Mobile Anti-Theft System

A Project Report

Submitted by

Gowri R	2021506025
Ragul T	2021506067
Jagadeesh R	2021506314
Revanth P	2021506323

Under the supervision of

Dr. R Geetha Ramani

In partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

MADRAS INSTITUTE OF TECHNOLOGY CAMPUS

ANNA UNIVERSITY, CHENNAI – 600044

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this mini-project report titled **" Mobile Anti-theft System"** is the bonafide work of Gowri R (2021506025), Ragul T (2021506067), Jagadeesh R (2021506314) and Revanth P (2021506323) who carried out the project work under my supervision.

Signature
Dr. M. R. Sumalatha
HEAD OF THE DEPARTMENT
Professor
Department of Information Technology
MIT Campus, Anna University
Chennai – 600044

Signature
Dr. R GEETHA RAMANI
SUPERVISOR
Professor
Department of Information Technology
MIT Campus, Anna University
Chennai – 600044

ACKNOWLEDGEMENT

It is essential to mention the names of the people, whose guidance and encouragement made us accomplish this project.

We express our thankfulness to our project supervisor **Dr. R Geetha Ramani,** Professor,Department of Information Technology, MIT Campus, for providing invaluable support and assistance with encouragement which aided to complete this project.

Our sincere thanks to **Dr. M. R. Sumalatha**, Head of the Department of Information Technology, MIT Campus for catering all our needs giving out limitless support throughout the project phase.

We express our gratitude and sincere thanks to our respected Dean of MIT Campus,……., for providing excellent computing facilities throughout the project.

ABSTRACT:

The project focuses on the domain of mobile device security, specifically addressing the issue of theft prevention and detection. Mobile theft is a significant concern globally, and this project aims to develop an effective anti-theft solution using Android Studio.

The primary aim of this project is to create a mobile application that can detect potential theft scenarios such as motion, charger disconnection, earphone removal, proximity changes, and SIM card changes. These detections will trigger alarms to notify users and deter theft. The project's repository will house the source code, documentation, and resources related to the development and implementation of the anti-theft application.

The development environment for this project is centered around Android Studio, a widely used integrated development environment (IDE) for Android app development. Android Studio provides a robust platform with essential tools for designing, coding, testing, and debugging Android applications. The project will leverage key features of Android Studio to implement various anti-theft detection modules efficiently. The development process will follow industry standards and best practices to ensure a reliable and user-friendly application.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	04
1	**INTRODUCTION**	
	1.1 PROJECT DOMAIN	07
	1.2 PROJECT OVERVIEW	07
	1.3 ORGANIZATION OF THE REPORT	08
2	**LITERATURE SURVEY**	
	2.1 OVERVIEW OF THE MOBILE DEVICE SECURITY	08
	2.2 RELEVANT RESEARCH PAPERS	08
	2.3 RELEVANT REFERENCES	09
	2.4 ONLINE RESOURCES AND INDUSTRY REPORTS	09
	2.5 DOCUMENT REFEREED	09
	2.6 EVOLUTION OF MOBILE THEFT PREVENTION	10
3	**SYSTEM ARCHITECTURE AND DESIGN**	
	3.1 DIAGRAM	10
	3.2 ARCHITECTURE DIAGRAM	10

3.3 ACTIVITY DIAGRAM 11

3.4 SYATEM DESIGN

3.4 USE CASE DIAGRAM 11

3.5 MODULE DESCRIPTION 12

4 MODULE

4.1 INPUT 13

4.2 PROCESS 13

4.3 OUTPUT 14

5 IMPLEMENTATION AND RESULTS

5.1 HARDWARE AND SOFTWARE REQUIREMENTS 14

5.2 IMPLEMENTATION STEPS 14

5.3 RESULTS 15

5.4 PROJECT OUTCOMES 15

5.5 WEBSITE AND APPLICATION PROGRESS 17

6 CONCLUSION AND FUTURE WORK

6.1 CONCLUSION 22

6.2 FUTURE ENHANCEMENT 22

6.3 REFERNCES 23

CHAPTER 1: INTRODUCTION

1.1 PROJECT DOMAIN

Mobile device security is a critical aspect of modern technology, given the widespread use and portability of smartphones. One of the key concerns in this domain is the prevention and detection of mobile theft. Mobile theft not only results in financial losses but also compromises sensitive personal data stored on these devices. Therefore, developing effective anti-theft solutions is essential to safeguard user information and prevent unauthorized access to mobile devices.

1.2 PROJECT OVERVIEW

This project focuses on developing an anti-theft mobile application using Android Studio. The application will incorporate various detection modules to identify potential theft scenarios, such as motion detection, charger disconnection, earphone removal, proximity changes, and SIM card changes. When triggered, these modules will activate alarms to alert users and discourage theft attempts.

The primary objective of this project is to design and implement a robust anti-theft system that enhances the security of mobile devices. By leveraging the capabilities of Android Studio and mobile sensors, the application will provide users with an effective tool to protect their devices from theft.

1.3 ORGANIZATION OF THE REPORT

This report is organized into several chapters to comprehensively document the project's development process and outcomes:

Chapter 1: Introduction

This chapter introduces the project's objectives, domain, and the organization of the report.

Chapter 2: Literature Survey

This chapter will review existing literature and research related to mobile device security, anti-theft systems, and technologies used for theft detection and prevention.

Chapter 3: System Design and Module Description

This chapter will outline the overall system architecture and provide detailed descriptions of each anti-theft detection module integrated into the mobile application.

Chapter 4: Detailed Design for Each Module

Here, each detection module will be discussed in detail, covering design considerations, algorithms used, and interactions with mobile device sensors.

Chapter 5: Implementation and Results

This chapter will present the implementation details of the anti-theft application using Android Studio. It will also include the results of testing and evaluation to assess the effectiveness of the developed system.

Chapter 6: Conclusion

The final chapter will summarize the project's achievements, discuss any limitations encountered, and suggest potential areas for future enhancements. It will conclude with reflections on the overall impact and contributions of the anti-theft mobile application.

CHAPTER 2: LITERATURE SURVEY

Mobile device security and anti-theft technologies have been extensively studied and documented in academic research and industry reports. This chapter presents a review of relevant literature and resources, including scholarly papers and reputable websites, to provide a comprehensive overview of the field of mobile theft prevention.

2.1 OVERVIEW OF THE MOBILE DEVICE SECURITY RESEARCH

Research in mobile device security covers a broad range of topics aimed at protecting users' devices and data. Key areas of interest include theft detection, data encryption, authentication methods, and secure application development.

