A

Project Report

on

"A NOVEL MODEL FOR FRAUD DETECTION OF SHORT FUELING BY DISTRACTION"

Submitted in partial fulfillment of requirement for the degree

of

Bachelor of Engineering

in

Computer Engineering

Under Faculty of Science & Technology

Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur

Submitted By

Ms. Angadha Pawade **Mr. Rahul Nagalkar**

Mr. Sahil Telgote **Ms. Shweta Thakre**

Ms. Sonali Dangare **Ms. Vrushali Pohane**

Under the guidance of

Prof. K. V. Warkar

Assistant Professor

Department of Computer Engineering

Bapurao Deshmukh College of Engineering,
Sevagram-442102

(Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur)

Session: 2022-23

A

Project Report

on

“A NOVEL MODEL FOR FRAUD DETECTION OF SHORT FUELING BY DISTRACTION ”

Submitted in partial fulfillment of requirement for the degree

of

Bachelor of Engineering

in

Computer Engineering

Under Faculty of Science & Technology

Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur

Submitted By

Ms. Angadha Pawade

Mr. Sahil Telgote

Ms. Sonali Dangare

Mr. Rahul Nagalkar

Ms. Shweta Thakre

Ms. Vrushali Pohane

Under the guidance of

Prof. K. V. Warkar

Assistant Professor

Department of Computer Engineering

Bapurao Deshmukh College of Engineering,

Sevagram-442102

(Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur)

Session: 2022-23

Declaration

We **“Ms. Angadha Pawade, Mr. Rahul Nagalkar, Mr. Sahil Telgote, Ms. Shweta Thakre, Ms. Sonali Dangare, Ms. Vrushali Pohane”** hereby declare that the project titled **“A Novel Model for Fraud Detection of Short Fueling by Distraction”** is our own work carried out under the guidance of “**Prof. K. V. Warkar”** in **Department of Computer Engineering,** at **BDCE, Sevagram**. This work in the same form is not submitted by us at any other institute for the award of a degree.

Name of Students	**Signature**
Ms. Angadha Pawade	
Mr. Rahul Nagalkar	
Mr. Sahil Telgote	
Ms. Shweta Thakre	
Ms. Sonali Dangare	
Ms. Vrushali Pohane	

Certificate

The project titled **“A Novel Model for Fraud Detection of Short Fueling by Distraction”** submitted by “**Ms. Angadha Pawade, Mr. Rahul Nagalkar, Mr. Sahil Telgote, Ms. Shweta Thakre, Ms. Sonali Dangare, Ms. Vrushali Pohane”** is partial fulfillment of requirement for the award of degree of **Bachelor of Engineering in Computer Engineering**, has been carried out under our supervision at the **Department of Computer Engineering of Bapurao Deshmukh College of Engineering, Sevagram.**

PROF. K. V. WARKAR
Project guide
CE Department.

PROF. S. V. RAUT
Project Incharge
CE Department

DR. A. N. THAKRE
Head of Department
CE Department.

DR. G. V. THAKRE
Principal
BDCE, Sevagram

External Examiner

Name: -

Date: - / /2023

ACKNOWLEDGMENT

On the submission of our Mega Project report of **"A Novel Model for Fraud Detection of short Fueling by Distraction",** We would like to extend our gratitude & sincere thanks to our Guide **Prof. K. V. Warkar** for his constant motivation and support during the course of our work. It is all because of his/her untiring endeavors, able guidance and valuable suggestions, that could synchronize our efforts in covering the many diverse features of the project and thus helped us for the smooth progress and success of the project.

We would also like to extend our sincere thanks with gratitude to **Dr. A. N. Thakare, HOD(CE)** for his constant motivation and guidance during the course of our work.

We would also like to thank with gratitude to **Dr. G. V. Thakre, Principal, BDCE, Sewagram** for giving us an opportunity to complete our Mega Project in the college and for providing the necessary facilities.

We also thank all whose direct and indirect support helped us in completing our project work in time. Last but not least, we would like to thank almighty and our parents, for their support and co-operation in completing the project work. We would like to share this moment of happiness with them.

Name of projectees:

Ms. Angadha Pawade,
Mr. Rahul Nagalkar,
Mr. Sahil Telgote,
Ms. Shweta Thakre,
Ms. Sonali Dangare,
Ms. Vrushali Pohane

VIIIth Sem. CE Deptt.,
BDCE, Sevagram.

CONTENTS

Contents	**Page No.**
List of Figures	**i**
List of Screenshots	**ii**
ABSTRACT	**iii**
Chapter 1 INTRODUCTION	**1**
1.1 Motivation	2
1.2 Scope of Work	2
Chapter 2 LITERATURE REVIEW	**5**
2.1 Background History	8
2.2 Existing Systems	9
2.2 Limitations	10
Chapter 3 METHODOLOGY	**11**
3.1 Problem Definition	11
3.2 Technical Background	11
3.2.1 Hardware Description	12
3.2.2 Software Description	12
Chapter 4 PROPOSED WORK	**14**
4.1 Proposed System	14
Chapter 5 DESIGN AND IMPLEMENTATION	**15**
5.1 The working of power button service	15
5.2 The power screen	17
5.3 The SMS sending functionality	18

5.4 Creating a custom power off screen overlay 20

5.5 Presenting overlay screen 22

5.6 Device administration 23

5.7 Architecture 25

5.8 Flowchart 26

Chapter 6 RESULT AND ANALYSIS 27

6.1 Result 27

6.2 Analysis 28

Chapter 7 CONCLUSION AND FUTURE SCOPE 31

7.1 Conclusion 31

7.2 Future Scope 31

REFERENCES 33

PLAGIARISM REPORT

PATENTS SEARCH RESULT 43

LIST OF PAPERS PUBLISHED

CERTIFICATES 43

PROJECT GROUP PHOTO

PO ATTAINMENT

REVIEW AND CRITIQUE SHEET

LIST OF FIGURES

Sr. No.	**Name of Figures**	**Page No.**
1	Fig.4.1 Architecture Diagram	15
2	Fig.4.2 Flow Chart	16

LIST OF SCREENSHOTS

Sr. No.	Screenshots No.	Name of Screenshots	Page No.
1	Screenshot 3.1	Android Studio	13
2	Screenshot 5.1	Working of power button service	17
3	Screenshot 5.2	Power off screen activity	19
4	Screenshot 5.3	SMS Sending Functionality	20
5	Screenshot 5.4	Creating a custom poweroff screen overlay	22
6	Screenshot 5.5	Presenting overlay screen	24
7	Screenshot 5.6	Device Administration	25

ABSTRACT

As the world is progressing towards digitalization, owning a smartphone has become an essential requirement in today's society. In fact, not having a smartphone is almost unthinkable now. Recent data obtained under the Right To Information (RTI) act reveals that only 3.5% of lost phone cases were reported, indicating that the number of lost smartphones might be significantly higher than we think.

According to a study conducted by Kensington, a technology company, approximately 70 million smartphones are lost each year, with only 7% of them being recovered. This alarming figure highlights the importance of security and privacy of lost smartphones. Losing a smartphone can result in the loss of important data, such as personal photos, documents, and confidential information. Therefore, it is crucial to take measures to ensure the safety and privacy of such data.

To address this issue, we propose an improved approach to secure lost smartphones and protect personal data. By implementing advanced security measures, such as remote locking and data wiping, we can minimize the risk of data breaches and unauthorized access to personal information. Our approach aims to provide users with a reliable and efficient solution to safeguard their smartphones and personal data.

***Keywords* –** Android, Location, Tracing, Tracking, Switch-off, Lost smartphone, Missing smartphone.

Chapter 1

INTRODUCTION

In addition to the benefits mentioned earlier, our proposed system will also incorporate several advanced security features to protect the owner's data and prevent unauthorized access to the lost smartphone. For instance, the system will enable remote data wiping, which allows the owner to erase all sensitive information from the lost device, ensuring that it does not fall into the wrong hands. Additionally, the system will utilize biometric authentication to prevent unauthorized access to the device, thereby further enhancing its security.

To ensure the widespread adoption of our solution, we will collaborate with various smartphone manufacturers to incorporate our system into their devices. By doing so, we hope to provide a seamless and hassle-free experience for smartphone owners, enabling them to track and retrieve their lost devices effortlessly.

Moreover, we plan to leverage the power of big data and machine learning to analyze patterns of lost smartphone cases and identify potential areas of improvement in our system. This will enable us to continually enhance and optimize our solution to address new challenges and emerging threats in the digital landscape.

Finally, we recognize that our solution will not only benefit smartphone owners but also law enforcement agencies in recovering stolen devices. As such, we will work closely with local authorities to ensure that our system complies with relevant laws and regulations and facilitate their efforts to recover lost and stolen smartphones.

In conclusion, our proposed system aims to revolutionize the way we approach the issue of lost smartphones by providing a comprehensive, secure, and user-friendly solution. We are confident that our system will set a new benchmark for mobile security and privacy in the digital age and help alleviate the concerns of smartphone owners across the country.

1.1 Motivation

With India heading towards becoming a digital economy, it's no surprise that the number of smartphone users is expected to reach one billion by 2026. This growth is especially driven by rural areas where internet-enabled phones are becoming more accessible. However, with the increase in smartphone usage, the issue of theft and misplacement of phones has become a common problem. Most users simply accept their fate and do not take any action such as registering an FIR. Even those who do file a complaint see a low percentage of success in recovering their lost phone.

The situation calls for the development of a system that can aid in the recovery of lost or stolen phones, while also ensuring the security and privacy of users' personal data. The need for such a system cannot be overstated, as smartphones have become an integral part of our daily lives, containing important and sensitive information that needs to be safeguarded. Therefore, it is important to have a robust system in place that can not only help in recovering the lost phones but can also deter potential thieves and provide a sense of security to smartphone users.

1.2 Scope of Work

As digital technology advances, owning a smartphone has become a necessity in today's world. However, losing a smartphone has become a common issue, with Kensington's study revealing that 70 million smartphones are lost each year, and only 7 percent of them are ever recovered. Surprisingly, as per data obtained under the Right to Information (RTI) Act, only 3.5% of lost phone cases are registered. The consequences of losing a smartphone are severe, including the potential compromise of personal data, financial loss, and the inconvenience of losing an indispensable device.

To address this serious issue, we propose implementing an improved approach that ensures the security and privacy of lost smartphones while enabling their owners to retrieve them. Our strategy involves developing a comprehensive system that utilizes advanced technologies, including GPS and real-time tracking, to locate lost smartphones. This system will also send immediate notifications to the owner's registered phone number or email address, allowing them to take prompt action. Furthermore, our system will include enterprise-level security features, such as device encryption and remote wipe capabilities, to protect the owner's data from potential misuse.

To ensure the efficiency, robustness, and user-friendliness of our system, we will conduct thorough analysis and testing in real-world conditions. We aim to create a solution that not only addresses the problem of lost smartphones but also sets a new standard for mobile security and privacy. In addition to developing the technology, we plan to collaborate with law enforcement agencies to provide additional support to smartphone owners in recovering their lost devices. Our ultimate goal is to create a safer and more secure digital environment for all smartphone users in the country.The organization of the rest of the chapters is as follows:

Chapter 2 describes in detail the literature review of papers and the methods they used for their work using various techniques as a result, we surveyed every existing work.

Chapter 3 describes the methodology and the methods and techniques used to fully comprehend the design The chapter contains detailed information about the methods, and the flowchart of the proposed system shows how the proposed system works.

Chapter 4 describes a proposed project for planning the development of information systems by understanding and specifying in detail what a system should do and how the system's components should be implemented and work together.

Chapter 5 describes design and implementation as the carrying out, execution, or practice of a plan, method, or any design, idea, model, specification, standard, or policy for doing something. As such, implementation is the action that must follow any preliminary thinking in order for something to actually happen.

Chapter 6 describes the entire result and analysis of the proposed work, displaying both correct and incorrect results. It also explains how the system is more efficient than previous work.

Chapter 7 describes the conclusion and future scope of our project, highlighting both the positive and negative aspects of our proposed work. It also describes our project's future scope.

