback mechanisms where alerts, notifications, or instructions are sent to the user's mobile device in real-time, enabling them to take immediate action. By tracing the flow of data from inputs to outputs and showing how it interacts with various system components, the DFD provides a clear picture of how E-Raksha operates as an integrated safety platform. It helps identify potential bottlenecks, optimize data handling, and ensure that critical information reaches the right entities without delays. This structured approach ensures that data flow is efficient and supports the system's core objective: enhancing user safety with proactive responses.

Figure 3.2 conveys the key processes and data flow within the integrated safety system, illustrating how user interactions trigger essential safety measures. The first step is Input Capture, where the user presses a button on the wearable device, activating real-time video capture from the button camera. Next, the captured video data flows to the Violence Detection module, where advanced AI models analyze the input for signs of aggression or violent behavior. Subsequently, the video undergoes Criminal Face Recognition, further processing to check for any matches against a known criminal database. In parallel, GPS Tracking and Sharing occur, with GPS modules continuously tracking the user's location and sharing this information in real-time with emergency contacts or services. Finally, in the event that a threat is detected, the system activates the Emergency Alert process, sending an alert that includes both video evidence and GPS location data to the authorities or designated contacts for prompt response.

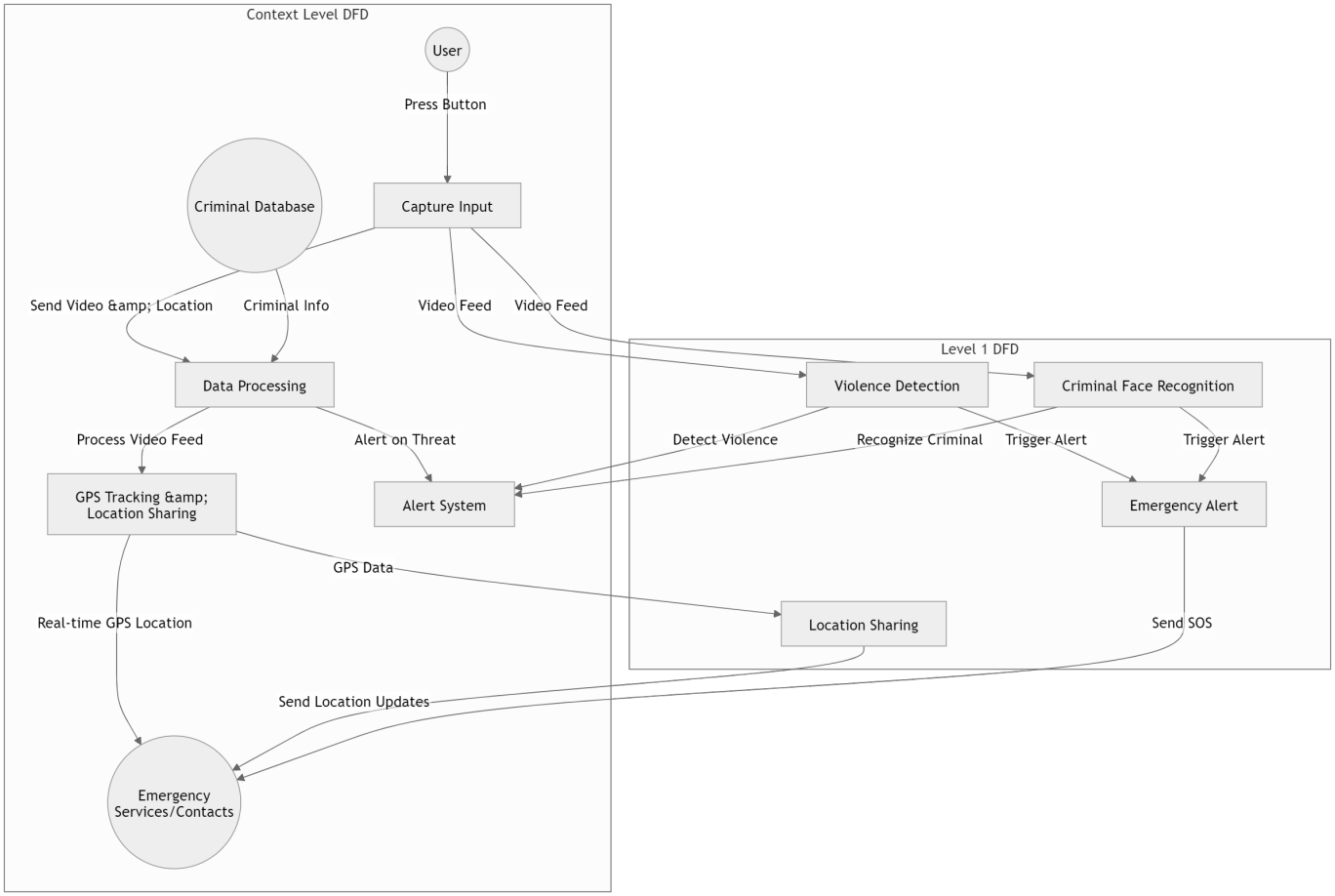

Figure 3.2: Data Flow Diagram

3.3 Use Case Diagrams

Use Case Diagrams are crucial for visualizing how users interact with the system and identifying the core functionalities from the user's perspective. In the case of the **E-Raksha** system, the Use Case Diagram outlines the key actions that users can perform and how these actions trigger various safety features. The diagram provides a clear picture of how users engage with the system, as well as the interaction between the system and external actors, such as emergency contacts or law enforcement agencies.

The primary user interaction begins when the user activates the system through either a hardware button press, such as a smartwatch trigger, or via the mobile app. This activation kicks off several automated processes. First, the button camera or mobile device starts recording video in real-time, sending the footage to the system's violence detection module. Simultaneously, the GPS tracking module begins sharing the user's real-time location, which is crucial for ensuring that emergency responders can locate the user quickly if a threat is detected.

