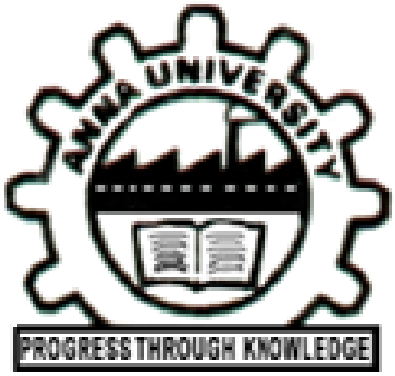
MADRAS INSTITUTE OF TECHNOLOGY

ANNA UNIVERSITY CHENNAI

CHENNAI - 600 044.



IT5613 SOCIALLY RELEVANT PROJECT LABORATORY

MOBILE ANTI-THEFT SYSTEM

6/8 B.TECH INFORMATION TECHNOLOGY

BATCH 1

TEAM 15

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

DATA COLLECTION :

LIST OF STOLEN MOBILES IN DIFFERENT COUNTRIES

Team Member : Gowri R (2021506025)

1. 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

2. Country: United Kingdom
   Mobile Phone Loss in Previous Three Years:
   Year 1: 8000
   Year 2: 9000
   Year 3: 10000
   Popular Mobile Phone Models:
   iPhone 11
   Samsung Galaxy S21
   OnePlus 9
   Models Used for Anti-Theft Systems:
   Find My iPhone
   Lookout Security
   Bitdefender Mobile Security

3. Country: Canada
   Mobile Phone Loss in Previous Three Years:
   Year 1: 5000
   Year 2: 6000
   Year 3: 7000
   Popular Mobile Phone Models:

iPhone SE
Google Pixel 4a
Samsung Galaxy A51
Models Used for Anti-Theft Systems:
Find My iPhone
Lookout Security
vast Anti-Theft

4. Country: Australia
   Mobile Phone Loss in Previous Three Years:
   Year 1: 6000
   Year 2: 7000
   Year 3: 8000
   Popular Mobile Phone Models:
   iPhone XR
   Samsung Galaxy S20 FE
   Google Pixel 5
   Models Used for Anti-Theft Systems:
   Find My iPhone
   Lookout Security
   AVG Antivirus

5. Country: Germany
   Mobile Phone Loss in Previous Three Years:
   Year 1: 9000
   Year 2: 10000
   Year 3: 11000
   Popular Mobile Phone Models:
   iPhone 12 Pro
   Samsung Galaxy S10
   Xiaomi Mi 11
   Models Used for Anti-Theft Systems:
   Find My iPhone
   Lookout Security
   Kaspersky Anti-Theft

6. Country: Brazil
   Mobile Phone Loss in Previous Three Years:
   Year 1: 12000
   Year 2: 13000
   Year 3: 14000
   Popular Mobile Phone Models:

Samsung Galaxy A71
Motorola Moto G Power
Xiaomi Redmi Note 8
Models Used for Anti-Theft Systems:
Find My iPhone
Lookout Security
F-Secure SAFE

7. Country: Russia
   Mobile Phone Loss in Previous Three Years:
   Year 1: 11000
   Year 2: 12000
   Year 3: 13000
   Popular Mobile Phone Models:
   Samsung Galaxy A52
   iPhone SE 2020
   Xiaomi Redmi 9
   Models Used for Anti-Theft Systems:
   Find My iPhone
   Kaspersky Anti-Theft
   Dr.Web Security Space

MOBILE BRANDS AND MODEL SPECIFICATION

Team Member : Jagadeesh R (2021506314)

Brand : Samsung

Model	Specification
Galaxy S20	Display: 15.71 cm (6.2 inch) Full HD+ Display Camera: 12MP + 10MP | 8 MP Front Camera RAM: 8 GB, Storage: 128/256 GB Battery: 4000 mAh Processor: Exynos 990
Galaxy S24	Display: 15.49 cm (6.1 inch) Full HD+ Display Camera: 50MP + 12MP + 10MP | 12MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 3900 mAh Processor: Snapdragon 8 Gen 3

Galaxy S24 Ultra	Display: 17.27 cm (6.8 inch) Quad HD+ Display Camera: 200MP + 10MP + 12MP + 10MP | 12MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 5000 mAh Processor: Snapdragon 8 Gen 3