Chapter 2

LITERATURE REVIEW

The paper titled "Anti-theft application for android based devices" proposes a system that can help in securing android-based devices from theft. The authors have presented an application that can be used to track and recover lost or stolen mobile devices. The paper starts with a brief introduction of the growing trend of smartphone thefts and the need for a reliable security system.

The authors have conducted a detailed literature review of the existing anti-theft systems and apps that are available for mobile devices. They have discussed the limitations and drawbacks of the existing systems and have identified the need for a better anti-theft application. The authors have also reviewed the Android operating system architecture and its security features.

The proposed system uses the Global Positioning System (GPS) to track the location of the stolen device. The system also provides remote locking and wiping of data on the device to prevent unauthorized access. The authors have provided a flowchart of the proposed system, and they have explained the working of each component in detail. The authors have also discussed the implementation of the system and the results of the testing conducted on the application.

Overall, the paper presents a detailed study of the anti-theft application for android-based devices. The authors have identified the limitations of the existing systems and have proposed a system that is more reliable and effective in securing mobile devices. The proposed system can be useful for individuals and organizations who want to protect their mobile devices from theft or unauthorized access.[1]

Lei et al. (2013) discuss the security threat of privacy theft attacks on Android smartphones that utilize sensor-based information. The authors highlight the potential for malicious apps to access sensitive information, such as location and accelerometer data, which can be used to identify users and track their movements. The paper also provides an overview of existing security solutions and limitations of current mobile security mechanisms in preventing such attacks.

The authors propose a novel security architecture that leverages trusted computing technologies to ensure the confidentiality and integrity of sensitive data collected by sensors. They suggest a trusted execution environment that isolates sensor data from the main operating system and uses cryptographic protocols to establish secure communication channels. The paper concludes with a discussion of the feasibility and potential impact of the proposed architecture.

Overall, Lei et al.'s (2013) work highlights the importance of addressing security threats associated with sensor-based information on mobile devices. The proposed architecture offers a promising solution to enhance privacy and security for mobile users, but further research is needed to evaluate its effectiveness in real-world scenarios. [2]

The study conducted by Ong et al. (2004) focused on the development of a proactive system for the detection and recovery of lost mobile phones. The researchers highlighted the fact that mobile phone theft is a significant problem worldwide, and there is a need for effective strategies to prevent or mitigate its impact.

The authors conducted a literature review of existing research on mobile phone theft and identified that most of the current solutions were reactive in nature, which means they only work after the phone has been lost or stolen. They argued that a proactive approach is needed to detect and recover lost mobile phones before they fall into the hands of thieves.

The proposed system uses the Global System for Mobile Communications (GSM) and Global Positioning System (GPS) technologies to locate the lost mobile phone. The system sends an alert to the owner's designated phone number and email address, and it also provides a link to a web-based interface to track the phone's location.

The authors concluded that the proposed system can provide an effective solution to mobile phone theft by allowing the owner to take immediate action to recover the lost phone. They suggested that the system could be further improved by integrating other technologies such as Bluetooth and Wi-Fi for more precise location tracking.

Overall, the study by Ong et al. (2004) presents a proactive approach to address the issue of mobile phone theft. The literature review conducted in the study provides valuable insights into existing solutions and highlights the need for a proactive approach. The proposed system is a promising solution that could help prevent the loss of valuable mobile phones. [3]

The article titled "A Software Tool for Recovering Lost Mobile Phones Using Real-time Tracking" by Arikpo and Osuobiem (2020) focuses on developing a software tool that enables users to recover lost mobile phones using real-time tracking. The authors explain that mobile phone theft is a common problem globally, and many people lose their phones daily, leading to the loss of valuable data and personal information.

The article begins by discussing the current methods used to recover lost mobile phones, such as filing a police report and contacting the network provider. However, these methods are not always effective, and the authors argue that a software tool that uses real-time tracking could be more efficient in locating lost mobile phones.

The authors then describe the methodology used to develop the software tool. They used Android Studio to develop the application, and the tool's primary function is to track the phone's location using GPS and send the location data to a secure server. The application also has other features, such as taking a photo of the thief and sending it to the phone owner's email address.

The authors conducted several tests to validate the software tool's effectiveness in recovering lost phones. The results showed that the tool can locate lost phones accurately and send real-time location updates to the phone owner.

Overall, the article by Arikpo and Osuobiem (2020) provides insight into the development of a software tool that can help recover lost mobile phones. The authors' research addresses an important problem and proposes a solution that can be useful to many people who have lost their phones. The study's findings demonstrate the effectiveness of the tool in real-world scenarios, highlighting its potential usefulness. [4]

2.1 Background History

The history of lost smartphones can be traced back to the early days of mobile phones. Prior to smartphones, losing a phone was often a minor inconvenience as it was primarily used for making calls and sending text messages. However, the advent of smartphones changed the game, as they became much more than just communication devices.

With the rise of smartphones, people started storing more and more personal and sensitive information on their devices, such as email accounts, social media profiles, bank account details, and more. Losing a smartphone thus became a much more serious matter, as it could potentially lead to identity theft, financial loss, or even blackmail.

In response to this, various software and hardware solutions have been developed to help people track and recover their lost smartphones. The first such solutions were basic phone tracking apps that relied on the phone's GPS signal to pinpoint its location. As technology advanced, more sophisticated solutions were developed, such as remote lock and wipe features, which allow users to protect their data in case their phone falls into the wrong hands.

2.2 Existing Systems

1.Google's Find My Device is a service that helps Android users locate, lock, or erase their lost or stolen devices. To use this service, the lost device must be turned on and connected to a Google Account with an active internet connection. Once logged into the Google Account, users can access the Find My Device service by going to android.com/find.

If there are multiple phones connected to the same Google Account, users can select the lost device from the top of the screen. If the lost device has multiple user profiles, users must sign in with a Google Account associated with the primary profile.

Once the lost device is selected, it will receive a notification from Google. Users can then see the approximate location of their device on a map. It is important to note that the location shown may not be completely accurate. If the lost device cannot be found, the service will show the last known location, if available.

In addition to locating the lost device, Find My Device also offers the option to lock or erase the device remotely. This can be useful in preventing unauthorized access to personal information or data. If the device is locked, users can set a message to display on the lock screen, such as contact information for the owner or a message to the person who may have found the device.

2. The CEIR initiative was launched in India in 2019 with the primary objective of curbing the circulation of counterfeit mobile phones and discouraging mobile phone theft. The CEIR acts as a central system for all network operators in India to share blacklisted devices to prevent their use on any other network, even if the Subscriber

Identity Module (SIM) card in the device is changed. The system is designed to connect to the International Mobile Equipment Identity (IMEI) database of all mobile operators in the country. IMEI is a unique identifier assigned to every mobile phone that allows it to be traced and located.

The CEIR system aims to protect consumer interest and facilitate lawful interception by law enforcement authorities. In case of a stolen or lost mobile phone, the user can report it to their network operator, who can then blacklist the device on the CEIR database. Once a device is blacklisted, it cannot be used on any other network, rendering it useless for any potential thieves or buyers of stolen phones. The CEIR system also enables law enforcement authorities to track the location of lost or stolen devices, as long as they are connected to a network.

The CEIR initiative is a significant step towards improving mobile phone security in India. It provides a centralized platform for all network operators to share information on blacklisted devices and ensures that stolen or lost phones are rendered useless, reducing the incentive for mobile phone theft. The system also helps in reducing the circulation of counterfeit mobile phones, which can be a potential threat to national security. By facilitating lawful interception, the CEIR system enables law enforcement authorities to track and prevent criminal activities using mobile phones.

2.3 Limitations

1) IMEIs can sometimes be removed from a blocklist, depending on local arrangements. This would typically include quoting a password chosen at the time of block listing.
2) IMEI tracking is expensive and cannot be done without legal interference
3) Tracking is not possible in case of internet disconnection and if the tracking services are not setup (e.g. Google Find my device)
4) Once the device get switch-off no existing system can work.

Chapter 3

METHODOLOGY

3.1 Problem Definition

The proposed system has a clear problem definition: to locate a missing smartphone, regardless of whether it has been turned off or not. To achieve this goal, the system must continue to function even if the phone is turned off.

The methodology involves incorporating different technologies such as GPS, cellular data, SMS, and Wi-Fi to track the phone's location. When the system is turned on, these technologies are activated, allowing the phone's location to be traced. In addition, if someone tries to turn off the phone, it will go to sleep instead of turning off completely, making it trackable even after a switch-off attempt.

The system's functioning is based on real-time tracking, allowing the phone's location to be determined accurately. This method can help to recover lost or stolen smartphones, even if the thief switches off the device. It is essential to note that the system only becomes inoperable when it is turned off, making it possible to track the phone's location as long as the system is running.

3.2 Technical Background:

The technical background for securing lost smartphones and protecting personal data involves a combination of smartphone security features, GPS and location tracking, remote control capabilities, central server management, application development, data security, and user privacy considerations. By leveraging these technologies effectively, a comprehensive solution can be developed to address the increasing concern of lost smartphones and safeguard user data.

3.2.1 Hardware Description

I. Processor:

Core i3 processor-based Laptop or higher.

II. RAM:

4 GB RAM is recommended, 8 GB for better performance.

III. Hard Drive:

3 GB storage required.

IV. Internet Connection:

Internet connection is required to find the phone.

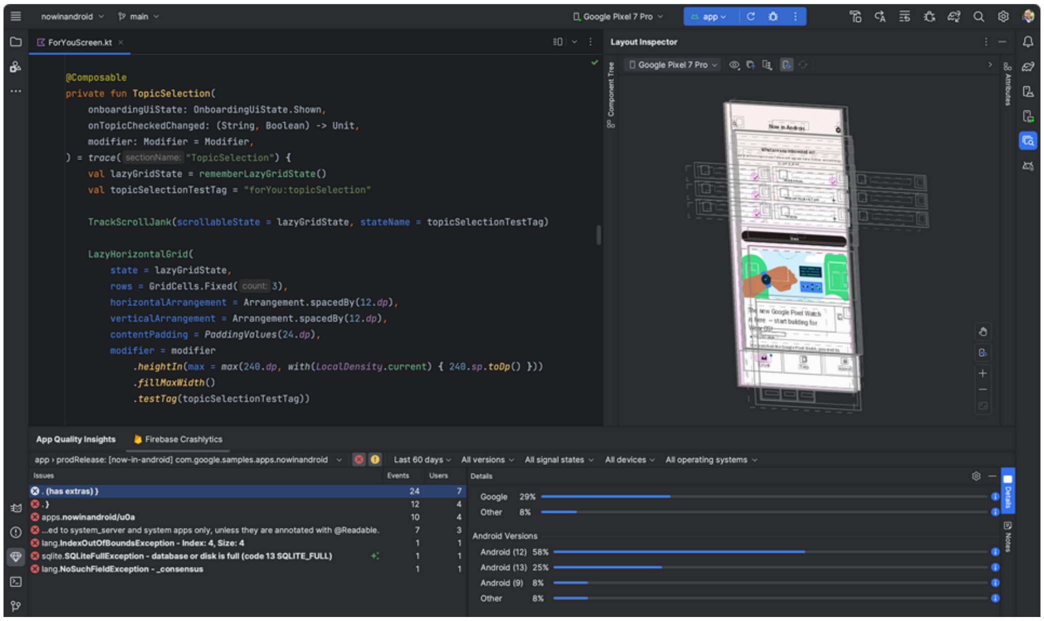
V. Smartphone:

A smartphone is required to run the application.