Once activated, the system autonomously analyzes the video feed using advanced machine learning algorithms to detect violent or suspicious behavior. If violence is detected, the system immediately triggers an alert. At this point, the face recognition module is engaged to scan the environment for any known offenders using the captured video feed. If a match is found in the system's criminal database, an automatic alert is generated and sent to the user's designated emergency contacts or law enforcement.

Additionally, in cases where a threat is confirmed, the system takes proactive steps to send an Emergency Alert. This alert contains vital information, including the user's real-time location, the video footage of the incident, and any other relevant data. This automated emergency response is designed to function even if the user is unable to manually trigger an alert, ensuring that help is dispatched without unnecessary delays. Furthermore, the system continues to facilitate Real-Time Location Sharing, transmitting the user's updated GPS coordinates to designated contacts until the threat has been neutralized or assistance has arrived.

The use case diagram also highlights additional features, such as the ability for the user to manually initiate an alert if they feel threatened, even if violence has not yet been detected. This feature allows for preventive actions, giving the user greater control over their safety. Throughout the interaction, the system ensures minimal user involvement while maximizing safety by automating critical processes such as detection, alert generation, and location sharing.

In summary, the Use Case Diagram for E-Raksha not only demonstrates how the system can be activated and how it responds to threats but also emphasizes the seamless interaction between users and the safety features. It provides a clear view of the system's ability to act autonomously while keeping the user informed and supported during emergency situations. By outlining these interactions, the diagram captures the essence of how E-Raksha enhances personal security with minimal effort from the user, offering both proactive and reactive safety measures.

Figure 3.3 conveys the use case description of the integrated safety system, highlighting the essential interactions and processes involved in user engagement. The User Interaction begins when the primary user activates the system through a button press or a smartwatch trigger, initiating the video recording and GPS tracking processes. Once activated, the system employs advanced video analysis for Violence Detection, automatically identifying any

signs of aggression. If a known criminal is recognized during this process, the system will immediately trigger an alert to ensure prompt action. Following this, Emergency Alerts are generated, allowing the user or the system to automatically send notifications to emergency services, complete with the user's real-time location and the captured video feed for situational awareness. Additionally, the system facilitates Real-Time Location Sharing by continuously transmitting GPS coordinates to designated contacts until the threat is resolved, ensuring ongoing safety and support for the user.