Brand : Apple

Model	Specification
iPhone SE	Display: 11.94 cm (4.7 inch) Retina HD Display Camera: 12MP Rear Camera | 7MP Front Camera Storage: 64/128 GB Battery: 3000 mAh Processor: A15 Bionic Chip
iPhone 15	Display: 15.49 cm (6.1 inch) Super Retina XDR Display Camera: 48MP + 12MP | 12MP Front Camera Storage: 128/256/512 GB Battery: 4000 mAh Processor: A16 Bionic Chip
iPhone 15 Pro	Display: 15.49 cm (6.1 inch) Super Retina XDR Display Camera: 48MP + 12MP + 12MP | 12MP Front Camera Storage: 128/256/512 GB Battery: 4200 mAh Processor: A17 Pro Chip

Brand : Google

Model	Specification
Pixel 7 Pro	Display: 17.02 cm (6.7 inch) Quad HD+ Display Camera: 50MP + 48MP + 12MP | 10.8MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 4926 mAh Processor: Google Tensor G2
Pixel 8	Display: 15.75 cm (6.2 inch) Full HD+ Display Camera: 50MP + 12MP | 10.5MP Front Camera RAM: 8/12 GB, Storage: 128/256 GB Battery: 4575 mAh Processor: Google Tensor G3
Pixel 8 Pro	Display: 17.02 cm (6.7 inch) Full HD+ AMOLED Display Camera: 50MP + 48MP + 48MP | 10.5MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 5050 mAh Processor: Google Tensor G3

Brand : Vivo

Model	Specification
V30	Display: 17.22 cm (6.78 inch) Full HD+ Display Camera: 50MP + 50MP | 50MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 5000 mAh Processor: Snapdragon 7 Gen 3
X100	Display: 17.22 cm (6.78 inch) Full HD+ Display Camera: 50MP + 50MP + 64MP | 32MP Front Camera RAM: 8/12/16 GB, Storage: 128/256/512 GB Battery: 5000 mAh Processor: Mediatek Dimensity 9300
X100 Pro	Display: 17.22 cm (6.78 inch) Full HD+ Display Camera: 50MP + 50MP + 50MP | 32MP Front Camera RAM: 12/16 GB, Storage: 128/256/512 GB Battery: 5000 mAh Processor: Mediatek Dimensity 9300

Brand : Nothing

Model	Specification
Phone 1	Display: 16.64 cm (6.55 inch) Full HD+ Display Camera: 50MP + 50MP | 16MP Front Camera RAM: 8/12 GB, Storage: 128/256 GB Battery: 4500 mAh Processor: Snapdragon 778G+
Phone 2	Display: 17.02 cm (6.7 inch) Full HD+ Display Camera: 50 MP(OIS) +50MP | 32MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 4700 mAh Processor: Snapdragon 8+ Gen 1

Brand : Xiaomi

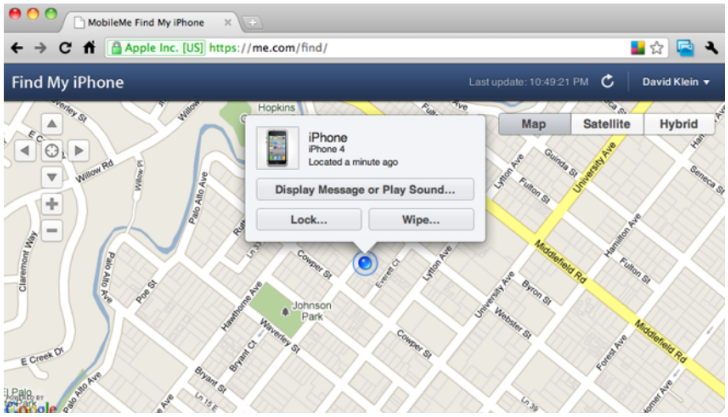
Model	Specification
14	Display: 17.09 cm (6.73 inch) Full HD+ Display Camera: 50MP + 16MP + 50MP | 32MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 4660 mAh Processor: Snapdragon 8 Gen 3
14 pro	Display: 17.09 cm (6.73 inch) Full HD+ Display Camera: 50MP + 50MP + 50MP | 32MP Front Camera RAM: 8/12 GB, Storage: 128/256/512 GB Battery: 4880 mAh Processor: Snapdragon 8 Gen 3