3.2.2 Software Description

I. IDE (Integrated Development Environment):

Android Studio is an Integrated Development Environment (IDE) designed for developing Android applications. It is the official IDE for Android app development and offers a range of features to enhance developer productivity. Based on IntelliJ IDEA, Android Studio provides a flexible Gradle-based build system, a fast emulator, and a unified environment to develop for all Android devices.



```kotlin
@Composable
private fun TopicSelection(
    onboardingUiState: OnboardingUiState.Shown,
    onTopicCheckedChanged: (String, Boolean) -> Unit,
    modifier: Modifier = Modifier,
) = trace( sectionName: "TopicSelection") {
    val lazyGridState = rememberLazyGridState()
    val topicSelectionTestTag = "forYou:topicSelection"

    TrackScrollJank(scrollableState = lazyGridState, stateName = topicSelectionTestTag)

    LazyHorizontalGrid(
        state = lazyGridState,
        rows = GridCells.Fixed( count: 3),
        horizontalArrangement = Arrangement.spacedBy(12.dp),
        verticalArrangement = Arrangement.spacedBy(12.dp),
        contentPadding = PaddingValues(24.dp),
        modifier = modifier
            .heightIn(max = max(240.dp, with(LocalDensity.current) { 240.sp.toDp() }))
            .fillMaxWidth()
            .testTag(topicSelectionTestTag))
```

app › prodRelease: [now-in-android] com.google.samples.apps.nowinandroid   Last 60 days   All versions   All signal states   All devices   All operating systems

Issues	Events	Users
. (has extras) }	24	7
.}	12	4
apps.nowinandroid/u0a	10	4
...ed to system_server and system apps only, unless they are annotated with @Readable.	7	3
lang.IndexOutOfBoundsException - Index: 4, Size: 4	1	1
sqlite.SQLiteFullException - database or disk is full (code 13 SQLITE_FULL)	1	1
lang.NoSuchFieldException - _consensus	1	1

```
Details
  Google        29%
  Other          8%
Android Versions
  Android (12)  58%
  Android (13)  25%
  Android (9)    8%
  Other          8%
```

Screenshot 3.1. Android Studio

II. Operating System:

Windows 8.1 or higher required to install the Andorid Studio

Chapter 4

PROPOSED WORK

4.1 Proposed System

Losing a smartphone can be a stressful and frustrating experience, especially if it contains important personal or business data. In response to this issue, various technological advancements have been developed to locate lost or stolen smartphones. One of the most widely used and popular tools for tracking lost or stolen Android devices is Google's Find My Device. This tool allows users to locate, lock, or erase their Android devices remotely. It is automatically enabled on all Android devices linked to a Google account and requires the device to be turned on, signed in to a Google account, connected to mobile data or Wi-Fi, visible on Google Play, and have the location and Find My Device features turned on.

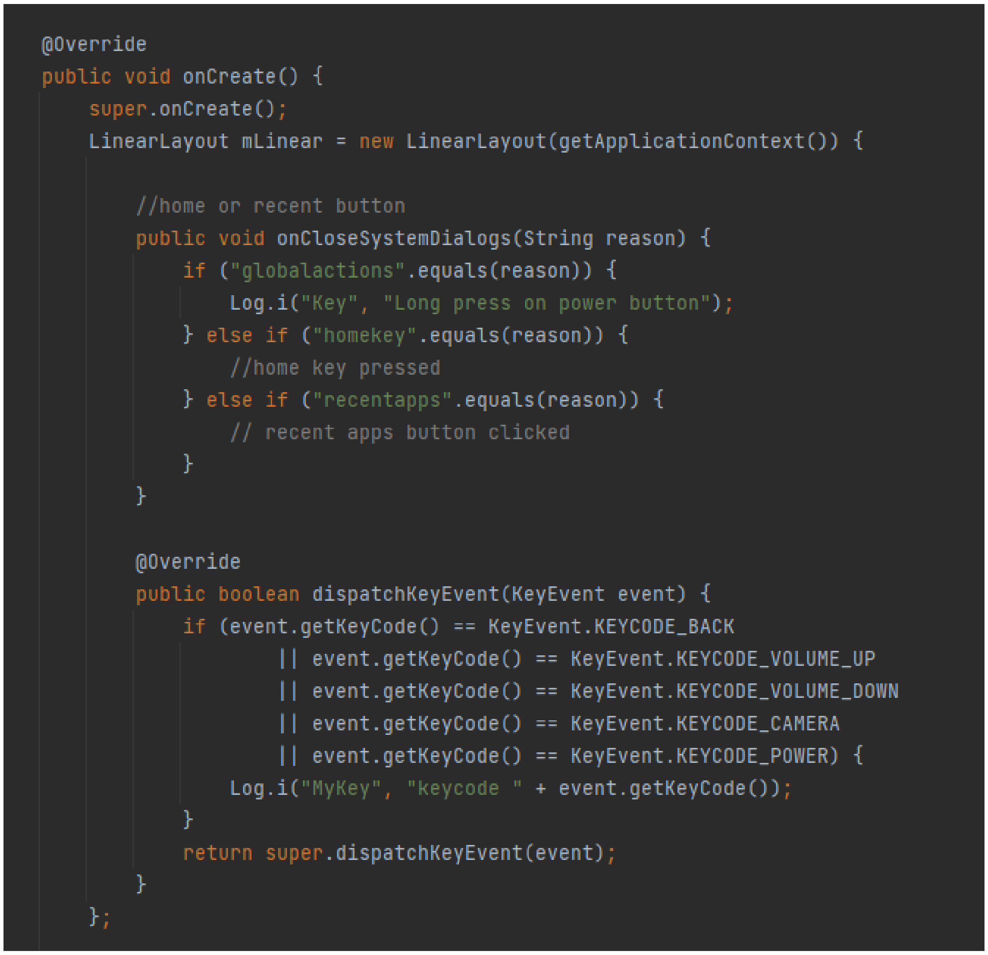
In addition to tools like Find My Device, governments and mobile network operators have also taken steps to combat smartphone theft through initiatives like the Central Equipment Identity Register (CEIR). The CEIR was developed in India with the goal of curbing the counterfeit mobile phone market and deterring mobile phone theft. It serves as a central system for all network operators to share blacklists, so if a device is blacklisted on one network, it will not work on another network, even if the SIM card is changed. This initiative not only helps protect consumers from stolen devices but also facilitates lawful interception by law enforcement authorities.

However, despite these advancements in technology and initiatives, the issue of lost or stolen smartphones remains prevalent. This has led to the development of various anti-theft applications, including those designed specifically for Android-based devices. These applications offer features such as remote locking and erasing of devices, as well as GPS tracking to locate the missing device. One such application is the Anti-Theft Application for Android-Based Devices, which was developed to recover lost smartphones even after they are switched off.

Chapter 5

DESIGN AND IMPLEMENTATION

5.1 The working of Power button service



```java
@Override
public void onCreate() {
    super.onCreate();
    LinearLayout mLinear = new LinearLayout(getApplicationContext()) {

        //home or recent button
        public void onCloseSystemDialogs(String reason) {
            if ("globalactions".equals(reason)) {
                Log.i("Key", "Long press on power button");
            } else if ("homekey".equals(reason)) {
                //home key pressed
            } else if ("recentapps".equals(reason)) {
                // recent apps button clicked
            }
        }

        @Override
        public boolean dispatchKeyEvent(KeyEvent event) {
            if (event.getKeyCode() == KeyEvent.KEYCODE_BACK
                    || event.getKeyCode() == KeyEvent.KEYCODE_VOLUME_UP
                    || event.getKeyCode() == KeyEvent.KEYCODE_VOLUME_DOWN
                    || event.getKeyCode() == KeyEvent.KEYCODE_CAMERA
                    || event.getKeyCode() == KeyEvent.KEYCODE_POWER) {
                Log.i("MyKey", "keycode " + event.getKeyCode());
            }
            return super.dispatchKeyEvent(event);
        }
    };
```

Screenshot 5.1 Working of Power button service

The given code is an implementation of the PowerButtonService class, which extends the Service class in Android. This service is responsible for handling events related to the power button and other key events.

When the service is created (onCreate()), it initializes a LinearLayout and overrides its methods to handle system dialogs and dispatch key events. The LinearLayout is given focus and a view is inflated from a layout file (R.layout.service_layout).

The WindowManager is then obtained from the system service, and WindowManager.LayoutParams are set based on the Android version. If the Android version is Oreo or higher, the layout params use the TYPE_APPLICATION_OVERLAY flag, which allows the window to be displayed over other applications. Otherwise, it uses the TYPE_PHONE flag.

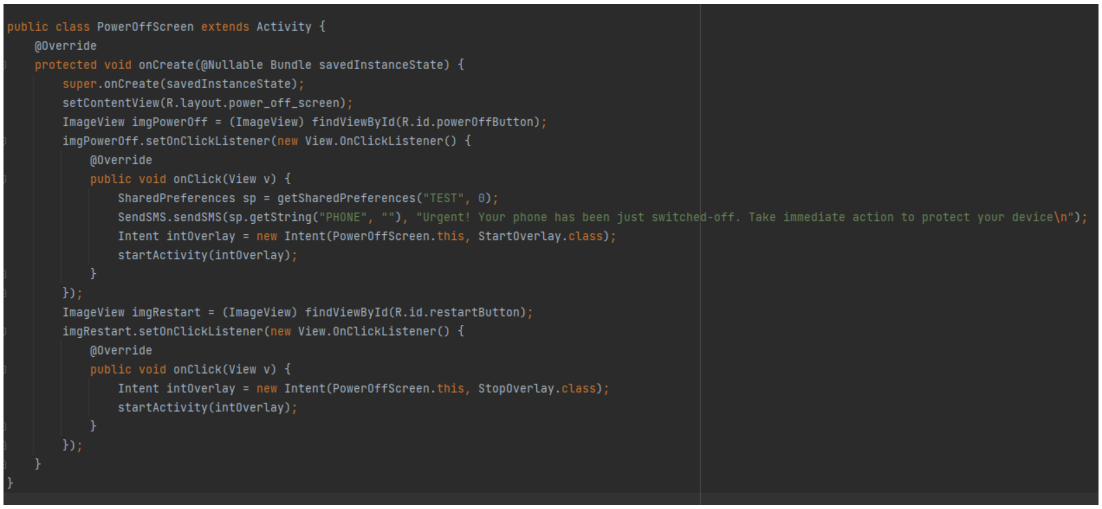
The layout parameters define the size, type, flags, and gravity of the window. The gravity is set to LEFT | CENTER_VERTICAL, positioning the window on the left side of the screen.

The code also sets click listeners on two ImageViews, imgTurnOff and imgTurnRestart. When imgTurnOff is clicked, it starts the AccessibilityOverlayService by creating an intent and calling startService().

Finally, a log message is printed to indicate that the service initialization is complete.

In summary, the PowerButtonService class creates a system service that handles power button events and key events, displays a window with specified layout parameters, and provides functionality to start another service based on user interaction.

5.2 The Power off screen



```java
public class PowerOffScreen extends Activity {
    @Override
    protected void onCreate(@Nullable Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.power_off_screen);
        ImageView imgPowerOff = (ImageView) findViewById(R.id.powerOffButton);
        imgPowerOff.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                SharedPreferences sp = getSharedPreferences("TEST", 0);
                SendSMS.sendSMS(sp.getString("PHONE", ""), "Urgent! Your phone has been just switched-off. Take immediate action to protect your device\n");
                Intent intOverlay = new Intent(PowerOffScreen.this, StartOverlay.class);
                startActivity(intOverlay);
            }
        });
        ImageView imgRestart = (ImageView) findViewById(R.id.restartButton);
        imgRestart.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                Intent intOverlay = new Intent(PowerOffScreen.this, StopOverlay.class);
                startActivity(intOverlay);
            }
        });
    }
}
```

Screenshot 5.2 Power off screen activity

This code snippet provided represents the implementation of the PowerOffScreen class, which extends the Activity class. This code is responsible for handling the functionality related to powering off and restarting the device through the user interface.

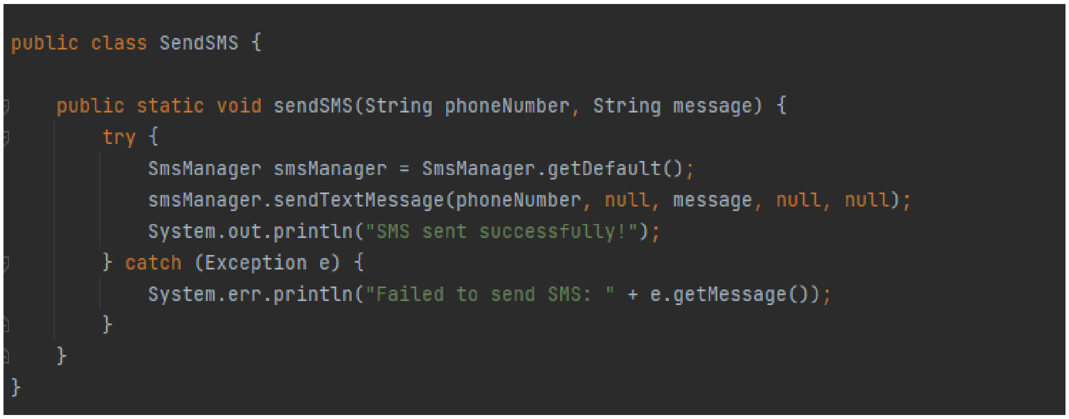
The onCreate() method is overridden to set up the necessary components and layout for the power off screen. It associates the layout file "power_off_screen.xml" with the activity using setContentView(). Two ImageViews, imgPowerOff and imgRestart, are initialized by finding their respective views in the layout.