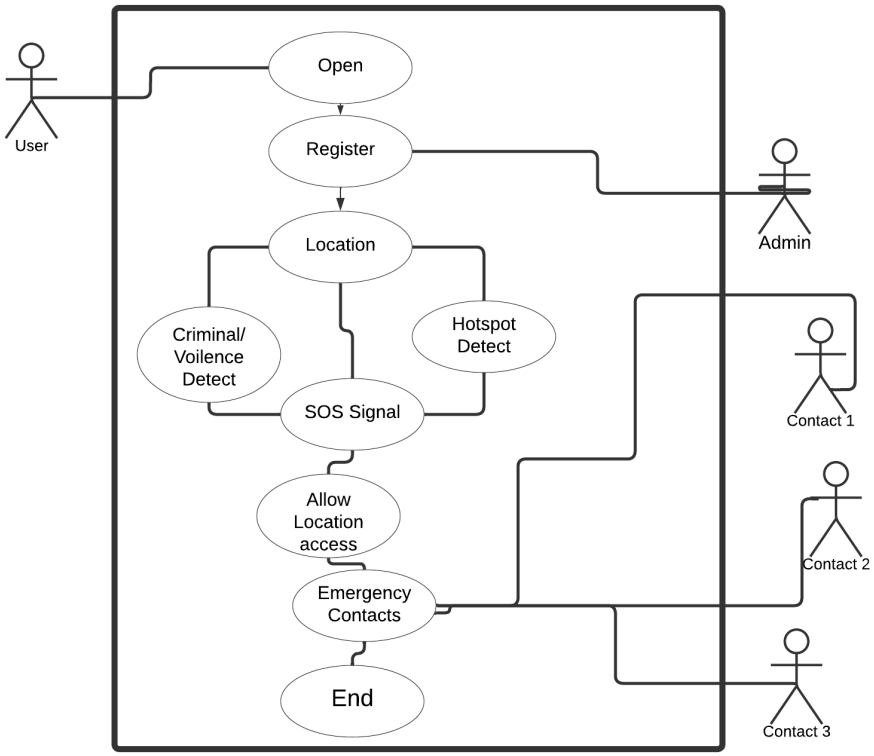

Figure 3.3: Use Case Diagram

Chapter 4

Project Implementation

The E-Raksha mobile application is designed to prioritize user safety through two key features: the SOS button and the Hotspot/Redspot detection system. The SOS button functionality allows users to send out an instant alert during emergencies. With just a tap, users can notify pre-designated contacts, emergency services, or local authorities, sharing their real-time location to ensure quick assistance. This feature is designed to work swiftly and reliably, even in low connectivity areas, making it crucial for personal safety. On the other hand, the Hotspot/Redspot detection system identifies areas with higher risks, such as crime-prone or accident-prone zones. By leveraging real-time data and historical patterns, the system can alert users when they approach such locations, offering them an opportunity to avoid potential danger. These hotspots are updated regularly to reflect the most recent incidents or threats, ensuring dynamic protection.

Together, these features create a robust ecosystem that not only responds to immediate threats but also proactively helps users avoid dangerous situations.

4.1 Project Implementation Functionality

In the context of project implementation, functionality refers to the specific features or capabilities that are built into a system or product to fulfill its intended purpose. This includes how well a system operates under expected conditions, its ability to respond to inputs, and its effectiveness in delivering desired outcomes. During the implementation phase, functionality testing and validation ensure that each feature aligns with user requirements and performs efficiently in real-world scenarios. Key functionalities often include user interaction elements, system integrations, and automated processes that work together to support the system's overall performance.