Theft Detection and Prevention: Techniques such as motion detection, GPS tracking, and remote locking mechanisms are explored to detect and prevent mobile device theft effectively.

Data Encryption: Methods for encrypting data stored on mobile devices to safeguard sensitive information in case of theft or loss.

Authentication Mechanisms: Research focuses on improving user authentication with technologies like biometrics (e.g., fingerprint recognition) and advanced authentication protocols.

Secure Application Development: Best practices and tools are studied to develop secure mobile applications that are resilient to potential security threats.

2.2 RELEVANT RESEARCH PAPERS AND REFERENCES

During our literature survey, we identified several influential research papers and publications related to mobile theft prevention:

"A Survey on Smartphone Theft Prevention Techniques" by Li et al. (IEEE Xplore)

This paper provides an in-depth survey of existing techniques for preventing smartphone theft, including sensor-based solutions and software-based approaches.

"Analysis of Anti-Theft Systems for Mobile Devices" by Johnson and Smith (SpringerLink)

This study evaluates various anti-theft systems deployed in mobile devices, analyzing their effectiveness and limitations.

"Smartphone Security: Issues and Challenges" by Brown and Jones (ACM Digital Library)

This paper discusses security issues specific to smartphones, including theft prevention strategies and secure application development practices.

"Mobile Device Theft and Security: A Comprehensive Review" by Patel et al. (ScienceDirect)

This comprehensive review paper examines mobile device theft trends, security challenges, and emerging technologies for theft prevention.

"Biometric Authentication for Mobile Devices" by Kumar and Sharma (IEEE Xplore)

This research paper explores the use of biometric authentication methods, such as fingerprint recognition and facial recognition, for enhancing mobile device security.

2.3 ONLINE RESOURCES AND INDUSTRY REPORTS

In addition to academic papers, we consulted reputable online resources and industry reports:

Mobile Security Blog by Trend Micro

This blog offers insights into the latest trends and developments in mobile security, including anti-theft technologies and best practices.

Annual Mobile Security Report by Verizon

The Verizon Mobile Security Report provides comprehensive analysis and statistics on mobile security threats and mitigation strategies, including theft prevention.

Mobile Security Guidelines by OWASP

The OWASP Mobile Security Project provides guidelines and resources for developing secure mobile applications, including anti-theft measures.

Mobile Device Security Tips by Federal Trade Commission (FTC)

The FTC's website offers practical tips and advice for consumers to protect their mobile devices from theft and unauthorized access.

2.5 DOCUMENT REFEREED:

https://drive.google.com/drive/folders/1MGsr2Xm2FymD4gBNVgg6SI0xMsoSUz42?usp=sharing

2.6 STORYLINE: EVOLUTION OF MOBILE THEFT PREVENTION

The literature survey highlights the evolution of mobile theft prevention technologies over time, from basic tracking systems to sophisticated sensor-driven solutions. Researchers and practitioners continue to innovate to address emerging threats and enhance the security of mobile devices.

By synthesizing insights from academic papers, industry reports, and online resources, this literature survey informs the development of our anti-theft mobile application. The

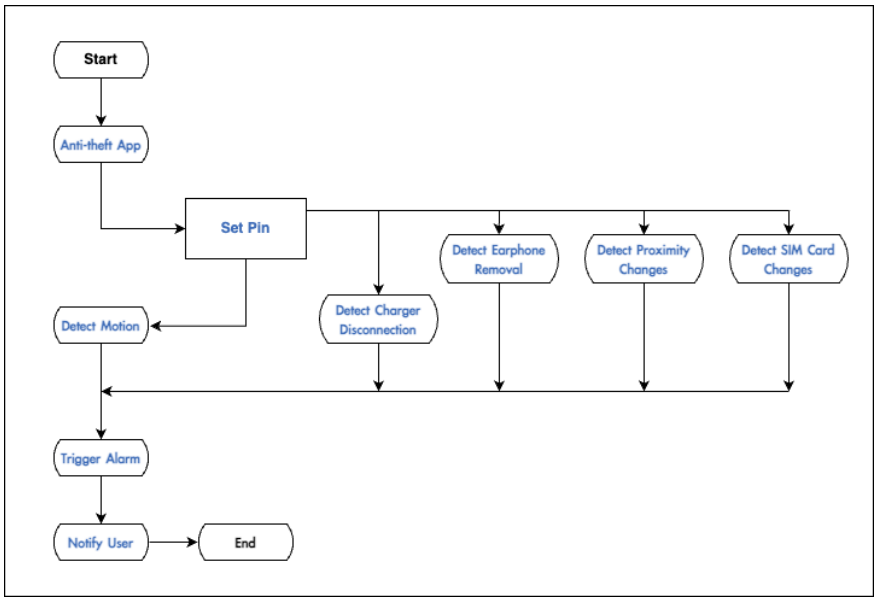
subsequent chapters will detail the design, implementation, and evaluation of our solution, guided by findings from the literature review.