For imgPowerOff, an onClickListener is set to handle the click event. When clicked, it retrieves the phone number stored in the SharedPreferences with the key "PHONE" and uses the SendSMS class to send an SMS message with the content "Phone Power OFF". Additionally, it creates an Intent for StartOverlay activity and starts it using startActivity().

Similarly, for imgRestart, another onClickListener is set. When clicked, it creates an Intent for the StopOverlay activity and starts it using startActivity().

In summary, this code handles the events when the user interacts with the power off and restart buttons in the power off screen. It performs actions such as sending an SMS message and starting specific activities based on the user's input.

5.3 The SMS Sending Functionality



```java
public class SendSMS {

    public static void sendSMS(String phoneNumber, String message) {
        try {
            SmsManager smsManager = SmsManager.getDefault();
            smsManager.sendTextMessage(phoneNumber, null, message, null, null);
            System.out.println("SMS sent successfully!");
        } catch (Exception e) {
            System.err.println("Failed to send SMS: " + e.getMessage());
        }
    }
}
```

Screenshot 5.3 SMS Sending Functionality

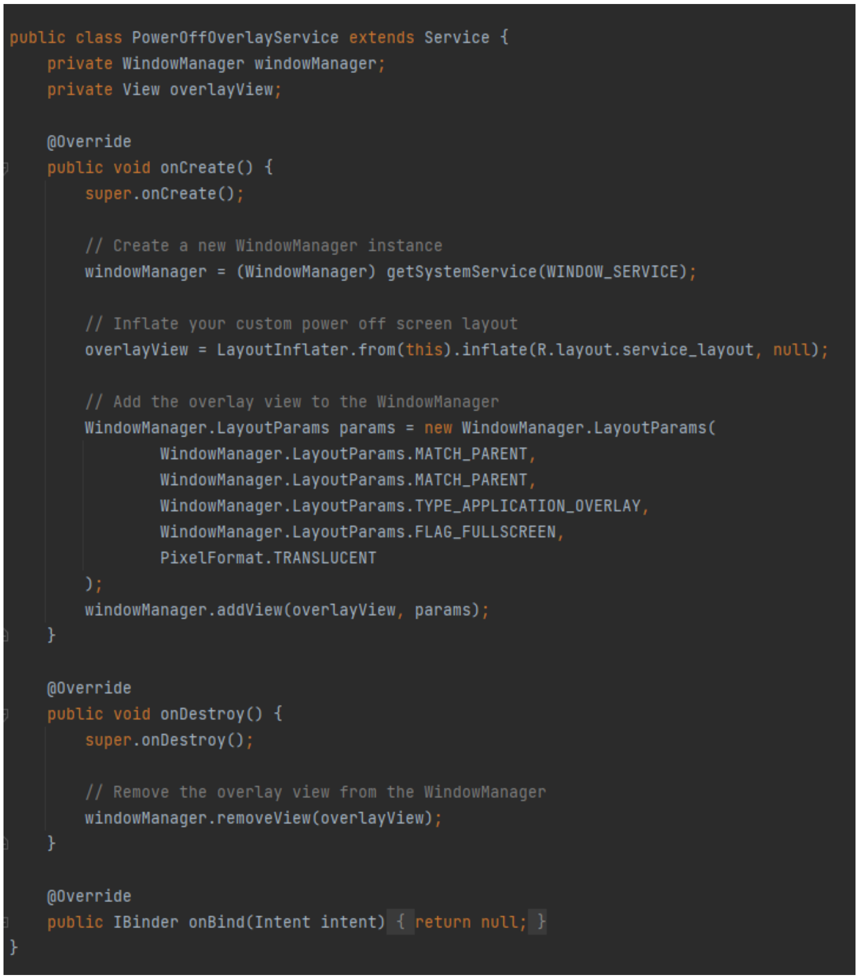
This code snippet implements a simple SMS sending functionality in Java. It defines a class called “SendSMS” with a static method named “sendSMS” that takes two parameters: phoneNumber (recipient’s phone number) and message (content of the SMS). Here is a pointwise summary of how the code works:

1. The class “SendSMS” contains a single static method, “sendSMS,” responsible for sending SMS messages.

2. Within the method, an instance of the SmsManager class is obtained by calling the “getDefault” method of the SmsManager class. This class provides the functionality to send SMS messages.
3. The “sendTextMessage” method of the SmsManager class is then called with the provided phoneNumber, null (indicating the default service center), message, null (indicating no PendingIntent for delivery reports), and null (indicating no PendingIntent for sent messages).
4. If the message is successfully sent without any exceptions, the console outputs the message “SMS sent successfully!”
5. If an exception occurs during the sending process, an error message is printed to the console, indicating the failure to send the SMS and providing the specific error message obtained from the caught exception.

Overall, this code snippet provides a straightforward implementation of sending SMS messages using the SmsManager class in Java, handling success and failure scenarios.

5.4 Creating a Custom Power Off Screen Overlay



```java
public class PowerOffOverlayService extends Service {
    private WindowManager windowManager;
    private View overlayView;

    @Override
    public void onCreate() {
        super.onCreate();

        // Create a new WindowManager instance
        windowManager = (WindowManager) getSystemService(WINDOW_SERVICE);

        // Inflate your custom power off screen layout
        overlayView = LayoutInflater.from(this).inflate(R.layout.service_layout, null);

        // Add the overlay view to the WindowManager
        WindowManager.LayoutParams params = new WindowManager.LayoutParams(
                WindowManager.LayoutParams.MATCH_PARENT,
                WindowManager.LayoutParams.MATCH_PARENT,
                WindowManager.LayoutParams.TYPE_APPLICATION_OVERLAY,
                WindowManager.LayoutParams.FLAG_FULLSCREEN,
                PixelFormat.TRANSLUCENT
        );
        windowManager.addView(overlayView, params);
    }

    @Override
    public void onDestroy() {
        super.onDestroy();

        // Remove the overlay view from the WindowManager
        windowManager.removeView(overlayView);
    }

    @Override
    public IBinder onBind(Intent intent) { return null; }
}
```

Screenshot 5.4 Creating a custom poweroff screen overlay

1. The "PowerOffOverlayService" is a class that extends the "Service" class in Android, responsible for creating a custom power off screen overlay.

2. The code utilizes the WindowManager to display a custom view on top of other applications.

3. In the "onCreate" method, the WindowManager instance is created, and a custom layout for the power off screen, defined in the "service_layout.xml" file, is inflated using LayoutInflater.

4. The overlay view is added to the WindowManager using a set of WindowManager. LayoutParams. These parameters define the size, type, flags, and format of the overlay view.

5. The overlay view is set to occupy the entire screen by using MATCH_PARENT for both width and height.

6. The type of the overlay view is set to TYPE_APPLICATION_OVERLAY, allowing it to be displayed on top of other applications.

7. The FLAG_FULLSCREEN flag ensures that the overlay view is displayed in full-screen mode.

8. The overlay view is displayed with a transparent background using the TRANSLUCENT format.

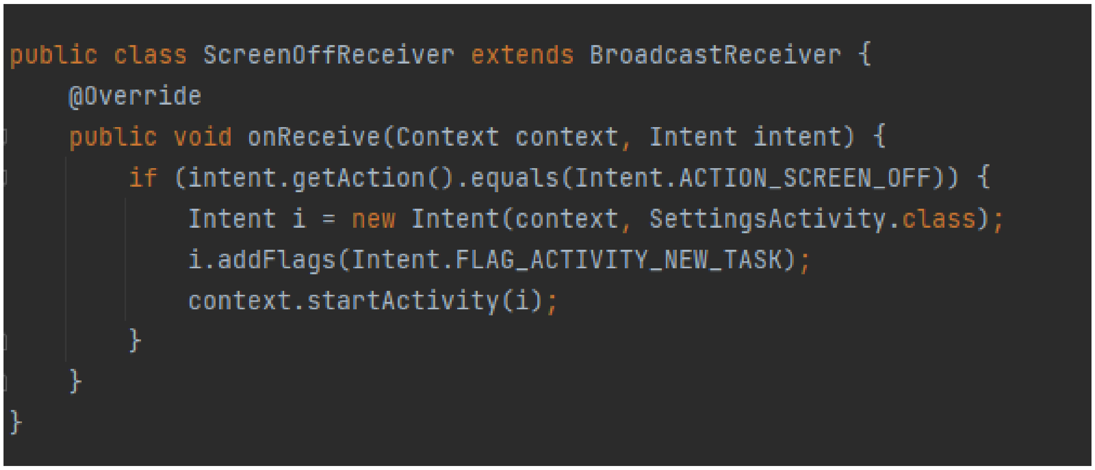
9. In the "onDestroy" method, the overlay view is removed from the WindowManager to clean up the resources when the service is destroyed.

10. The "onBind" method returns null, indicating that the service does not support binding.

Key Points:
- The code creates a custom power off screen overlay using a service in Android.
- The WindowManager is used to manage the display of the overlay view on top of other applications.
- The overlay view is added to the WindowManager with specified layout parameters.

Launching Settings Activity on Screen Off

5.5 Presenting overlay screen



```java
public class ScreenOffReceiver extends BroadcastReceiver {
    @Override
    public void onReceive(Context context, Intent intent) {
        if (intent.getAction().equals(Intent.ACTION_SCREEN_OFF)) {
            Intent i = new Intent(context, SettingsActivity.class);
            i.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
            context.startActivity(i);
        }
    }
}
```

Screenshot 5.5 Presenting overlay screen

1. Purpose: The code represents a BroadcastReceiver named "ScreenOffReceiver" that is responsible for handling the event when the device's screen is turned off.

2. Trigger Condition: The code checks if the received intent's action is equal to "Intent.ACTION_SCREEN_OFF", indicating that the screen has been turned off.

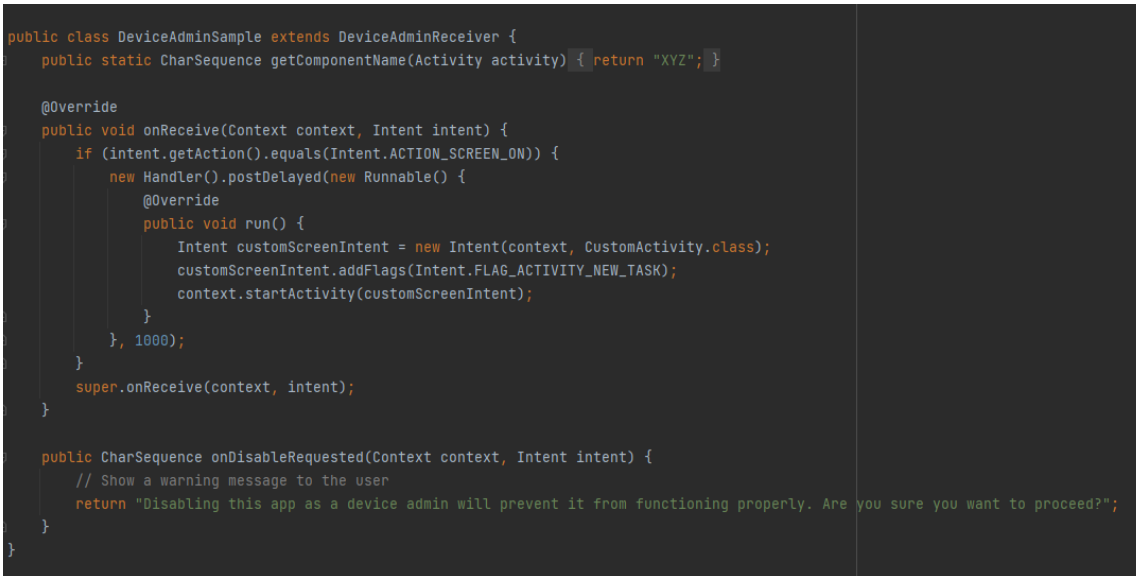
3. Launching Settings Activity: Once the screen-off event is detected, the code creates an instance of the Intent class, targeting the SettingsActivity class.