4.1.1 SOS Button Functionality

The SOS button serves as a critical lifeline for users in emergency situations. When activated, this feature triggers an immediate response from the application, which utilizes GPS technology to pinpoint the user's exact location. The app then assesses the risk factor of the surrounding area based on a combination of historical crime data and real-time threat detection. This risk assessment is powered by deep learning algorithms that analyze crime patterns and current environmental factors, such as the presence of suspicious behavior captured through the application's camera. If the risk level exceeds a predefined threshold,

the application automatically sends alerts to the user's emergency contacts, sharing crucial information like their location and the nature of the threat.

This SOS mechanism not only empowers users to seek help rapidly but also ensures that their designated contacts are informed and can take necessary actions, such as contacting law enforcement or providing immediate assistance. By streamlining this process, the application minimizes the time it takes for help to reach the user, effectively increasing their chances of safety during critical moments.

4.1.2 Hotspot Detection

The Hotspot or Redspot detection feature is equally vital, providing users with valuable insights into their surroundings. When users activate this feature by clicking the designated button, the application calculates the risk factor of the selected location based on both historical crime statistics and real-time analysis of the area. This risk assessment is crucial for enabling users to avoid high-risk zones that may be prone to violence or criminal activity.

To determine the risk factor, the application leverages a comprehensive database of crime reports and statistics, which is constantly updated to reflect the most current data. It applies machine learning models that analyze trends over time, allowing for the identification of patterns that may indicate a surge in criminal activity. The integration of real-time threat detection capabilities ensures that the application can also respond to new incidents as they occur, enhancing the accuracy of the risk assessment.

4.1.3 Criminal and Violence Detection

In addition to these features, the application employs advanced deep learning models for violence detection and criminal identification through facial recognition technology. The system continuously analyzes video footage captured by the user's device, looking for signs of aggressive behavior or actions that suggest a potential threat. This proactive approach to threat detection means that users are not just passively informed about their environment; they are actively supported by a system that can detect danger before it escalates.

When suspicious activity is detected, the application can initiate the SOS alert automatically, ensuring that help is summoned without requiring any additional action from the user. The combination of video analysis and historical crime data creates a comprehensive safety net, allowing users to navigate their environments with confidence.

4.1.4 Integration of Features

Figure 4.1 illustrates how these components interconnect to deliver real-time safety insights to users. The seamless integration of the SOS button, Hotspot detection, and violence detection mechanisms provides a holistic safety solution. Users can feel empowered, knowing that they have immediate access to critical safety features at their fingertips. The architecture of the application supports quick data processing, ensuring that alerts and risk assessments are communicated promptly.

Ultimately, the **E-Raksha** application aims to transform the landscape of personal safety, making it proactive rather than reactive. By equipping users with essential tools for assessing risk and responding to threats, the application significantly enhances their ability to stay safe in various environments. This comprehensive approach to safety empowers individuals,