SEVERAL APPROACHES TO ANTI-THEFT SYSTEMS FOR MOBILE PHONES

Team Members : Ragul T (2021506067) | Revanth P (2021506323)

Find My iPhone (Apple) / Find My Device (Android):

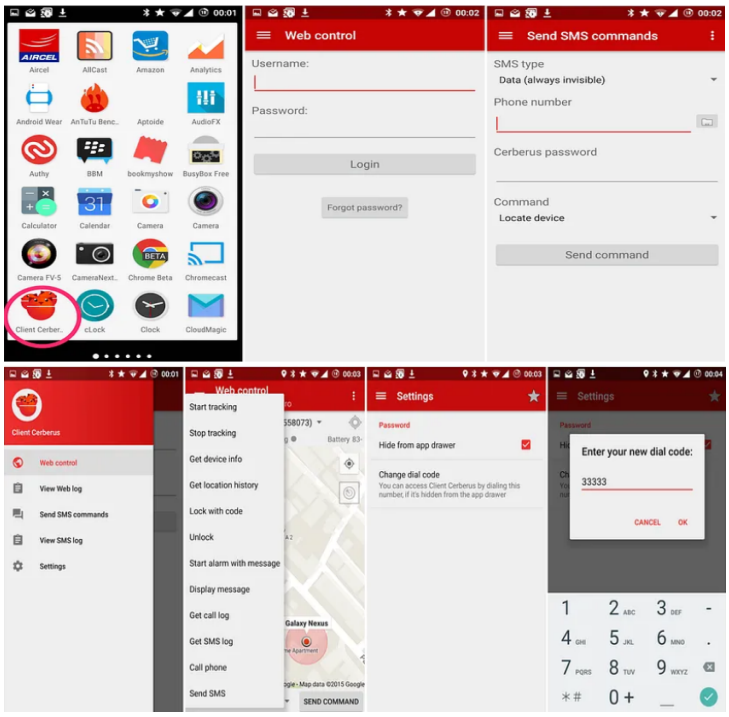
- Features: Both Find My iPhone and Find My Device offer similar features such as GPS tracking, remote lock and wipe, activation lock to prevent unauthorized use, and offline tracking using nearby Apple or Android devices.
- Target Users: Find My iPhone is specifically for Apple devices (iPhone, iPad, Mac, etc.), while Find My Device is for Android devices. These services are ideal for users of Apple and Android devices who want built-in anti-theft features.
- How to Use: Users need to enable these features in their device settings and sign in to their respective Apple or Google accounts. In case of theft or loss, users can log in to the respective online platforms (iCloud for Apple and Find My Device website for Android) to locate, lock, or erase their devices remotely.



Cerberus Anti-Theft (Android):

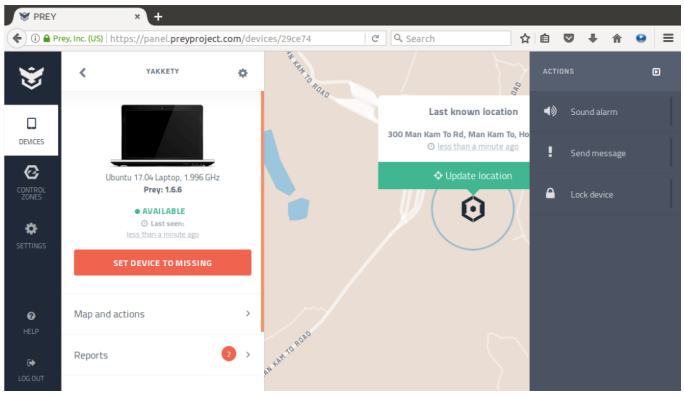
- Features: Cerberus offers advanced anti-theft features including remote control via SMS or website, GPS tracking, SIM card change detection, remote alarm, and capturing photos or videos of the thief.
- Target Users: Cerberus is designed for Android users who want robust anti-theft protection beyond built-in features.

- How to Use: Users need to install the Cerberus app on their Android device and set up their account. In case of theft or loss, users can access the Cerberus website or send SMS commands to remotely control their device and track its location.