4. Intent Flags: The code adds the flag "Intent.FLAG_ACTIVITY_NEW_TASK" to the intent, ensuring that the SettingsActivity is started as a new task.

5. Starting Activity: Finally, the code starts the SettingsActivity by calling "context.startActivity(i)".

This code defines a BroadcastReceiver called "ScreenOffReceiver" that listens for the "ACTION_SCREEN_OFF" event, indicating when the device's screen is turned off. Once this event occurs, the code launches the SettingsActivity as a new task. This code can be useful for performing specific actions or launching certain activities when the screen goes off, allowing customization and control over the device's behavior in response to screen events.

5.6 Device Administration



```java
public class DeviceAdminSample extends DeviceAdminReceiver {
    public static CharSequence getComponentName(Activity activity) { return "XYZ"; }

    @Override
    public void onReceive(Context context, Intent intent) {
        if (intent.getAction().equals(Intent.ACTION_SCREEN_ON)) {
            new Handler().postDelayed(new Runnable() {
                @Override
                public void run() {
                    Intent customScreenIntent = new Intent(context, CustomActivity.class);
                    customScreenIntent.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
                    context.startActivity(customScreenIntent);
                }
            }, 1000);
        }
        super.onReceive(context, intent);
    }

    public CharSequence onDisableRequested(Context context, Intent intent) {
        // Show a warning message to the user
        return "Disabling this app as a device admin will prevent it from functioning properly. Are you sure you want to proceed?";
    }
}
```

Screenshot 5.6 Device Admistration

1. The given code represents a class named `DeviceAdminSample`, which extends the `DeviceAdminReceiver` class.

2. The code includes several methods and functionalities for device administration and handling specific events.

3. The `onReceive()` method is overridden from the `DeviceAdminReceiver` class and is triggered when a specific intent action, `Intent.ACTION_SCREEN_ON`, is received.

4. Inside the `onReceive()` method, a new Handler is created, which schedules a task to be executed after a delay of 1000 milliseconds (1 second).

5. The scheduled task involves creating an intent for a custom activity, `CustomActivity`, and starting that activity using the `context.startActivity()` method.

6. The `onDisableRequested()` method is another overridden method that is called when a request to disable the device admin functionality is received.

7. In this method, a warning message, provided as a CharSequence, is returned to alert the user about the consequences of disabling the app as a device admin.

8. The `DeviceAdminSample` code is responsible for managing device administration tasks and handling specific events related to device activity and admin functionality.

9. The `onReceive()` method is triggered when the screen is turned on and starts a custom activity after a short delay.

10. The `onDisableRequested()` method displays a warning message to the user when a request to disable the device admin functionality is received.

5.7 Architecture Diagram

When a thief steals a smartphone, their first action is often to turn it off, rendering traditional methods of recovery useless. However, this new system aims to prevent this by remaining active even after the smartphone has been turned off. This system uses a combination of GPS, cellular data, SMS, and wi-fi to track the location of the device. Even if the smartphone has been turned off by the thief, it will continue to transmit a signal, making it possible to recover the phone.

To further enhance its effectiveness, this system employs a sleep mode feature that ensures the phone remains trackable even after a failed attempt to turn it off. When someone attempts to switch off the smartphone, the device will instead enter a sleep mode that keeps it fully functional but appears to be switched off to the thief. This is achieved by deactivating the screen and other visible indicators, making the smartphone appear to be switched off while it is actually functioning normally.

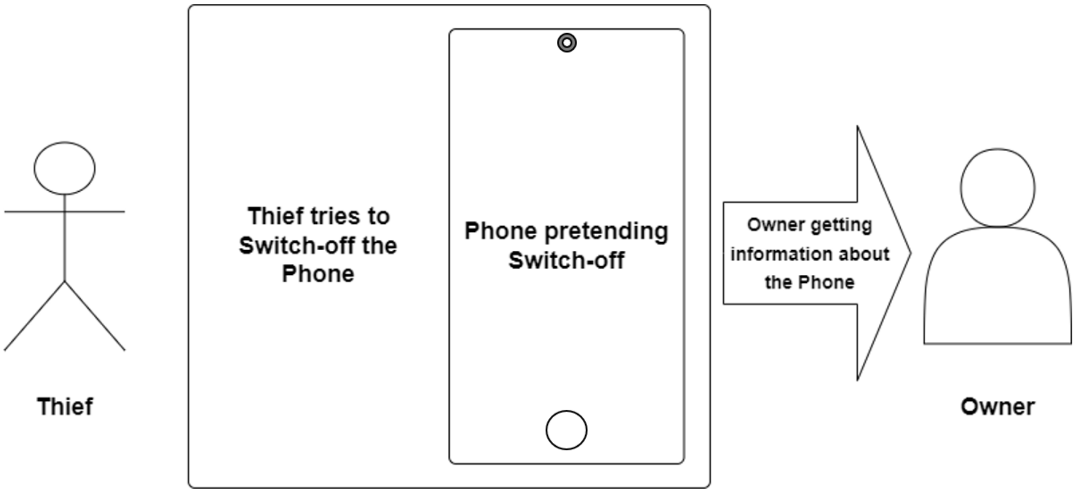

Thief
Thief tries to Switch-off the Phone
Phone pretending Switch-off
Owner getting information about the Phone
Owner

Fig.4.1 Architecture Diagram

5.8 Flow Chart

The flowchart is simply a symbol of the design of the steps. It shows the steps in their sequence and is widely used to present algorithm, tasks flow or processes.

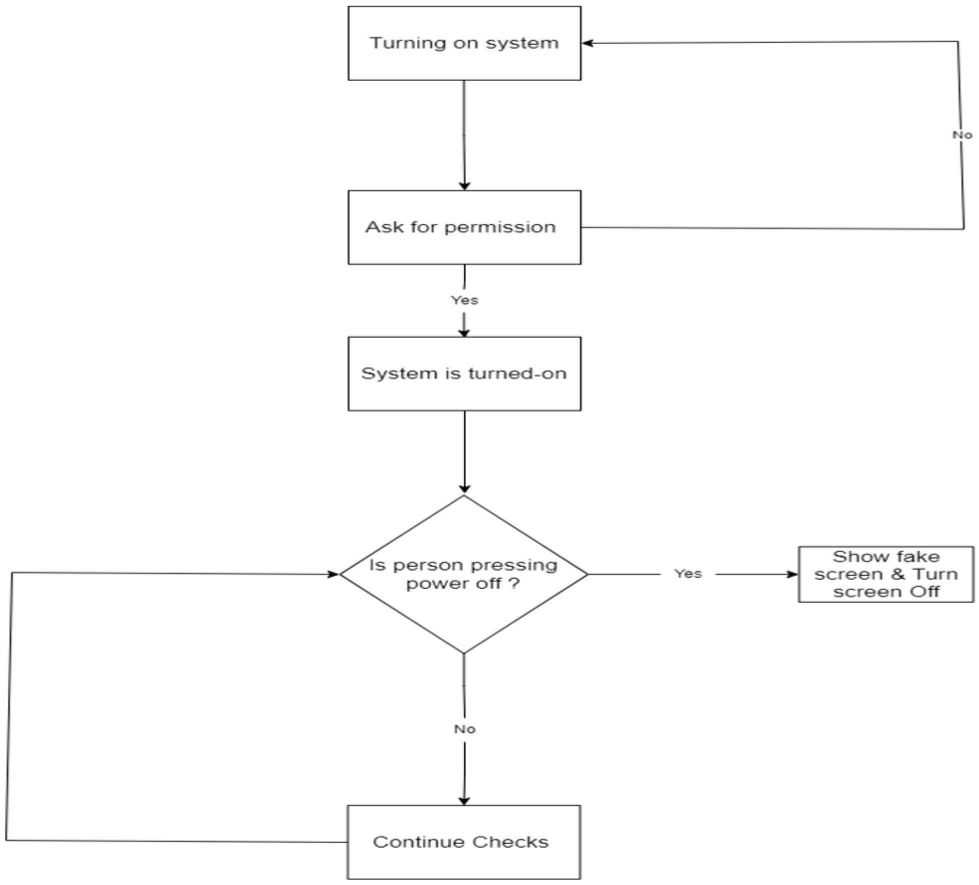


Fig.4.2 Flow Chart

Chapter 6

RESULT AND ANALYSIS

Result:

The objective of our project is to develop an improved approach for the recovery of lost smartphones, addressing the critical issue of low recovery rates and ensuring the security and privacy of these devices. Through our research and analysis, we have identified the shortcomings of existing systems such as Google Find My Device and CEIR (Central Equipment Identity Register). These systems face limitations when the device is switched off or lacks internet connectivity, making it challenging to track and locate the lost smartphone.

To overcome these limitations, we propose a comprehensive solution that incorporates advanced functionalities and techniques. Our system operates even when the smartphone is switched off, ensuring continuous tracking and recovery possibilities. We have designed the system to leverage GPS, cellular data, SMS, and Wi-Fi, enabling the smartphone to remain traceable even after an attempt to switch it off.

The technical background of our project involves the utilization of a device administration receiver. We have implemented a class called "DeviceAdminSample" that extends the "DeviceAdminReceiver" class. This class includes a method named "getComponentName" that returns a component name, serving as an identification mechanism within the application. Furthermore, we have overridden the "onReceive" method, which is triggered when the device's screen is turned on. Within this method, we initiate a delay and launch a custom screen activity using an intent.

Through our efforts, we aim to enhance user experience and provide a reliable solution for smartphone recovery. Our application deploys an enterprise security solution that fulfills both immediate and long-term requirements. It incorporates features such as sending location and message alerts via SMS and email, facilitating the identification of the thief and aiding law enforcement in apprehending them.

The developed system offers significant advantages over existing solutions. By considering loss mitigation and prioritizing security and privacy, our system addresses the shortcomings of current methods. We emphasize robustness, efficiency, and user-friendliness, and as such, the system will undergo thorough analysis and testing in real-world conditions.

In conclusion, our project focuses on the recovery of lost smartphones through an improved approach. We have presented a technical background that outlines the implementation details of our system, including the utilization of a device administration receiver and custom screen activation. Our system provides advanced functionalities and addresses the limitations of existing systems, ensuring continuous traceability and recovery possibilities, even when the smartphone is switched off. By deploying an enterprise security solution and prioritizing user requirements, our system enhances the overall user experience and aids in the identification and apprehension of thieves. We envision that our system will make a significant impact in the field of smartphone security and contribute to the growing need for effective lost smartphone recovery solutions.

Analysis

The discussion in the chat provided information on various aspects of a project related to the recovery of lost smartphones using an improved approach. Let's analyze the key points covered in the conversation.

The project aims to address the problem of lost smartphones, which is a significant concern in a country rapidly advancing towards digitization. The data obtained under the Right to Information (RTI) Act revealed that only a small percentage of lost phone cases are reported. Additionally, studies indicate that a large number of smartphones are lost each year, with a low percentage of recovery. This emphasizes the need for better security and privacy measures for lost smartphones.

The existing systems for tracking lost smartphones were discussed, including Google's Find My Device and the Central Equipment Identity Register (CEIR). While these systems provide some level of tracking and blocking functionalities, they have limitations. For example, once a device is switched off, its location cannot be accessed, and tracking using the IMEI number becomes ineffective. These limitations create opportunities for an improved approach to address the issue.

The proposed system focuses on developing a solution that can recover lost smartphones even after they are switched off. By leveraging technologies such as GPS, cellular data, SMS, and Wi-Fi, the system aims to make the phone traceable even when attempts are made to power it off. The system employs a methodology that involves setting up the environment, granting necessary permissions, and ensuring continuous tracking and monitoring of the device. It utilizes a specific algorithm that guides the recovery process step by step.