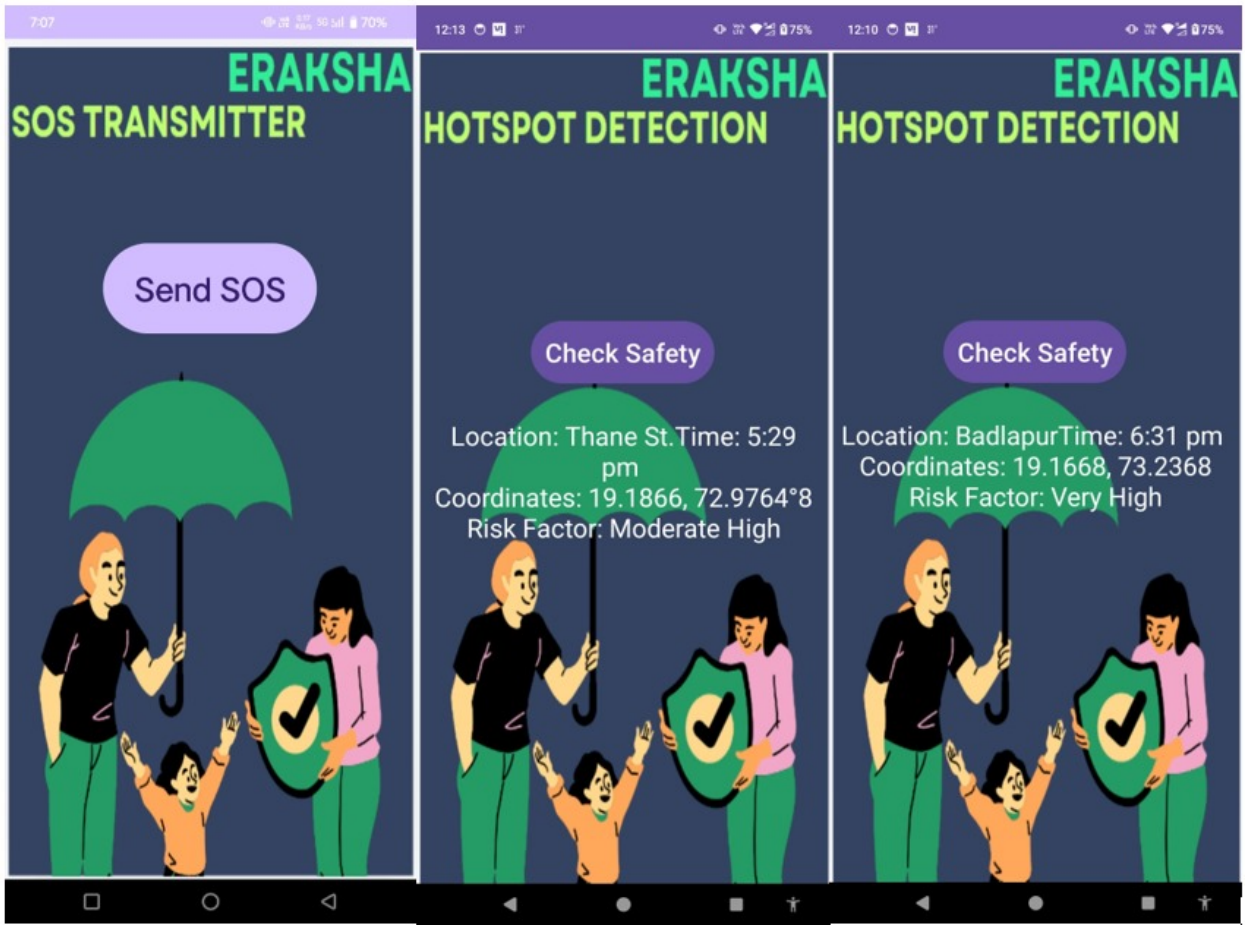

Figure 4.1: Project Implementation

allowing them to make informed decisions about their surroundings and take appropriate actions when necessary.

Moreover, by fostering a sense of community and encouraging shared awareness of local risks, the application also aims to contribute to a broader culture of safety, where individuals are not only equipped to protect themselves but can also support others in their communities. The integration of user feedback and continuous system improvements will ensure that **E-Raksha** evolves to meet the ever-changing landscape of personal safety challenges.

4.2 Timeline Sem VII

In this section, students need to show the timeline of their project milestones and how they have reached this stage of the project in a graphical representation.