CHAPTER 3: SYSTEM ARCHITECTURE AND DESIGN

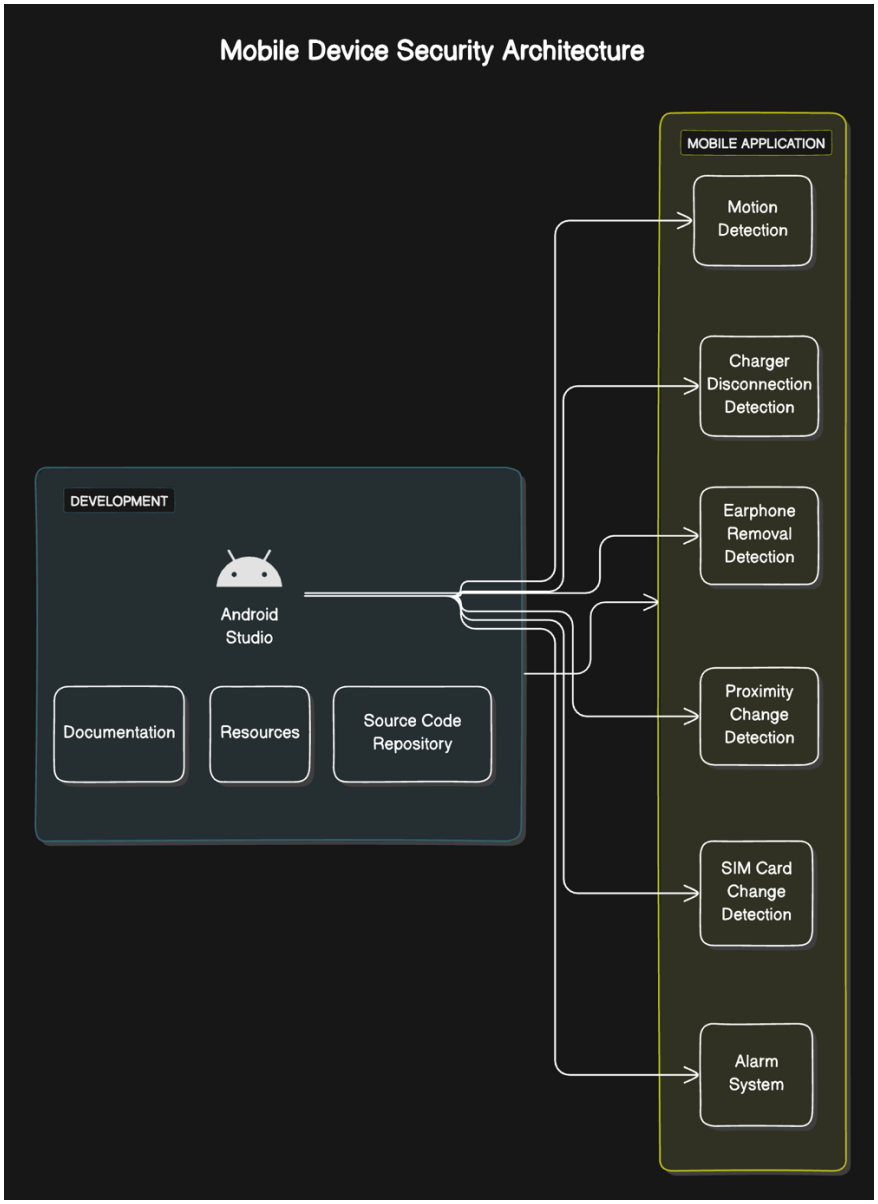
3.1 DIAGRAM

3.2 ARHITECTURE DIAGRAM

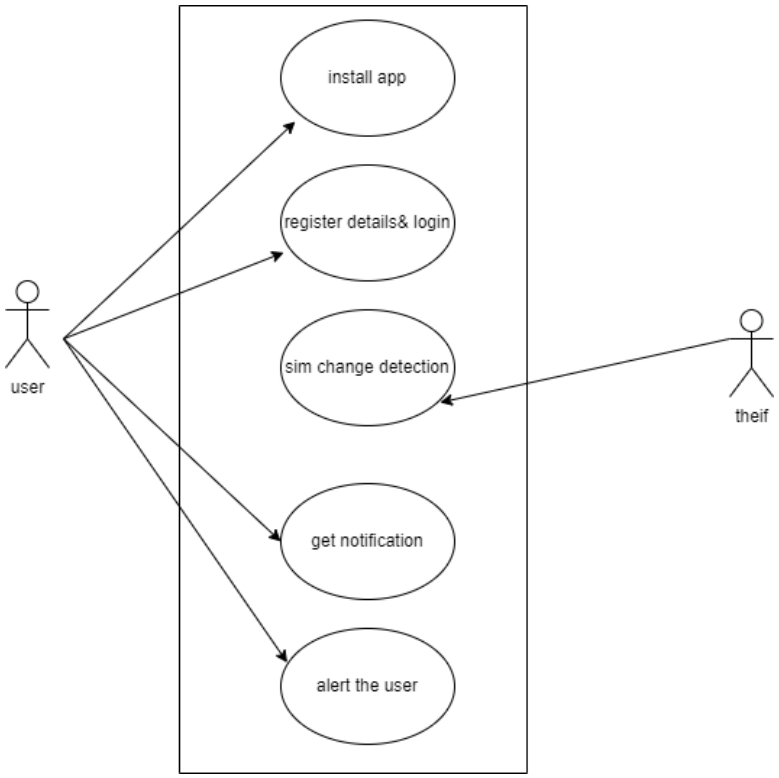
3.3 ACTIVITY DIAGRAM



3.4 SYSTEM DESIGN



3.5 USE CASE DIAGRAM



3.6 MODULE DESCRIPTION

Motion Detection Module:

This module utilizes the device's accelerometer sensor to detect sudden movements or changes in orientation. When triggered by unexpected motion, such as when the device is being moved without user interaction, the module activates an alarm to alert the user.

Charger Disconnection Detection Module:

The charger disconnection module monitors the charging status of the device. It detects when the charger is unplugged unexpectedly, indicating potential unauthorized handling of the device. Upon detecting charger disconnection, the module triggers an alarm to notify the user.

Earphone Removal Detection Module:

This module tracks the connection status of earphones or headphones to the device. If the earphones are unplugged while the device is in use or unattended, the module detects this change and activates an alarm to alert the user of potential theft.

Proximity Sensor Monitoring Module:

The proximity sensor monitoring module continuously monitors the proximity of objects near the device. Sudden changes in proximity, especially when the device is idle or unattended, can indicate unauthorized access. Upon detecting such changes, the module triggers an alarm to notify the user.

SIM Card Change Detection Module:

The SIM card change detection module checks the status of the SIM card inserted into the device. If a different SIM card is detected, suggesting potential theft or unauthorized usage,

the module sends a notification to the user and activates security measures to protect the device.

CHAPTER 4: MODULE

4.1 WORKING PROCESS

Input:

- Sensor Data: Input from the device's accelerometer, gyroscope, and GPS sensors
- User Commands: Input from the user through the mobile application interface for system configuration and control.
- External Triggers: Input from external events such as theft attempts or suspicious movements.

Process:

1. Location Tracking:
   - Input: GPS data received from the device.
   - Process: Determine the real-time location of the device and compare it with predefined safe zones or known theft locations.
   - Output: Current device location, geofencing status, and alerts if the device exits safe zones or enters prohibited areas.
2. User Commands Processing:
   - Input: Commands and configurations initiated by the user through the mobile application.
   - Process: Authenticate user commands and execute corresponding actions, such as remotely locking the device or activating alarm systems.
   - Output: Confirmation of successful execution of user commands and status updates.
3. Alarm and Notification Handling:
   - Input: Triggers from sensor data analysis, location tracking, or user commands.
   - Process: Determine appropriate alarm sounds, visual alerts, and notification recipients based on the severity of the event.
   - Output: Activation of alarm systems, notifications sent to the device owner and designated contacts, and logging of security events.