Prey Anti-Theft (Cross-platform):

- Features: Prey offers cross-platform support for Windows, Mac, Linux, Android, and iOS devices, with features such as GPS tracking, remote lock and wipe, device alarm, camera capture, and Wi-Fi auto-connect.
- Target Users: Prey is suitable for users who want a unified anti-theft solution for multiple devices across different platforms.
- How to Use: Users need to install the Prey app on their devices and create an account. They can then use the Prey web dashboard to manage and track their devices remotely.

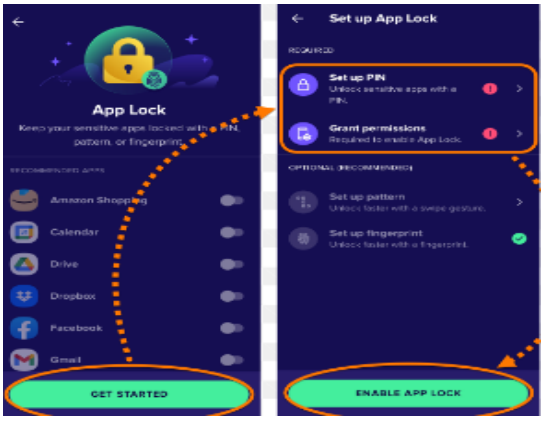


Lookout Security & Antivirus (Cross-platform):

- Features: Lookout provides anti-theft features such as device location tracking, remote lock and wipe, theft alerts, backup and restore capabilities, and malware protection.
- Target Users: Lookout is suitable for users who prioritize both anti-theft protection and overall device security.
- How to Use: Users can download and install the Lookout app from the respective app stores (Google Play Store for Android, Apple App Store for iOS). After setting up their account, they can access the various security features through the Lookout app.

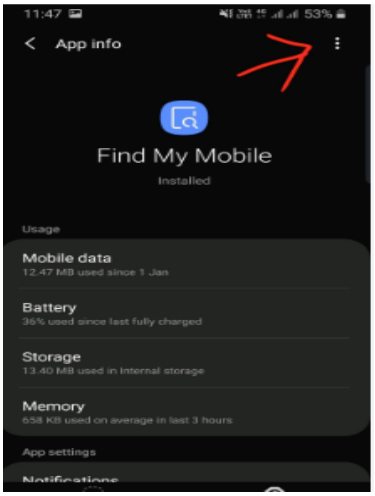
Avast Anti-Theft (Android):

- Features: Avast Anti-Theft includes remote control via SMS or web portal, GPS tracking, SIM card change notifications, remote lock and wipe, and stealth mode.
- Target Users: Avast Anti-Theft is designed for Android users seeking comprehensive anti-theft protection.
- How to Use: Users need to download and install the Avast Mobile Security app from the Google Play Store.



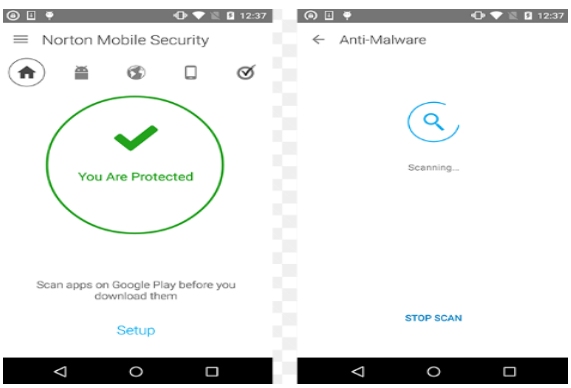
Samsung Find My Mobile (Samsung devices):

- Features: Samsung Find My Mobile offers features such as remote tracking, lock, and wipe, emergency mode, and backup and restore functionalities.
- Target Users: Samsung Find My Mobile is exclusively for users of Samsung devices.
- How to Use: Users with Samsung devices can access Find My Mobile by signing in with their Samsung account. They can then use the service to locate, lock, or erase their device remotely in case of loss or theft.



Norton Mobile Security (Cross-platform):

- Features: Norton Mobile Security provides features such as remote locate, lock, and wipe, SIM card lock, remote alarm, call and SMS blocking, and malware protection.
- Target Users: Norton Mobile Security is suitable for users who want a comprehensive security suite that includes anti-theft functionalities.
- How to Use: Users can download and install Norton Mobile Security from the respective app stores. After setting up their Norton account, they can access the anti-theft features through the Norton Mobile Security app.