The technical background highlights the functioning of the system. It explains that the phone appears to be switched off but is actually running in the background, possibly performing tasks without the user's knowledge. When a thief attempts to switch off the smartphone, the system enters a pretend switch-off mode, making it appear inactive. However, the phone remains traceable, and the owner starts receiving information about the smartphone's location and activities. This feature enhances the chances of identifying the thief and recovering the lost device.

The conclusion emphasizes the project's goal of designing and developing a system that assists in recovering lost smartphones. It underscores the significance of data from the lost phone, such as its location, in achieving this objective. The application incorporates enterprise security measures and provides information about the location of the smartphone via SMS and email, aiding in the identification and apprehension of the thief. The conclusion also mentions the system's focus on loss mitigation, privacy protection, and robustness, efficiency, and user-friendliness, which will be verified through real-world testing.

In terms of future scope, the project opens avenues for further advancements. Possible areas for improvement include enhancing the tracking capabilities when the device is disconnected from the internet, refining the system's compatibility with different devices and operating systems, and exploring additional security measures. The future development may also involve incorporating machine learning or artificial intelligence techniques to enhance the accuracy of tracking and increase the chances of recovery.

Overall, the analysis of the chat conversation provides a comprehensive understanding of the project's objectives, the limitations of existing systems, the proposed approach, and the potential for future enhancements. It highlights the importance of addressing the issue of lost smartphones and the value of implementing an improved system that prioritizes security, privacy, and effective recovery mechanisms.

Chapter 7

CONCLUSION AND FUTURE SCOPE

Conclusion

In conclusion, the discussion and information shared throughout the chat provide valuable insights into the development of a system aimed at recovering lost smartphones and mitigating the risks associated with theft. The proposed system addresses the limitations of existing solutions by incorporating features such as tracking the smartphone even when it is switched off, utilizing GPS, cellular data, SMS, and Wi-Fi functionalities. Additionally, the system enhances security by deploying an enterprise solution that sends message and location details via SMS and email, aiding in the identification and capture of thieves. The technical background highlights the functioning of the system, including the simulation of power-off states and the role of the DeviceAdminReceiver class. Overall, the approach shows promise in ensuring the privacy and security of smartphones while providing a means for their recovery.

Future Scope

1. Further Enhancements in Tracking Technology: The project can explore advanced tracking technologies such as GPS, geofencing, and real-time location updates to improve the accuracy and efficiency of smartphone recovery.

2. Integration with Law Enforcement Authorities: Collaborating with law enforcement agencies to establish a direct channel for reporting and tracking stolen smartphones can expedite the recovery process and increase the chances of catching thieves.

3. Integration with Third-Party Security Services: Partnering with security service providers can enhance the security features of the application, allowing for remote data

wiping, device locking, and advanced anti-theft measures to safeguard user data and deter theft.

4. Cross-Platform Compatibility: Expanding the project's compatibility to include other operating systems, such as iOS, will increase its reach and effectiveness in recovering lost or stolen smartphones across various platforms.

5. Collaboration with Mobile Network Operators: Establishing partnerships with mobile network operators can facilitate access to IMEI databases and strengthen the ability to track and disable stolen smartphones across different networks.

REFERENCES

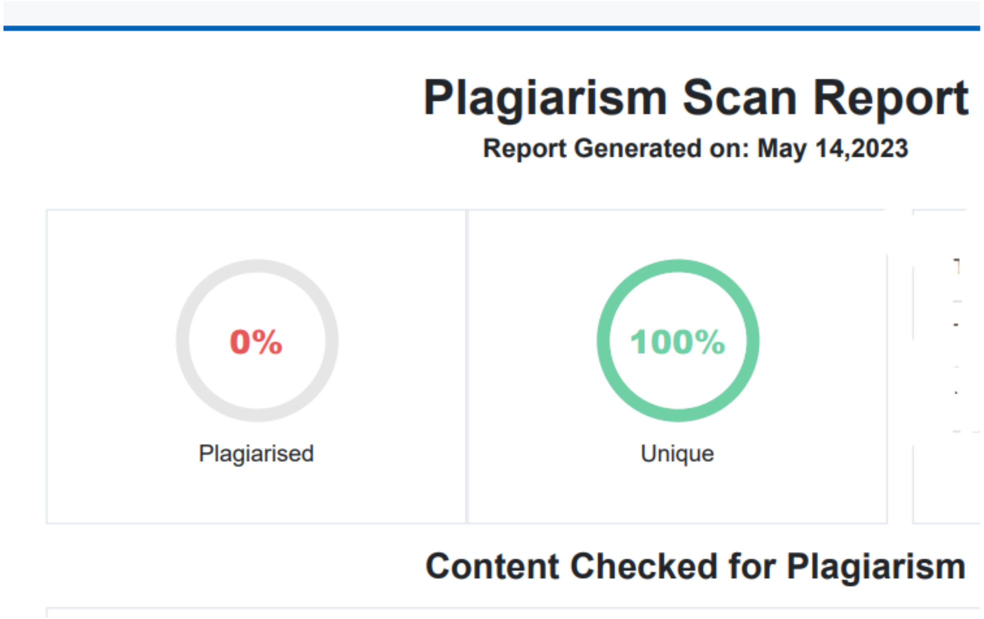
[1] Khan, A. U. S., Qureshi, M. N., & Qadeer, M. A. (2014). Anti-theft application for android based devices. 2014 IEEE International Advance Computing Conference (IACC). doi:10.1109/iadcc.2014.677935.

[2] Lei, L., Wang, Y., Zhou, J., Wang, L., & Zhang, Z. (2013). A Threat to Mobile Cyber-Physical Systems: Sensor-Based Privacy Theft Attacks on Android Smartphones. 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. doi:10.1109/trustcom.2013.20.

[3] Ong, Chen & Kasim, Nelly & Jayasena, Sajindra & Rudolph, Larry & Cham, Tat Jen. (2004). Proactive Detection and Recovery of Lost Mobile Phones.

[4] Arikpo, Iwara I., and Gabriel I. Osuobiem. "A SOFTWARE TOOL FOR RECOVERING LOST MOBILE PHONES USING REAL-TIME TRACKING." International Journal of Advanced Research in Computer Science 11.3 (2020).

PLAGIARISM REPORT



Plagiarism Scan Report

Report Generated on: May 14,2023

0%

Plagiarised

100%

Unique

Content Checked for Plagiarism

PUBLICATION DETAILS

[1] Dr. A. N. Thakare, Mr. Palash Wasu, Mr. Chinmay Meghare, Mr. Anup Chahande, Ms. Aishwarya Pise, Ms. Neha Gothe, **“Recovery of Lost Smartphone using Improved apporach”** at National Conference on Innovation in Science Engineering and Management (NCISEM-2023), Date: - 5th April 2023

[2] Dr. A. N. Thakare, Mr. Palash Wasu, Mr. Chinmay Meghare, Mr. Anup Chahande, Ms. Aishwarya Pise, Ms. Neha Gothe, **“Shoulder Surfing Resistant Authentication Using Enhanced Color-based Interface”** at International Journal of Applied Computing, Date: 5th April 2023 (Accepted for Journal publication).

PATENTS SEARCH RESULT

[1] Remote health monitoring system

Inventor: Michael Fahey

Application Number: US8478418B2

Publication Date: 02-07-2013

Assignee: INFOBIONIC Inc

Redwood shores: US

[2] Smart mobile health monitoring system and related methods

Inventor: Franz Baudenbacher, Susan Eagle, Rene Harder

Application Number: WO2014116968A1

Publication Date: 31-07-2014

Assignee: Vanderbilt University

Redwood shores: US

LIST OF PAPER PUBLISHED

Loss Mitigation and Recovery by Pretending Smartphone Switch-off

Palash Wasu
UG Student
Computer Department
B.D.C.E., Sewagram,
Wardha, Maharashtra
palashwasuak@gmail.com

Chinmay Meghare
UG Student
Computer Department
B.D.C.E., Sewagram,
Wardha, Maharashtra
chinmaym100@gmail.com

Anup Chahande
UG Student
Computer Department
B.D.C.E., Sewagram,
Wardha, Maharashtra
anupchahande2814@gmail.com

Dr. A. N. Thakare
Assistant Professor
Computer Department
B.D.C.E., Sewagram,
Wardha, Maharashtra
thak80@gmail.com

ABSTRACT

As the Country is advancing rapidly towards digitalization not owning a smartphone is thinkable. According to data obtained under Right To Information (RTI) act only 3.5 % of lost phone cases were registered. Kensington study says that 70 million smartphones are lost each year, with only 7 percent recovered. This makes the need for security and privacy of lost smartphones paramount. We are going to solve this serious issue using an improved approach.

General Terms

Tracking, Tracing, Lost Mitigation, IMEI (International Mobile Equipment Identity).

Keywords

Android, Location, Tracing, Tracking, Switch-off, Lost smartphone, Missing smartphone,

1. INTRODUCTION

Nowadays not possessing a smartphone in this country, which is moving quickly towards digitization, is unimaginable. Only 3.5% of lost phone cases, as per information obtained under the Right to Information (RTI) Act, were reported. According to research by Kensington, only 7% of misplaced smartphones are ever found. Due to this, the security and privacy of lost devices are essential. We're going to use a better strategy to resolve this important problem.

2. SCOPE

As the Country is advancing rapidly towards digitalization not owning a smartphone is unthinkable. According to data obtained Right to Information (RTI) act only 3.5 % of lost phone cases were registered. Kensington's study says that 70 million smartphones are lost each year, with only 7 percent recovered. This makes the need for security and privacy of lost smartphones paramount. We are going to solve this serious issue using an improved approach.

3. EXISTING SYSTEMS

3.1 Google Find My Device

Find, lock, or erase a lost Android device If you lose an Android phone or tablet, or Wear OS watch, you can find, lock, or erase it. If you've added a Google Account to your device.

Find My Device is automatically turned on. To find, lock, or erase an Android phone, that phone must:

- Be turned on
- Be signed in to a Google Account
- Be connected to mobile data or Wi-Fi
- Be visible on Google Play
- Have the Location turned on
- Have to Find My Device turned on

If you used your lost phone for 2-step verification, you must have a backup phone or backup code. Remotely find, lock, or erase

1. Go to android.com/find and sign in to your Google Account.

- If you have more than one phone, click the lost phone at the top of the screen.
- If your lost phone has more than one user profile, sign in with a Google Account that's on the main profile. Learn about user profiles.

2. The lost phone gets a notification.

3. On the map, you'll get info about where the phone is.

- The location is approximate and might not be accurate.
- If your phone can't be found, you'll see its last known location, if available.

4. Pick what you want to do. If needed, first click Enable lock & erase.

- Play sound: Rings your phone at full volume for 5 minutes, even if it's set to silent or vibrate.
- Secure device: Locks your phone with your PIN, pattern, or password.

If you don't have a lock, you can set one.

To help someone return your phone to you, you can add a message or phone number to the lock screen.

- Erase device: Permanently deletes all data on your phone (but might not delete SD cards).

After you erase it, Find My Device won't work on the phone.

Disadvantage:- The main drawback of this system is that once the device is switched-off it can no longer access location, internet, camera, and other systems, and application.

4.1 CEIR (Central Equipment Identity Register)

CEIR (Government Initiative) CEIR (Central Equipment Identity Register) With the aim to counterfeit mobile phone market and discourage mobile phone theft, protect consumer interest, and facilitate, law enforcement authorities for lawful interception, DoT intends to implement Central Equipment Identity Registry (CEIR) that connects to the IMEI database of all the mobile Operators. CEIR acts as a central system for all network Operators to share blacklisted so that devices blacklisted in one network will not work on other networks even if the Subscriber Identity Module (SIM) card in the device is changed.