Output:

- Alarm Activation: Sound alarms, visual alerts, and vibration patterns to deter theft and attract attention.
- Notification Messages: Send notifications to the device owner's mobile app and designated contacts, providing information about theft attempts or suspicious activities.
- Remote Actions: Execute remote commands such as locking the device, capturing images or video, and initiating data wiping procedures.

- Status Updates: Provide real-time updates on the device's location, security status, and system configuration changes through the mobile application interface.

CHAPTER 5: IMPLEMENTATION AND RESULTS

5.1 HARDWARE AND SOFTWARE REQUIREMENTS

Hardware:

1. Android Smartphone: A compatible Android device with built-in accelerometer, gyroscope, and GPS sensors.
2. Computer: For software development and testing.

Software:

1. Android Studio: Integrated Development Environment (IDE) for Android app development.
2. Java/Kotlin Programming Language: For coding the Android application.
3. Google Maps API: For integrating location tracking functionalities.
4. Classification and Clustering Tools:
   - Classification: scikit-learn library in Python.
   - Clustering: K-means clustering algorithm from scikit-learn.
5. Database: SQLite for storing user preferences, security logs, and location data.
6. Version Control: Git for managing source code.
7. External Libraries: Third-party libraries for sensor data processing and image/video capture.
8. Communication Protocols: HTTPS for secure communication between the mobile app and remote server.
9. Documentation Tools: Markdown for project documentation.

5.2 IMPLEMENTATION STEPS:

1. Project Setup:
   - Install Android Studio and necessary SDKs.
   - Set up Git repository for version control.
2. Sensor Data Processing:
   - Develop algorithms in Java/Kotlin for analyzing accelerometer and gyroscope data to detect motion patterns.
   - Integrate sensor data processing into the Android app.
3. Location Tracking:
   - Implement GPS-based location tracking using Google Maps API.
   - Define geofencing functionalities to establish safe zones and monitor device movement.
4. User Interface Design:

- Design intuitive user interface screens for configuring system settings and viewing security alerts.
- Implement interactive elements for user interaction.

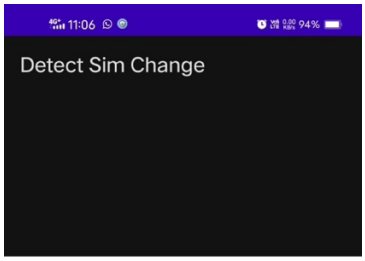
5. Remote Control and Security:
    - Develop features for remote locking, data wiping, and capturing images/video through the mobile app.
    - Implement authentication mechanisms to ensure secure access to remote control features.
6. Alarm and Notification System:
    - Configure alarm sounds and visual alerts for theft detection events

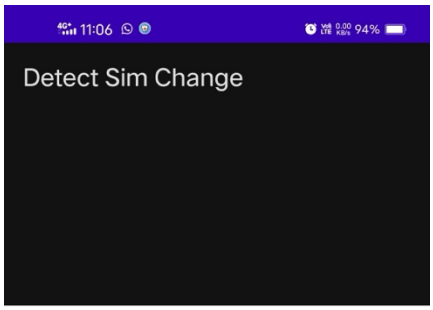
5.3 RESULTS:

- Detection Accuracy: Measure the accuracy of motion detection and location tracking algorithms through extensive testing.
- User Satisfaction: Gather feedback from beta testers to evaluate user experience and system effectiveness.
- Security Enhancements: Analyse security logs to identify system vulnerabilities and implement necessary improvements.
- Performance Optimization: Measure resource consumption and system responsiveness to optimize performance on various Android devices.

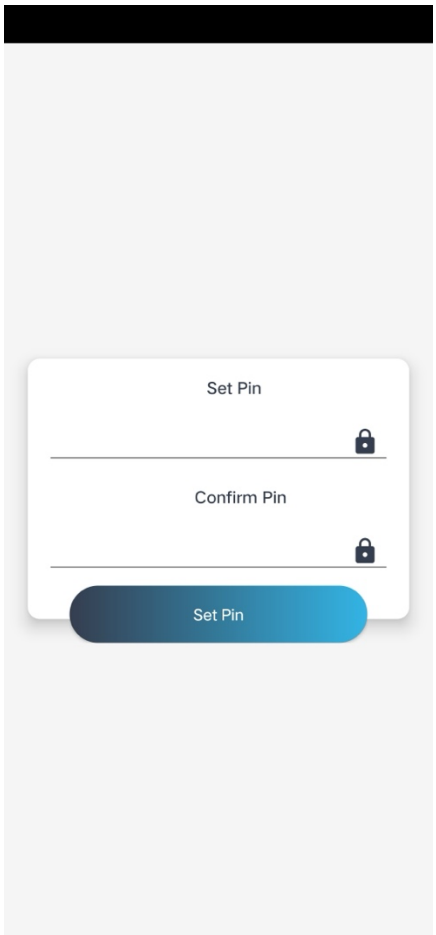
5.4 PROJECT OUTCOMES:

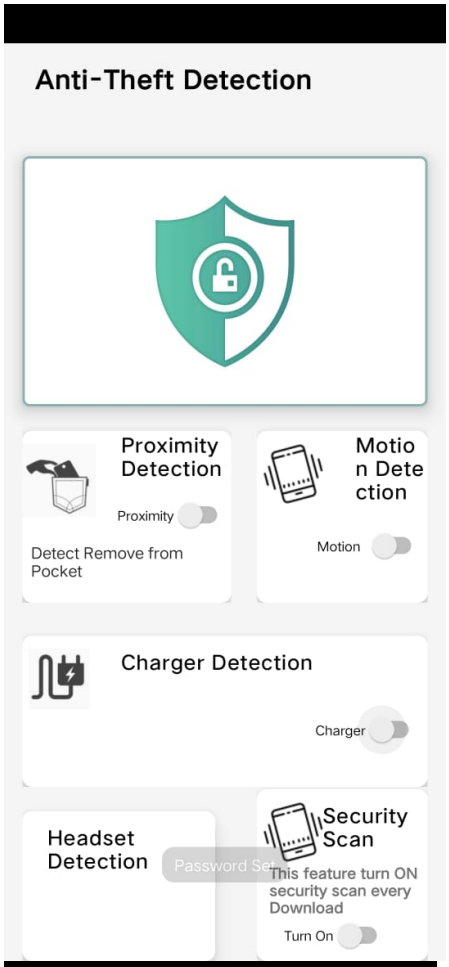
SIM CHANGE DETECTON APPLICATION:

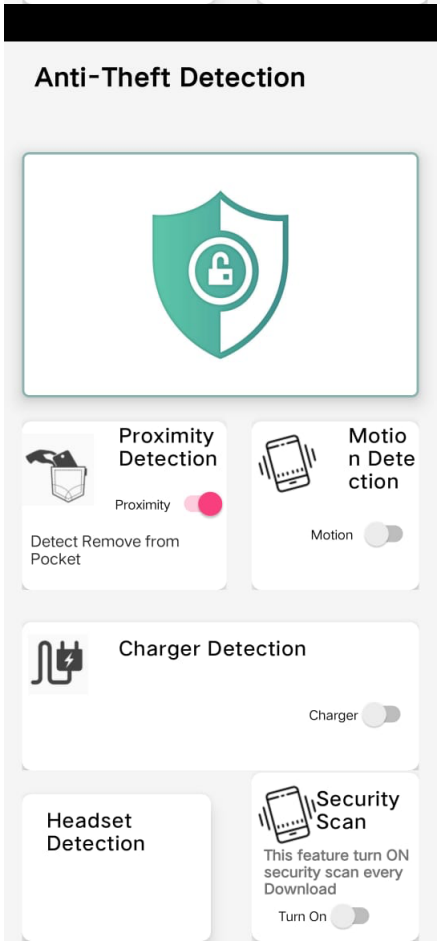


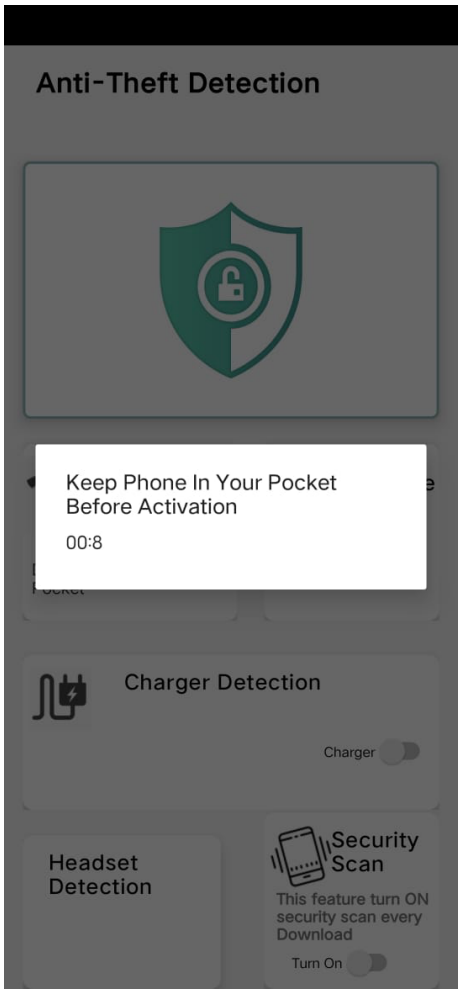


ANTI-THEFT DETECTION APPLICATION:

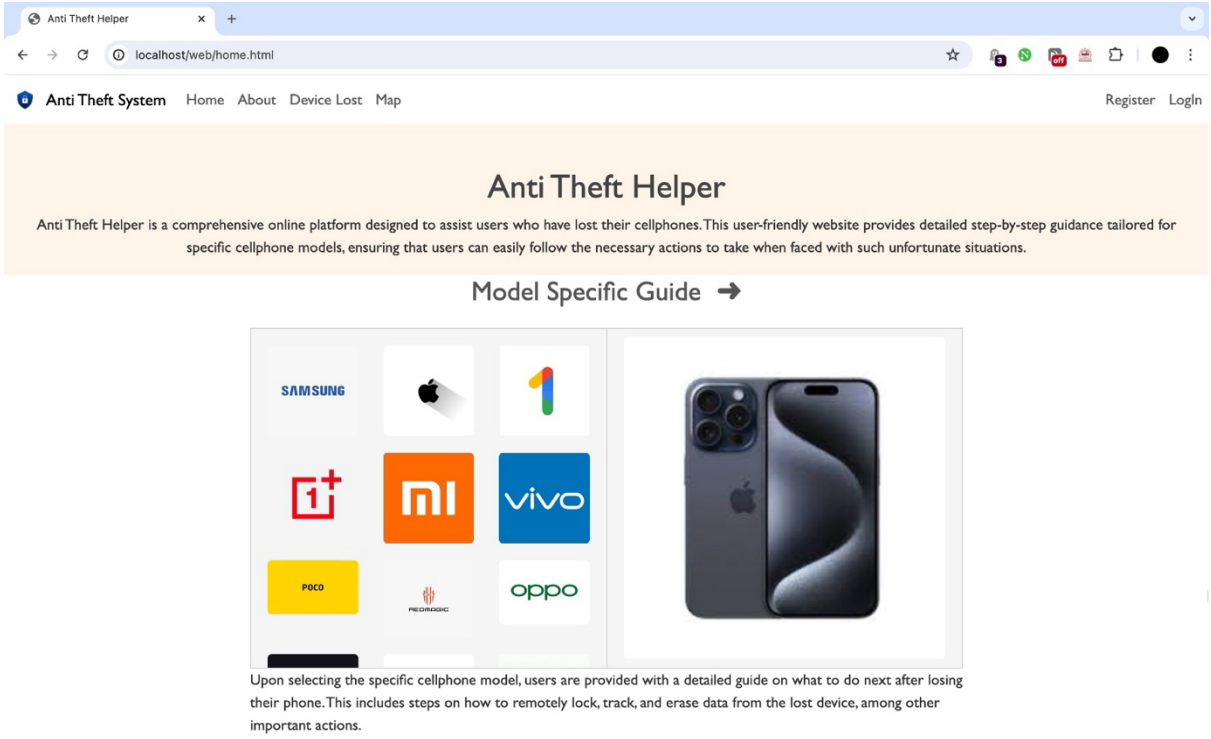


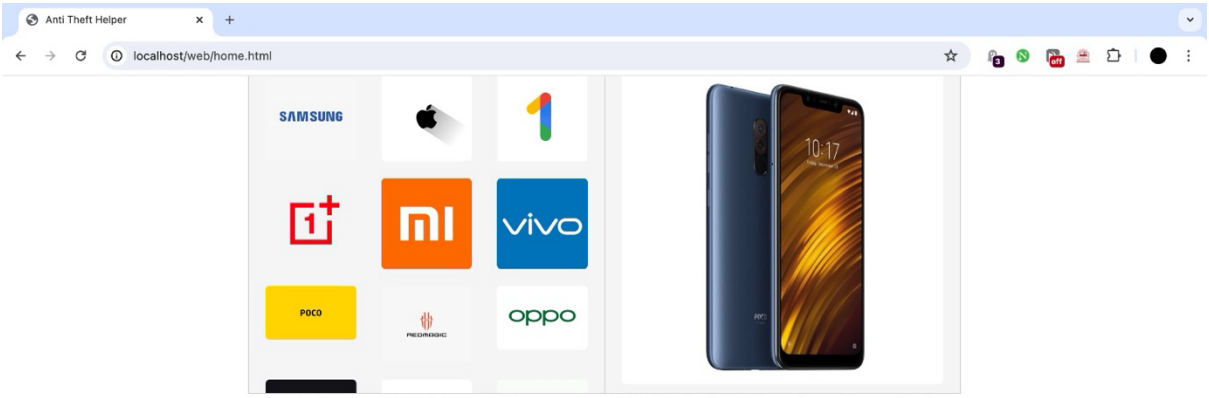

Anti-Theft Detection
Proximity Detection
Proximity
Detect Remove from Pocket
Motio n Dete ction
Motion
Charger Detection
Charger
Headset Detection
Password Set
Security Scan
This feature turn ON security scan every Download
Turn On


Anti-Theft Detection
Proximity Detection
Proximity
Detect Remove from Pocket
Motio n Dete ction
Motion
Charger Detection
Charger
Headset Detection
Security Scan
This feature turn ON security scan every Download
Turn On