Anti-Theft Phone Strap:

- Overview: A physical anti-theft solution in the form of a strap or band attached to the phone.
- Features: The strap is designed to secure the phone to the user's wrist or bag, making it difficult for thieves to snatch the device unnoticed. It can have a locking mechanism for added security.
- Target Users: Users who frequently travel in crowded areas or have concerns about pickpocketing.
- How to Use: Users can attach the anti-theft strap to their phone and wear it securely around their wrist or attach it to their bag. The strap can be easily detached when needed.

Motion-Activated Alarm:

- Overview: An alarm system triggered by motion to deter theft attempts.
- Features: The phone is equipped with motion sensors that detect movement when it's not in the user's possession. Upon detection, an alarm is triggered to alert nearby individuals and discourage theft.
- Target Users: Users who want an additional layer of security against theft, especially in public places.
- How to Use: Users can activate the motion-activated alarm feature on their phone through settings or a dedicated app. The alarm system remains active whenever the phone is left unattended.

Fingerprint Lockout:

- Overview: A security feature that locks the phone after a certain number of unsuccessful fingerprint authentication attempts.
- Features: The phone's fingerprint scanner is integrated with a lockout mechanism that temporarily disables access to the device after multiple failed attempts, preventing unauthorized access.
- Target Users: Users who prioritize biometric security and want to protect their phones from unauthorized access.
- How to Use: Users can enable the fingerprint lockout feature in their phone's security settings. They can set the number of allowed unsuccessful attempts before the lockout is activated.

Proximity-Based Locking:

- Overview: A feature that automatically locks the phone when it's moved away from the user's proximity.
- Features: The phone utilizes Bluetooth or NFC technology to detect when it's moved away from a paired device, such as a smartwatch or Bluetooth key fob. It automatically locks to prevent unauthorized access.

- Target Users: Users who want seamless security measures that adapt to their behavior and surroundings.
- How to Use: Users can pair their phone with a compatible device and enable the proximity-based locking feature in their phone's settings. The phone will lock automatically when the paired device moves out of range.

Voice Recognition Lock:

- Overview: A security feature that uses voice recognition technology to unlock the phone.
- Features: The phone's voice recognition system verifies the user's voice pattern to grant access to the device. It can be configured to recognize specific voice commands or phrases.
- Target Users: Users who prefer alternative biometric authentication methods and want enhanced security against unauthorized access.
- How to Use: Users can enroll their voice profile in the phone's settings and enable voice recognition as a security option. They can then unlock the phone by speaking the designated passphrase.

Invisible Ink Marking:

- Overview: A covert marking system to identify stolen phones and deter theft.
- Features: Users apply invisible ink to their phone, which contains a unique identifier or owner's information. Law enforcement agencies and retailers can use UV lights to reveal the marking and trace the phone back to its owner.
- Target Users: Users who want a discreet anti-theft measure that aids in identifying and recovering stolen phones.
- How to Use: Users can purchase kits containing invisible ink markers and instructions for application. They mark their phone discreetly in inconspicuous areas.

Dynamic Lock Code:

- Overview: A security feature that generates a new lock code at regular intervals to prevent unauthorized access.
- Features: The phone's lock screen displays a dynamic code that changes periodically (e.g., every minute or hour). Users must enter the current code to unlock the device, enhancing security against brute-force attacks.
- Target Users: Users who prioritize dynamic security measures and want to prevent unauthorized access to their phones.

- How to Use: Users can enable the dynamic lock code feature in their phone's settings. The phone generates a new code automatically at set intervals.

Remote Audio Monitoring:

- Overview: A feature that allows users to listen to ambient sounds near their phone remotely.
- Features: Users can activate the remote audio monitoring feature to listen to live audio captured by their phone's microphone. This can help identify the location of the phone and potential thieves.
- Target Users: Users who want additional tools for locating their stolen phone and gathering evidence for law enforcement.
- How to Use: Users can activate the remote audio monitoring feature through a dedicated app or online platform. They can listen to the live audio feed from their phone's microphone in real-time.

Biometric Voice Recognition:

- Overview: An advanced biometric authentication method that uses voice recognition technology.
- Features: The phone analyzes the user's voice patterns to authenticate their identity. This offers a secure and convenient way to unlock the device and access sensitive information.
- Target Users: Users who value advanced biometric security measures and want a hands-free authentication option.
- How to Use: Users can enroll their voice profile in the phone's settings and enable biometric voice recognition as a security option. They can then unlock the phone by speaking a passphrase or designated command.