Disadvantage:- Again the main drawback of this system is that once the device is switched-off it can no longer track the device using the IMEI number

5. LIMITATIONS

1. IMEIs can sometimes be removed from a blocklist, depending on local arrangements. This would typically include quoting a password chosen at the time of block listing.
2. IMEI tracking is expensive and cannot be done without legal interference

3. Tracking is not possible in case of internet disconnection and if the tracking services are not setup (e.g. Google Find my device

4. Once the device get switch-off no existing system can work.

6. PROPOSED SYSTEM

The purpose of this system is to recover the lost smartphone. This system will work even after switching off the smartphone. The smartphone will be traceable even after if its switch off. So it is possible to recover the smartphone if the thief switch it off. The existing system can not work after switching off the smartphone. After turning on the system GPS, Cellular data, SMS and wi-fi start working for the purposed system. If the system turn on and someone trying switch off the smartphone then the smartphone will go to sleep. And this makes the phone traceable even after attempt switch off

6.1 Methodology

The main aim of the system is to find the missing smartphone. Even after turning off the smartphone, this mechanism will continue to function. It is possible to recover the smartphone if the thief switches it off because it will still be traceable after that. After turning off the smartphone, the current system is inoperable. When the system is turned on, GPS, cellular data, SMS, and wi-fi begin to function for the intended system. The smartphone will go to sleep if the system is turned on and someone tries to turn it off. This makes the phone trackable even after the switch-off attempt.

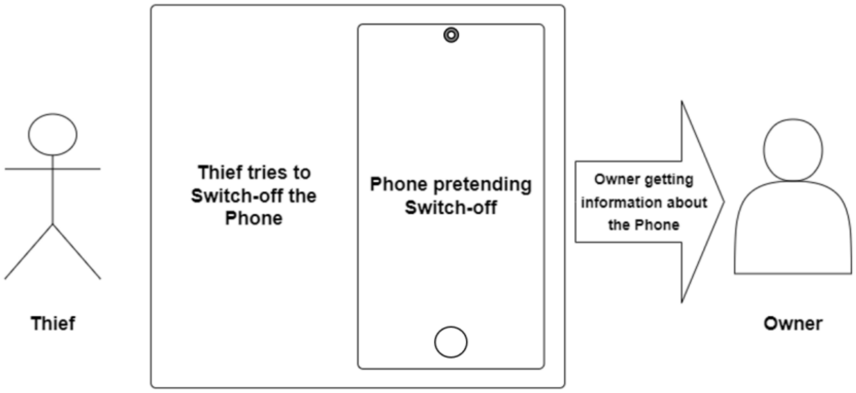

Thief
Thief tries to Switch-off the Phone
Phone pretending Switch-off
Owner getting information about the Phone
Owner

Fig 1 : Block diagram of the system

6.2 Algorithm

Recovery of lost smartphone algorithm

Step 1. Setup environment.

Step 2. Setup dependencies and check for compatibility on the device.

Step 3. Accept permissions for wi-fi, cellular data, send and view SMS and GPS.

Step 4. On clicking the complete access button.

Step 5. If the specified permissions are granted the services will start working.

Step 6. Else the system will request for granting the mandatory permissions.

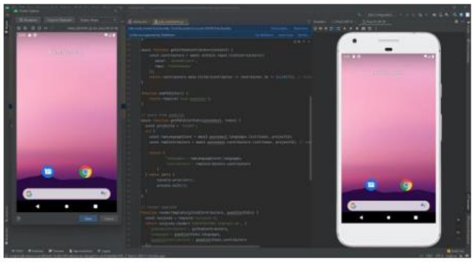
Step 7. Once granting the permissions and activating the access button the system is trackable.

Step 8. Now the system will continue to check whether someone tries to switch it off or not.

Step 9. If the thief tries to shut down the system a SMS will be sent to the alternat mobile number and the system will switch to Pretend mode.

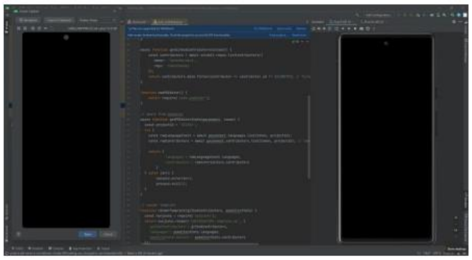
Step 10. Else continue with the system on and continuous checking for attempting switch-off.

6.3 Result



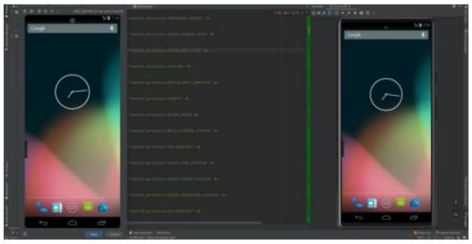
Screenshot 1 : Phone functioning normally

The phone in Fig 2 is functioning normally and the system is turned on. This means that the phone shown in the image is in working condition and the system software and application have started, indicating that it is ready to be used.



Screenshot 2 : Pretending the phone is switch-off

The phone in Fig 3 is apparently turned off, but it is actually operating normally in the background. This means that although the phone appears to be switch-off, it is still functioning and performing tasks, possibly without the user's knowledge or consent.



Screenshot 3 : Phone resumes to normal mode

The phone in Fig 4 returns to its regular operating mode after simulating a power-off state. This means that the phone shown in the image was made to appear as though it had been turned off, but was actually still running in the background. Later, it was brought back to its normal operating mode. This may be an intentional feature of the phone, such as a sleep mode

6.4 Conclusion

We are striving to design and develop a system that will help the owner recover the lost smartphone by using the data from the lost phone (location, etc). The application deploys an enterprise security solution that meets users immediate and long term requirements by providing the message and location via SMS and email, which makes easy for the user to identify the thief and make him/her get caught and arrested. It enhances the application by providing the information about the location the android based smart phone with the help of text smartphone system will be developed by considering loss mitigation and prevention of loss of security and privacy. The system will be thoroughly analyzed and tested in real-world conditions for robustness, efficiency, and user-friendliness.

7. ACKNOWLEDGEMENT

We would like to express our sincere appreciation to Dr. A. N. Thakare, our guide, for his continuous inspiration and invaluable guidance during our work. His unwavering commitment, astute leadership, and insightful recommendations allowed us to effectively coordinate our efforts and address the diverse aspects of the project, which was crucial to its successful completion.

8. REFERENCES

[1] Khan, A. U. S., Qureshi, M. N., & Qadeer, M. A. (2014). Anti-theft application for android based devices. 2014 IEEE International Advance Computing Conference (IACC). doi:10.1109/iadcc.2014.677935.

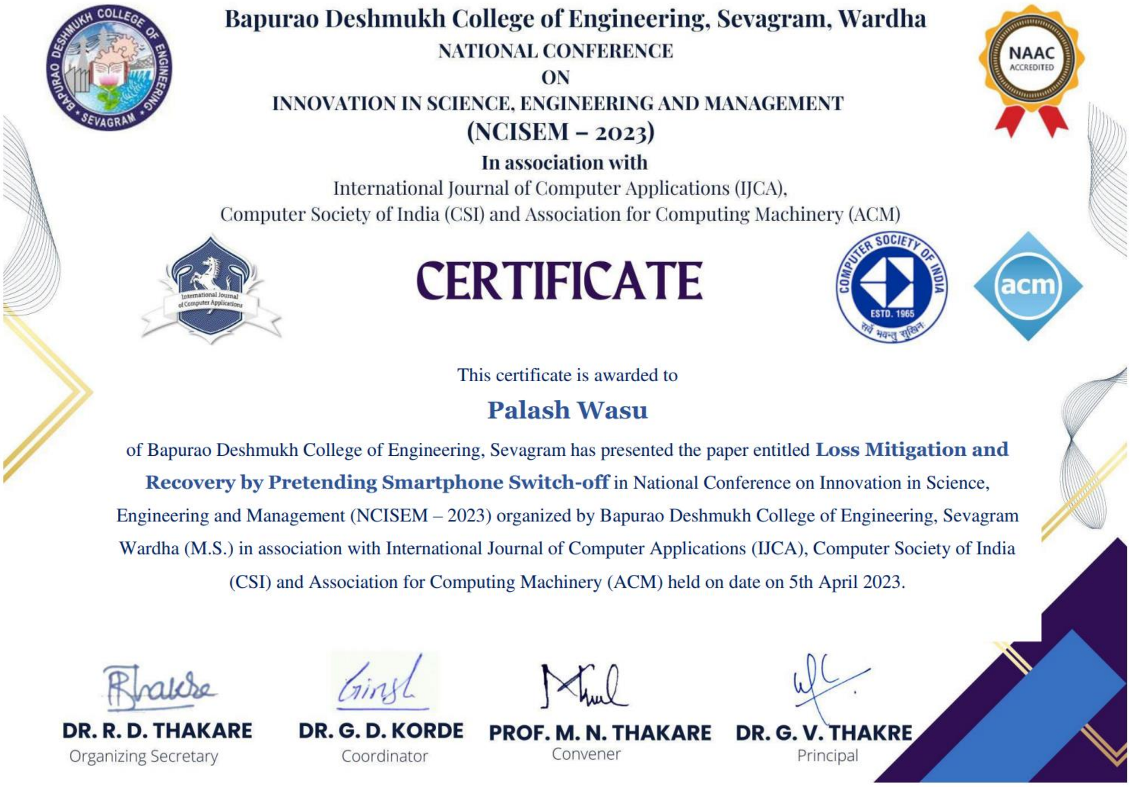
[2] Lei, L., Wang, Y., Zhou, J., Wang, L., & Zhang, Z. (2013). A Threat to Mobile Cyber-Physical Systems: Sensor-Based Privacy Theft Attacks on Android Smartphones. 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. doi:10.1109/trustcom.2013.20.

[3] Ong, Chen & Kasim, Nelly & Jayasena, Sajindra & Rudolph, Larry & Cham, Tat Jen. (2004). Proactive Detection and Recovery of Lost Mobile Phones.

[4] Arikpo, Iwara I., and Gabriel I. Osuobiem. "A SOFTWARE TOOL FOR RECOVERING LOST MOBILE PHONES USING REAL-TIME TRACKING." *International Journal of Advanced Research in Computer Science* 11.3 (2020).

CERTIFICATES

National Conference on Innovation in Science Engineering and Management (NCISEM) on 5th April 2023, Organized by Bapurao Deshmukh College of Engineering, Sewagram, Wardha (Maharashtra).



Bapurao Deshmukh College of Engineering, Sevagram, Wardha

NATIONAL CONFERENCE

ON

INNOVATION IN SCIENCE, ENGINEERING AND MANAGEMENT

(NCISEM – 2023)

In association with

International Journal of Computer Applications (IJCA),

Computer Society of India (CSI) and Association for Computing Machinery (ACM)

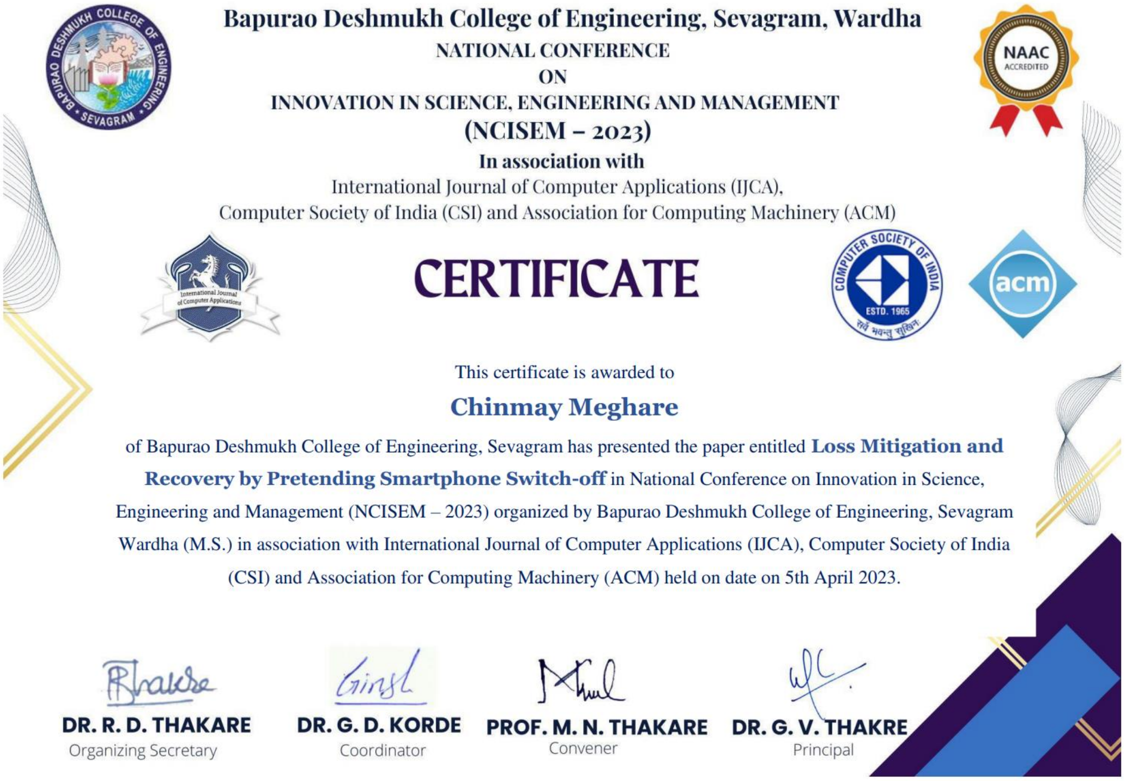
CERTIFICATE

This certificate is awarded to

Palash Wasu

of Bapurao Deshmukh College of Engineering, Sevagram has presented the paper entitled **Loss Mitigation and Recovery by Pretending Smartphone Switch-off** in National Conference on Innovation in Science, Engineering and Management (NCISEM – 2023) organized by Bapurao Deshmukh College of Engineering, Sevagram Wardha (M.S.) in association with International Journal of Computer Applications (IJCA), Computer Society of India (CSI) and Association for Computing Machinery (ACM) held on date on 5th April 2023.