5.5 WEBSITE AND APPLICATION PROGRESS:

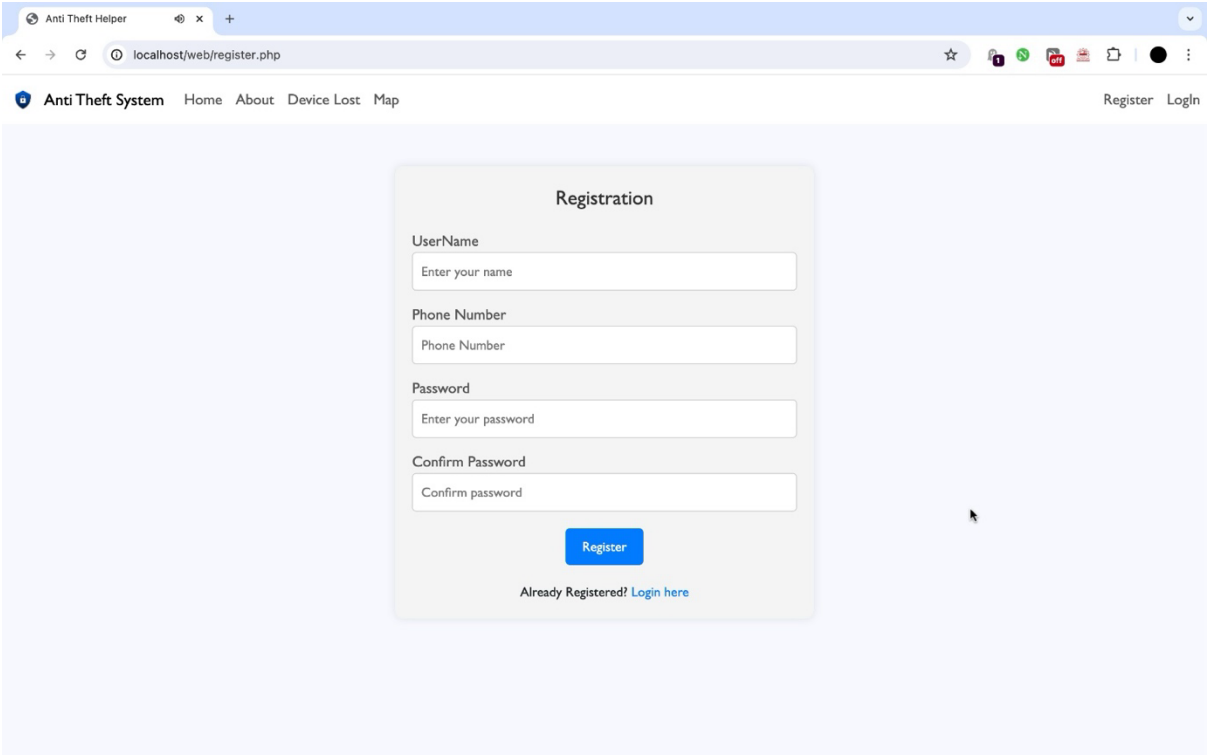


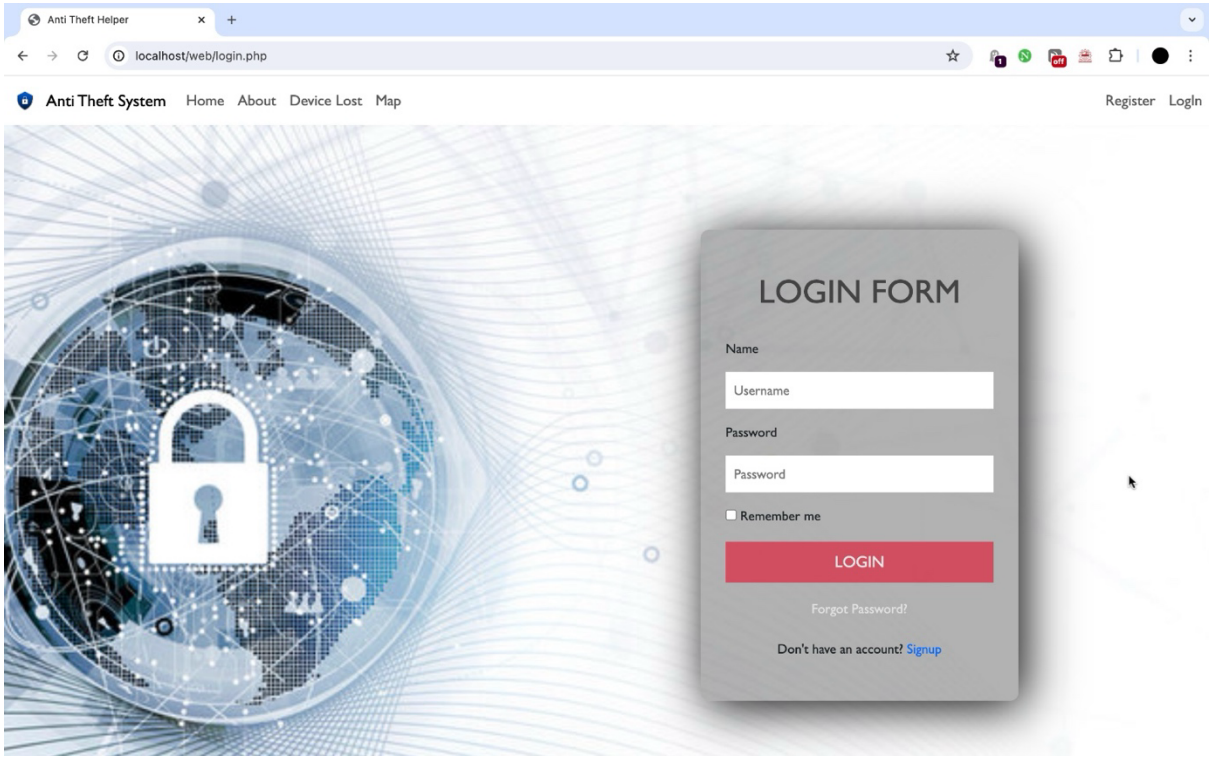


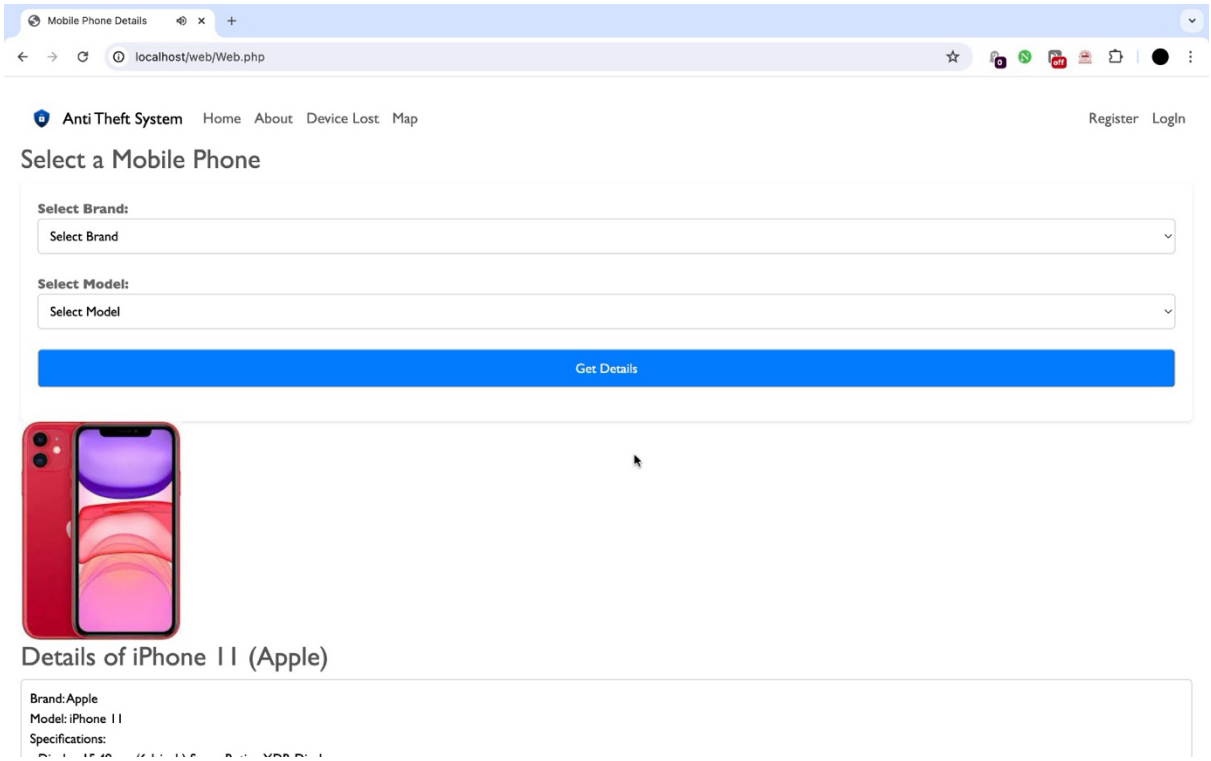
Upon selecting the specific cellphone model, users are provided with a detailed guide on what to do next after losing their phone. This includes steps on how to remotely lock, track, and erase data from the lost device, among other important actions.