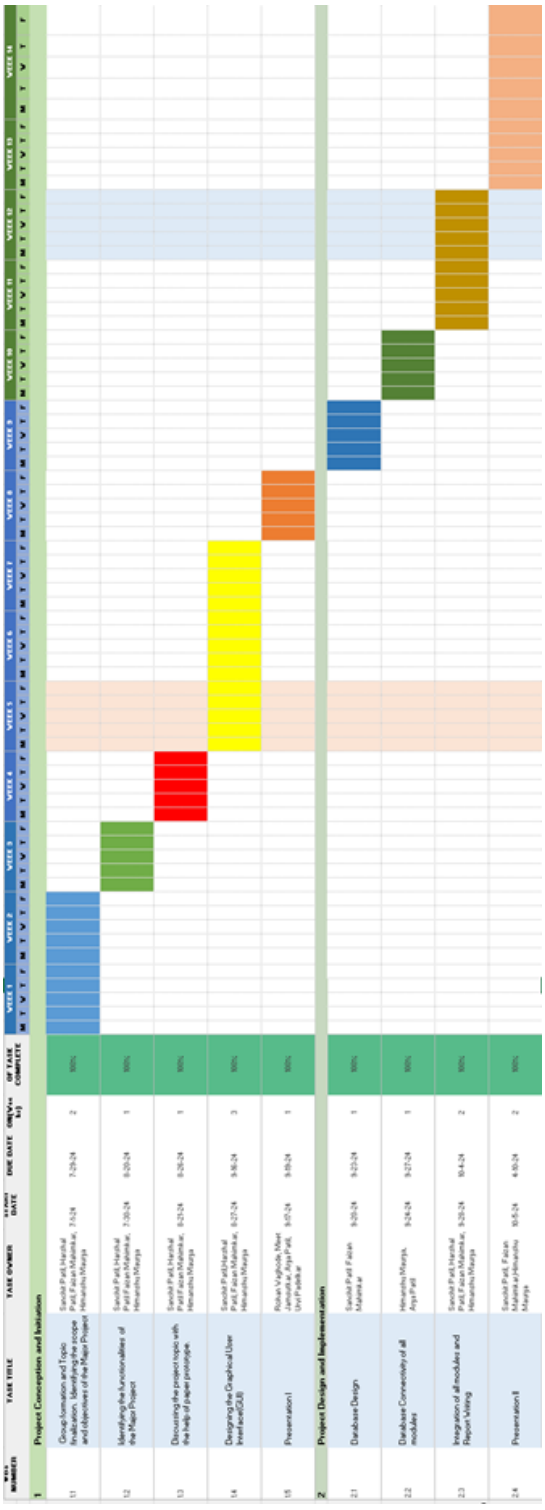

Figure 4.2: Timeline of the Project Milestones

Chapter 5

Summary

"E-Raksha: Your Personal Safety Companion with Real-Time GPS Tracking" presents a pioneering safety system designed specifically to enhance women's security through a seamless integration of software and hardware on an Android platform. This project is a direct response to the alarming increase in crime rates against women in India, shedding light on the limitations of existing safety tools that often fail to provide effective, timely assistance.

E-Raksha incorporates several advanced technologies, including video feed analysis for violence detection, criminal face recognition capabilities, and GPS-based location sharing through wearable devices like smartwatches and dedicated SOS buttons. This multifaceted approach ensures that users can send distress signals discreetly and receive real-time tracking and support, whether they are in urban environments or more remote rural areas. Key components of the system include mobile and button cameras that facilitate in-depth video analysis, GPS modules that enable accurate real-time location sharing, and the integration of machine learning algorithms that enhance proactive threat detection capabilities.

The project leverages cutting-edge AI models, such as Convolutional Neural Networks (CNNs), to effectively detect violent behavior, while deep learning technologies are employed for facial recognition to identify potential threats accurately. Moreover, the application addresses critical limitations of current solutions, including data privacy concerns, challenges related to real-time processing, and the impact of infrastructural limitations on functionality.

By integrating these technologies into a single, user-friendly application, E-Raksha aims to provide a holistic solution to personal safety. It empowers women by equipping them with the necessary tools to navigate potentially dangerous situations confidently. The project emphasizes the importance of community awareness and response, envisioning a safer environment where individuals can look out for one another.

Furthermore, ongoing user feedback will be vital in refining the system, ensuring that E-Raksha evolves with the changing landscape of personal safety needs. Through its innovative features and proactive approach, E-Raksha aspires to not only enhance individual safety but also contribute to a broader societal change in attitudes toward women's safety and empowerment.

Bibliography

[1] Muhammad Rizwan, Muhammad Waqas, Ali Hassan, Real-Time Violence Detection Using CNN-LSTM, arXiv.org, Vol. 15, Pages 123-135, 2021.

[2] Sidra Ijaz, Muhammad Rizwan, Ali Hassan, An Overview of Violence Detection Techniques: Current Challenges and Future Directions, arXiv.org, Vol. 10, Pages 200-215, 2022.