DR. R. D. THAKARE Organizing Secretary	DR. G. D. KORDE Coordinator	PROF. M. N. THAKARE Convener	DR. G. V. THAKRE Principal



Bapurao Deshmukh College of Engineering, Sevagram, Wardha

NATIONAL CONFERENCE

ON

INNOVATION IN SCIENCE, ENGINEERING AND MANAGEMENT

(NCISEM – 2023)

In association with

International Journal of Computer Applications (IJCA),
Computer Society of India (CSI) and Association for Computing Machinery (ACM)

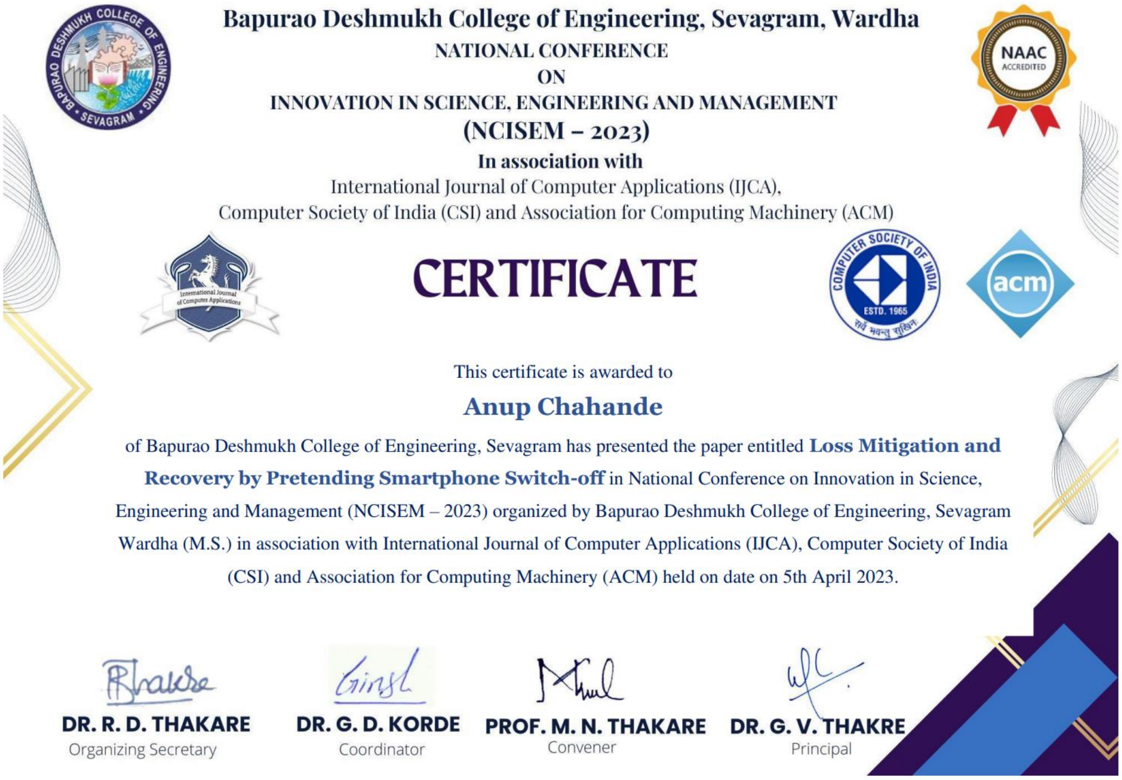
CERTIFICATE

This certificate is awarded to

Chinmay Meghare

of Bapurao Deshmukh College of Engineering, Sevagram has presented the paper entitled **Loss Mitigation and Recovery by Pretending Smartphone Switch-off** in National Conference on Innovation in Science, Engineering and Management (NCISEM – 2023) organized by Bapurao Deshmukh College of Engineering, Sevagram Wardha (M.S.) in association with International Journal of Computer Applications (IJCA), Computer Society of India (CSI) and Association for Computing Machinery (ACM) held on date on 5th April 2023.

DR. R. D. THAKARE Organizing Secretary	**DR. G. D. KORDE** Coordinator	**PROF. M. N. THAKARE** Convener	**DR. G. V. THAKRE** Principal



Bapurao Deshmukh College of Engineering, Sevagram, Wardha

NATIONAL CONFERENCE

ON

INNOVATION IN SCIENCE, ENGINEERING AND MANAGEMENT

(NCISEM – 2023)

In association with

International Journal of Computer Applications (IJCA),

Computer Society of India (CSI) and Association for Computing Machinery (ACM)

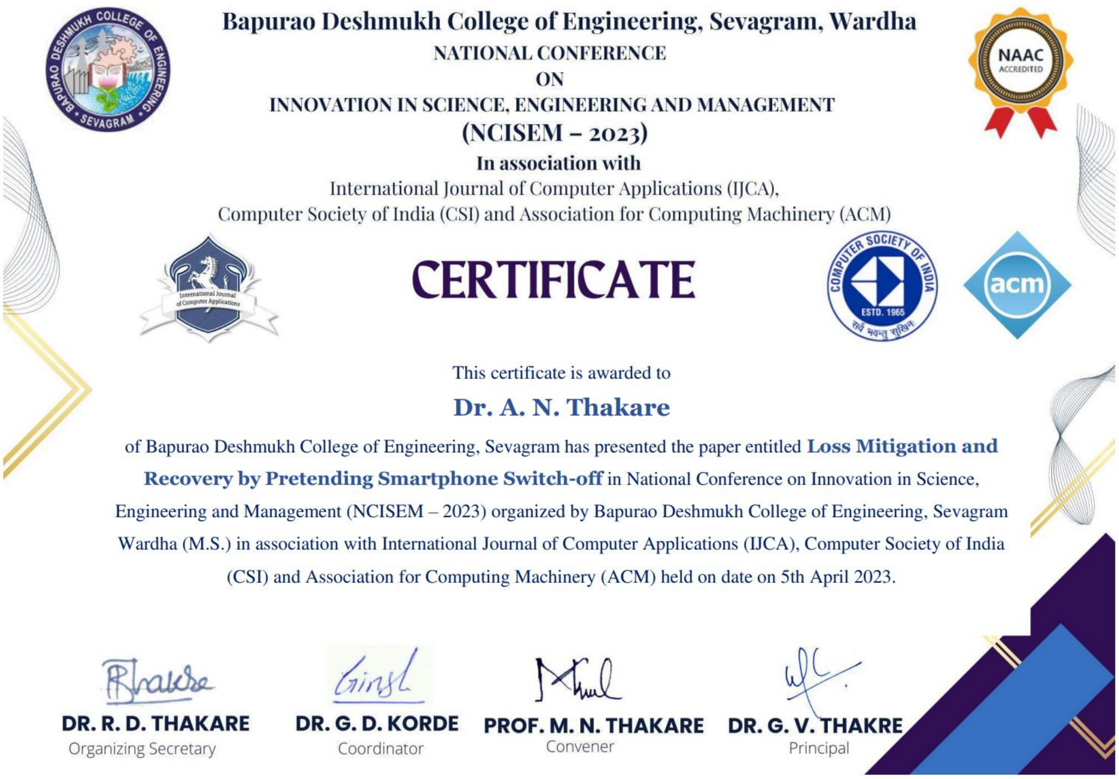
CERTIFICATE

This certificate is awarded to

Anup Chahande

of Bapurao Deshmukh College of Engineering, Sevagram has presented the paper entitled **Loss Mitigation and Recovery by Pretending Smartphone Switch-off** in National Conference on Innovation in Science, Engineering and Management (NCISEM – 2023) organized by Bapurao Deshmukh College of Engineering, Sevagram Wardha (M.S.) in association with International Journal of Computer Applications (IJCA), Computer Society of India (CSI) and Association for Computing Machinery (ACM) held on date on 5th April 2023.

DR. R. D. THAKARE Organizing Secretary	**DR. G. D. KORDE** Coordinator	**PROF. M. N. THAKARE** Convener	**DR. G. V. THAKRE** Principal



Bapurao Deshmukh College of Engineering, Sevagram, Wardha

NATIONAL CONFERENCE

ON

INNOVATION IN SCIENCE, ENGINEERING AND MANAGEMENT

(NCISEM – 2023)

In association with

International Journal of Computer Applications (IJCA),
Computer Society of India (CSI) and Association for Computing Machinery (ACM)

CERTIFICATE

This certificate is awarded to

Dr. A. N. Thakare

of Bapurao Deshmukh College of Engineering, Sevagram has presented the paper entitled **Loss Mitigation and Recovery by Pretending Smartphone Switch-off** in National Conference on Innovation in Science, Engineering and Management (NCISEM – 2023) organized by Bapurao Deshmukh College of Engineering, Sevagram Wardha (M.S.) in association with International Journal of Computer Applications (IJCA), Computer Society of India (CSI) and Association for Computing Machinery (ACM) held on date on 5th April 2023.

DR. R. D. THAKARE Organizing Secretary	**DR. G. D. KORDE** Coordinator	**PROF. M. N. THAKARE** Convener	**DR. G. V. THAKRE** Principal

Project Group Photo

PO Attainment of Mega Project

PO Attained by the Mega Project have to tick by the Group.

PO	Program Outcomes	Tick the PO Attained in Mega Project
PO1	An ability to apply knowledge of mathematical foundations and computer science theory.	
PO2	An ability to identify, analyze, formulate, and to solve the complex problems using computer engineering principles.	
PO3	An ability to design, develop and evaluate software as well as hardware solutions.	
PO4	An ability to conduct experiments with analysis and interpretation of data.	
PO5	An ability to use modern software and. hardware tools necessary for computer engineering practices.	
PO6	An understanding of social and legal issues with responsibility in professional engineering practices.	
PO7	An ability to understand the impact of computing and engineering solutions in a global, economic, environmental, and societal context.	
PO8	An understanding of professional ethics and responsibilities.	
PO9	An ability to work in multidisciplinary teams with cooperation, respect, creativity, and responsibility as a member or leader of a team.	
PO10	An ability to communicate effectively with engineering community and society at large.	
PO11	An understanding of engineering principles to demonstrate technical skills for project and finance management.	
PO12	An ability to recognize the need of lifelong learning and to sustain with rapidly changing technologies.	

Review and Critique Sheet

Sr. No.	Name of Reviewer & Date	Designation	Email ID & Mobile No.	Remark	
1				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
2				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
3				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
4				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
5				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
6				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	

				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
7				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
8				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
9				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	
10				Innovative Idea/Concept/Content	
				Novel Area with relevent rusult	
				Generalised matter/ concept need improvement	
				Outcome to be reviewed/analyzed/validated	
				Work to be reviewed from commercial point of view	