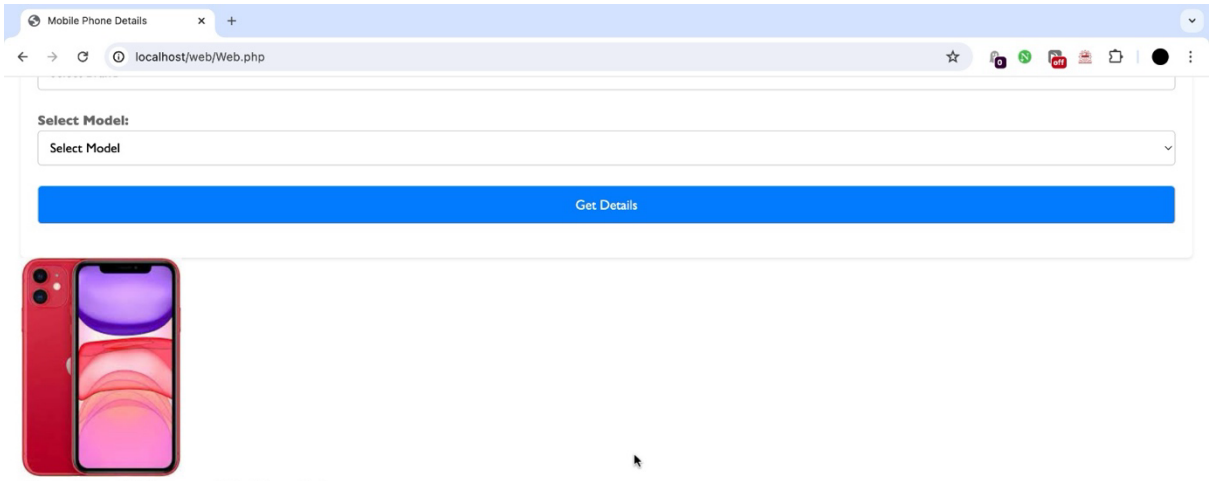
Global Mobile Lost Data(Map) ➜

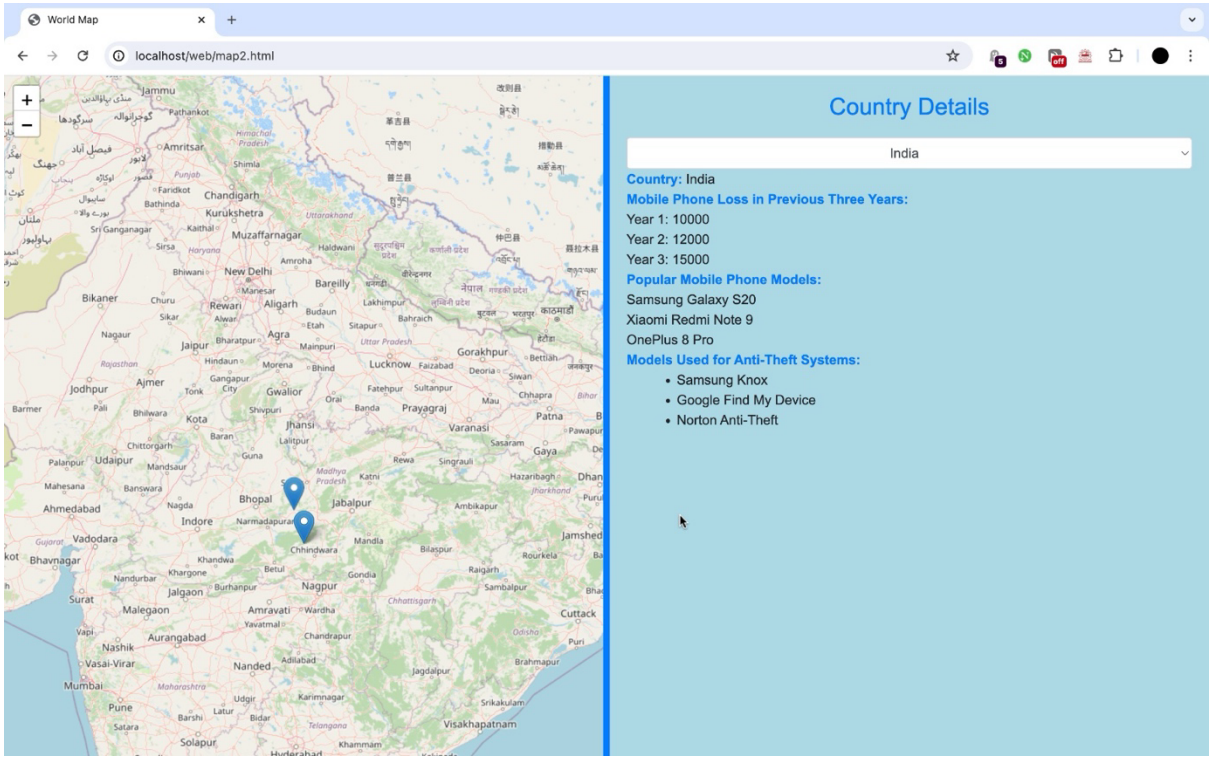
The website offers statistical data on the number of lost phones in various countries. This information is visualized using interactive embedded maps, allowing users to gain insights into the frequency and locations of phone losses globally.




Anti Theft Helper
localhost/web/login.php
Anti Theft System
Home
About
Device Lost
Map
Register
LogIn
LOGIN FORM
Name
Username
Password
Password
Remember me
LOGIN
Forgot Password?
Don't have an account? Signup


Mobile Phone Details
localhost/web/Web.php
Anti Theft System
Home
About
Device Lost
Map
Register
LogIn
Select a Mobile Phone
Select Brand:
Select Brand
Select Model:
Select Model
Get Details
Details of iPhone 11 (Apple)
Brand: Apple
Model: iPhone 11
Specifications:


Mobile Phone Details
localhost/web/Web.php
Select Model:
Select Model
Get Details
Details of iPhone 11 (Apple)
Brand: Apple
Model: iPhone 11
Specifications:
- Display: 15.49 cm (6.1 inch) Super Retina XDR Display
- Camera: 12MP + 12MP | 12MP Front Camera
- Storage: 64/128/256 GB
- Battery: 3000 mAh
- Processor: A13 Bionic Chip


World Map
localhost/web/map2.html
Country Details
India
Country: India
Mobile Phone Loss in Previous Three Years:
Year 1: 10000
Year 2: 12000
Year 3: 15000
Popular Mobile Phone Models:
Samsung Galaxy S20
Xiaomi Redmi Note 9
OnePlus 8 Pro
Models Used for Anti-Theft Systems:
Samsung Knox
Google Find My Device
Norton Anti-Theft

CHAPTER 6: CONCLUSION:

6.1 CONCLUSION:

In conclusion, the Anti-Theft Detection System for Android Phones embodies a comprehensive approach to enhancing device security and preventing unauthorized access. By leveraging motion detection algorithms, geolocation tracking techniques, and remote control features, the system aims to deter theft attempts effectively while empowering users with control over their device's security. Theoretical validations of the system's capabilities, including accurate detection with minimal false alarms, optimized performance, and continuous improvement through user feedback, reinforce its effectiveness in safeguarding devices and providing users with peace of mind. Through iterative development and adaptation, the system remains responsive to evolving security threats and user requirements, ensuring a robust and reliable solution for protecting Android smartphones against theft and unauthorized access.

6.2 FUTURE ENHANCEMENT:

1. Artificial Intelligence Integration: Integrate artificial intelligence (AI) algorithms to analyse user behaviour patterns and device usage, enabling the system to adapt its security measures dynamically. AI could also improve the accuracy of theft detection by learning from past incidents and continuously refining its detection algorithms.

2. Biometric Authentication: Implement biometric authentication methods, such as fingerprint or facial recognition, for accessing the device remotely. This additional layer of security would prevent unauthorized access to remote control features and enhance the overall security of the system.

3. Blockchain-based Tracking: Explore the use of blockchain technology to create a decentralized and immutable ledger for tracking device movements and security events. Blockchain-based tracking would provide enhanced transparency, security, and integrity of device location data, facilitating more efficient device recovery and reducing the risk of tampering or data manipulation.

6.3 REFERENCE:

In addition to academic papers, we consulted reputable online resources and industry reports:

Mobile Security Blog by Trend Micro

This blog offers insights into the latest trends and developments in mobile security, including anti-theft technologies and best practices.

Annual Mobile Security Report by Verizon

The Verizon Mobile Security Report provides comprehensive analysis and statistics on mobile security threats and mitigation strategies, including theft prevention.

Mobile Security Guidelines by OWASP

The OWASP Mobile Security Project provides guidelines and resources for developing secure mobile applications, including anti-theft measures.

Mobile Device Security Tips by Federal Trade Commission (FTC)

The FTC's website offers practical tips and advice for consumers to protect their mobile devices from theft and unauthorized access.