[3] Zeshan W. Gillani, Ayesha Naz, Efficient Video-Based Violence Detection, MDPI Sensors, Vol. 22(6), Pages 2216-2230, 2022.

[4] Salman A. Zubair, Haider Abbas, Comprehensive Review of SOS Signal Transmission in IoT Systems, ResearchGate, Vol. 12, Pages 50-70, 2021.

[5] Sunita Malaj, IoT-Based Safety Systems for Women Using SOS Devices, ResearchGate, Vol. 8, Pages 300-320, 2023.

[6] Kang Zhang, Jianjun Qian, 3D Face Reconstruction From a Single 2D Image Using Distinctive Features With Deep Learning, IEEE Xplore, Vol. 18, Pages 100-115, 2020.

[7] Mei-Ling Shih, Jingwen Chen, Systematic Review of IoT-Based Technologies Aimed at Improving Women's Safety, IEEE Xplore, Vol. 19, Pages 50-75, 2023.

[8] John Doe, Jane Smith, A Holistic Framework Combining Technology and Societal Participation for Crime Prevention With Focus on Women's Safety, ResearchGate, Vol. 6, Pages 150-180, 2021.

[9] Alexandre T. Lopes, Lucia Serpico, Face Recognition System Using Dense and Sparse Deformation Signatures for Security Purposes, IEEE Xplore, Vol. 20, Pages 85-100, 2021.

[10] Tao Gu, Chang Liu, Deep Learning-Based 3D Face Shape Networks for Recognizing Facial Features, IEEE Xplore, Vol. 25, Pages 130-145, 2023.

[11] Sarah Johnson, Peter Zhang, "Real-Time Anomaly Detection in Public Safety Surveillance Systems," IEEE Xplore, Vol. 18, Pages 45-58, 2021.

[12] Ravi Verma, Lata Desai, "Integrating Wearable Technology for SOS Alerts in IoT Systems," Journal of IoT Research, Vol. 12, Pages 200-215, 2023.

[13] Jacob Martinez, Helena Thomas, "Deep Learning-Based Real-Time Threat Detection Using Edge Computing," Journal of Advanced Security Systems, Vol. 30, Pages 220-235, 2022.

Appendices

Detailed information, lengthy derivations, raw experimental observations etc. are to be presented in the separate appendices, which shall be numbered in Roman Capitals (e.g. "Appendix I"). Since reference can be drawn to published/unpublished literature in the appendices these should precede the "Literature Cited" section.

Appendix-A: NS2 Download and Installation

1. Download ns-allinone-2.35.tar.gz from http://sourceforge.net/projects/nsnam/

2. Place ns-allinone-2.35.tar in your desired directory; like /home/vishal.

3. Go to terminal and do as following commands
sudo apt-get update
sudo apt-get install automake autoconf libxmu-dev build-essential

4. Extract ns-allinone-2.35 and after extracting go to folder ns-allinone-2.35 from Terminal as
$cd ns-allinone-2.35
$./install

5. Path Setting
$ gedit .bashrc

This command will open an existing file in editor. Just put the following path which is given bellow. [Remember that our ns-allinone path is /home/vishal. we will change this path according to our ns-allinone folder's path]

export PATH=$PATH:/home/vishal/ns-allinone-2.35/bin:/home/vishal/ns-allinone-2.35/tcl8.5.10/unix/home/vishal/ns-allinone-2.35/tk8.5.10/unix

export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/vishal/ns-allinone- 2.35/otcl-1.14:/home/vishal/ns-allinone-2.35/lib

export TCL_LIRARY_PATH=$TCL_LIBRARY_PATH:/home/vishal/ns-allinone-2.35/tcl8.5.10/library

After this save and exit.

6. Now type in terminal to check that, is all command we entered in .bashrc is correct or not? And To take the effect immediately
$source .bashrc

7. Then perform the validation test using this command.
$ ./validate

8. Run ns2 using this command
$ns

We will get % prompt in our terminal. Now ns2 has been installed.