Network-Based Lockdown:

- Overview: A security feature that automatically locks the phone when it detects suspicious activity or unauthorized access.
- Features: The phone analyzes network activity and user behavior to detect anomalies indicative of theft or hacking attempts. If suspicious activity is detected, the phone enters lockdown mode, restricting access to sensitive data.
- Target Users: Users who want proactive security measures that respond to potential threats in real-time.
- How to Use: Users can enable network-based lockdown in their phone's security settings. The phone continuously monitors network activity and triggers lockdown mode when necessary.

Augmented Reality Tracking:

- Overview: Utilizes augmented reality (AR) technology to assist in locating and recovering stolen phones.
- Features: Users can activate the AR tracking feature, which overlays digital markers or directions onto the phone's camera feed to guide them toward the device's location. This visual aid enhances the accuracy and efficiency of theft recovery efforts.
- Target Users: Users who prefer visual cues and immersive experiences for locating their stolen phones in real-world environments.
- How to Use: Users can activate the AR tracking feature through a dedicated app or online platform. They can then use their phone's camera to view the AR markers and follow the directions to retrieve their stolen device.

Self-Destruct Mode:

- Overview: A security feature that initiates a self-destruct sequence to render the phone unusable in case of theft.
- Features: When activated, the self-destruct mode triggers irreversible actions such as wiping the device's memory, disabling essential functions, and rendering the phone inoperable. This discourages theft by making the stolen device worthless to thieves.
- Target Users: Users who prioritize protecting their data and want a last-resort measure to prevent unauthorized access to their phones.
- How to Use: Users can activate the self-destruct mode through a dedicated app or online platform. They should carefully consider the consequences, as activating this feature results in permanent data loss and renders the phone unusable.

Community-Based Tracking Network:

- Overview: Establishes a network of users and volunteers to assist in tracking and recovering stolen phones collaboratively.
- Features: Users can opt into the community-based tracking network, allowing their phones to contribute anonymized location data to a centralized platform. When a phone is reported stolen, volunteers within the network receive notifications and assist in locating the device by sharing sightings and providing support.
- Target Users: Users who value community-driven initiatives and want to leverage collective efforts for theft recovery.
- How to Use: Users can opt into the community-based tracking network through a dedicated app or online platform. They can report stolen phones to activate the network's assistance and contribute to the recovery efforts of others.

Electromagnetic Disruption Field:

- Overview: Utilizes electromagnetic technology to create a localized disruption field around the phone, rendering it temporarily inoperable when stolen.
- Features: The phone is equipped with electromagnetic emitters that emit pulses to create a disruption field within a short radius. When the phone is reported stolen, users can activate the disruption field remotely, causing the stolen device to malfunction and become unusable.
- Target Users: Users who want a proactive approach to deter theft and render stolen phones worthless to thieves.
- How to Use: Users can activate the electromagnetic disruption field through a dedicated app or online platform. The disruption field should only be activated in situations where the phone is confirmed stolen, as it may affect nearby electronic devices.

Biometric Authentication Chain:

- Overview: Establishes a chain of biometric authentication across multiple devices to prevent unauthorized access to stolen phones.
- Features: Users link their mobile phone to other personal devices such as smartwatches, tablets, or laptops, creating a biometric authentication chain. To unlock the phone, users must authenticate themselves via biometric data (e.g., fingerprint, facial recognition) on one of the linked devices within a specified time frame.
- Target Users: Users who want a multi-layered security approach that requires authentication from multiple trusted devices to access their phones.
- How to Use: Users can establish the biometric authentication chain through a dedicated app or online platform. They need to enroll their biometric data on each linked device and configure the authentication settings accordingly.

Dynamic Encryption Key:

- Overview: Utilizes dynamic encryption keys to protect the data on the phone, rendering it unreadable in case of theft.
- Features: The phone generates a new encryption key at regular intervals, encrypting the stored data with the current key. If the phone is reported stolen, users can remotely revoke the current encryption key, making the data inaccessible to unauthorized users.
- Target Users: Users who prioritize data security and want to prevent unauthorized access to their sensitive information.

- How to Use: Users can enable the dynamic encryption key feature in their phone's security settings. They can remotely revoke the current encryption key through a dedicated app or online platform in case of theft.

Decoy Mode:

- Overview: Creates a decoy environment on the phone to deceive thieves and protect sensitive data.
- Features: When activated, the phone enters decoy mode, displaying a simulated interface with fake data and apps. Meanwhile, the real data and apps are hidden or encrypted, protecting them from unauthorized access.
- Target Users: Users who want to deter theft by disguising their valuable data and making the phone less attractive to thieves.
- How to Use: Users can activate decoy mode through a dedicated app or online platform. They can customize the decoy environment to mimic their typical usage patterns while keeping their real data secure.

Dynamic Behavioral Analysis:

- Overview: Utilizes machine learning algorithms to analyze user behavior and detect anomalies indicative of theft.
- Features: The phone continuously monitors the user's behavior patterns, such as usage habits, location history, and biometric data.
- If deviations from the norm are detected (e.g., unusual usage patterns or unfamiliar biometric data), the phone triggers an alert and activates anti-theft measures.
- Target Users: Users who want proactive security measures that adapt to their behavior and provide real-time threat detection.
- How to Use: Users can enable dynamic behavioral analysis in their phone's security settings. The phone uses machine learning algorithms to analyze user behavior and identify potential theft or unauthorized access attempts.

Tamper-Proof Hardware Module:

- Overview: Integrates a tamper-proof hardware module into the phone's design to prevent unauthorized access and tampering.
- Features: The hardware module contains secure storage for sensitive data and cryptographic keys. It also includes sensors to detect physical tampering attempts, such as opening the device casing or removing components. If tampering is detected, the module triggers security measures to protect the data and alert the owner.
- Target Users: Users who require robust protection against physical tampering and unauthorized access to their devices.

- How to Use: Users benefit from the tamper-proof hardware module's protection automatically, as it is integrated into the phone's design and operates continuously in the background.

Social Media Lockdown:

- Overview: Employs social media integration to aid in theft recovery efforts and discourage unauthorized access.
- Features: Users can link their social media accounts (e.g., Facebook, Twitter) to their phone's anti-theft system. In case of theft, the system posts automated messages to the user's social media profiles, alerting friends and followers about the theft and soliciting assistance in locating the device.
- Target Users: Users who want to leverage their social networks for theft recovery and increase awareness about stolen devices.
- How to Use: Users can connect their social media accounts to the anti-theft system through a dedicated app or online platform. They can configure the system to post automated messages in the event of theft.

Intelligent Lockdown Zones:

- Overview: Defines intelligent lockdown zones based on user-defined criteria to enhance security in specific locations.
- Features: Users can designate certain geographic areas (e.g., home, workplace) as lockdown zones within the anti-theft system. When the phone enters or leaves these zones, the system adjusts its security settings accordingly. For example, it may require additional authentication or activate theft deterrent measures when outside designated safe zones.
- Target Users: Users who want customizable security measures that adapt to different environments and locations.
- How to Use: Users can define and configure intelligent lockdown zones through the anti-theft system's settings or a dedicated app. They can specify criteria such as location boundaries and desired security actions for each zone.

Remote Access Sandbox:

- Overview: Creates a secure sandbox environment on the phone that allows remote access for authorized users.
- Features: The sandbox environment isolates sensitive data and apps from the rest of the device, providing a secure space for remote access and management. Authorized users can remotely access the sandbox to retrieve data, track the device's location, or perform maintenance tasks without compromising the phone's security.

- Target Users: Users who require remote access to their devices for management or recovery purposes while maintaining data security.
- How to Use: Users can activate and configure the remote access sandbox through the anti-theft system's settings or a dedicated app. They can grant access permissions to authorized users and define the scope of actions allowed within the sandbox environment.

Intelligent Theft Prediction:

- Overview: Utilizes predictive analytics and machine learning algorithms to anticipate and prevent theft before it occurs.
- Features: The anti-theft system analyzes various factors such as user behavior, location data, and environmental conditions to identify patterns indicative of potential theft incidents. If a high-risk situation is detected, the system proactively activates security measures or sends alerts to the user to prevent theft.
- Target Users: Users who want proactive theft prevention measures that leverage predictive analytics and advanced algorithms.
- How to Use: Users can enable intelligent theft prediction in the anti-theft system's settings.