**SOLUTION TO IDENTIFY SPOOFED CALLS RECEIVED BY GENERAL PUBLIC**

**Presented at the Smart India Hackathon-2022**

**PROBLEM DESCRIPTION:**

Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. This can lead to a caller ID display showing a phone number different from that of the telephone from which the call was placed. Some websites and mobile applications are available, which provides call spoofing service. In India, generally such calls are coming through International gateway with the CLI of the intended person (spoofed CLI) to recipient. Generally, such calls are made by fraudster with the intention of cheating called party (recipient). Calling party gets the CLI as mentioned by fraudster on his mobile device. If that CLI is stored in recipient mobile then the name will also be displayed. General public gets cheated with such call spoofing. We need solution such that whenever general public receives spoofed call from international route he shall be notified that the CLI is spoofed and the person whose CLI is displayed on recipient mobile device is not the person calling him. We need to consider following while formulating solutions: 1) Such calls are coming through international gateway and some solution needs to be implemented at those gateways. 2) There are some genuine numbers are also coming through international gateway and CLI of those number shall not be disturbed. 3) If a Person having Indian Mobile number, roaming outside India, makes a call to India, CLI will be exactly like India Numbering series. Such CLI shall also not be disturbed."

**INTRODUCTION:**

There are many people who are affected by identity theft, and with the advent of technology, this is quickly becoming a major concern for users. Caller ID spoofing is a form of identity theft in which the caller ID, the number displayed on a phone through an incoming number, has been modified by a spoofer to appear as if the call is trustworthy. With the arrival of new types of technology like *Asterisk* or *FreeSWITCH*, it is easy for anyone to create a fake call to masquerade as a trustworthy caller, for example, from a bank, the government, and entice the

user to give away personal information, resulting in identity theft.

This means that spoofers can masquerade as trustworthy banks, friends, or family members, and they can steal private information from the intended recipient. Spoofers have many methods of doing this, especially under the claim of a critical situation.

Some scenarios are:

1 .Spoofers can convince the user that he or she is under a critical and urgent situation in an attempt coax private

information from them.

Unfortunately, little research has been conducted on this topic thus far. Although some mobile

applications, such as Trapcall, help prevent scammed calls, they cannot prevent spoofed calls because the calls themselves appear to be trustworthy.

1. Another difficulty is that spoofed calls usually cannot be traced.
2. The initial solution involved blocking and redialing every single call

that may pose a potential threat to identity theft; however, this ruthless attempt to block spoofed calls can be annoying to users. Although it may protect users from spoofed calls, it is not the most efficient or user-friendly solution.

**VULNERABLE AND RISK:**

Spoofing cell phone numbers may not seem like a serious threat.But by altering caller ID information,Scammers can pretend to be from reputable organizations,manipulate people into divulging sensitive personal data,and defraud them out of lots of money.

Deceptive spam calls purport to be from the IRS(Internal Revenue Service)and try to intimidate people into making bogus back-payments for taxes.Another common grift is the tech-support scam,where the spoof caller claims to represent a well-known company with malware,such as ransomware or steal your credit card details.

POPULAR METHODS OF CALLER ID SPOOFING:

1.SPOOF CARD:

One of the popular methods of caller ID spoofing is by the use of SPOOF CARD.It is the world’s first real time voice changer.With the use of spoof card,it is possible to customize the voice like a men or women and even add background sounds.

1. ASTERISK:

**Asterisk allows for easy configuration of the outbound caller ID**. All that needs to be configured to start spoofing outgoing calls is to configure the outbound caller ID field. This field doesn't have any verification to determine whether or not the system is authorized to use the provided number for the caller ID.The pre-requisites for this are: VoIP service from companies like NuFone or VoicePulse which allow you to use your own PBX and basic LINUX knowledge.

Identifying spoofed calls based on VLR

VLR(Visitor Location Register)

ABSTRACT:

VLR is a server in a cellular network that supports roaming functions for users outside the coverage area of their own HLR(Home Location Register)

Spoofing uses social engineering based on people’s trust in telephone services to trick people into divulging financial data or transferring it to a spoofer.In the proposed system the VLR of the telephone services are stored in the data base and is available in the MSS.When a call is made ,it is compared with the available information in the database.If the number is available it is not a spoof else spoof is detected.

Background of Caller ID Spoofing

Caller ID spoofing is a technique that modifies the displayed number of an incoming call. This is crucial in vishing attacks since most people rely on the displayed number to authenticate the caller.

PROPOSED WORK:

STATIC DATA:

Consider a small database that consists of numbers from different service providers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AIRTEL | 8056170767 | 9840265574 | 8056197641 | 9566061192 |
| JIO | 6382159738 | 7904085835 | 9384716883 | 9092187464 |
| BSNL | 9443666583 | 9442476883 | 9445792265 | 9445229321 |
| VI | 8939481729 | 8190046163 | 8966061192 | 8966061191 |

The proposed solution based onthe location of thephone numbers of different service providers determines whether it’s international roaming or state roaming.

If the MSC database and the service provider database have the same number then the call is not spoofed else the call is spoofed.

CODE:

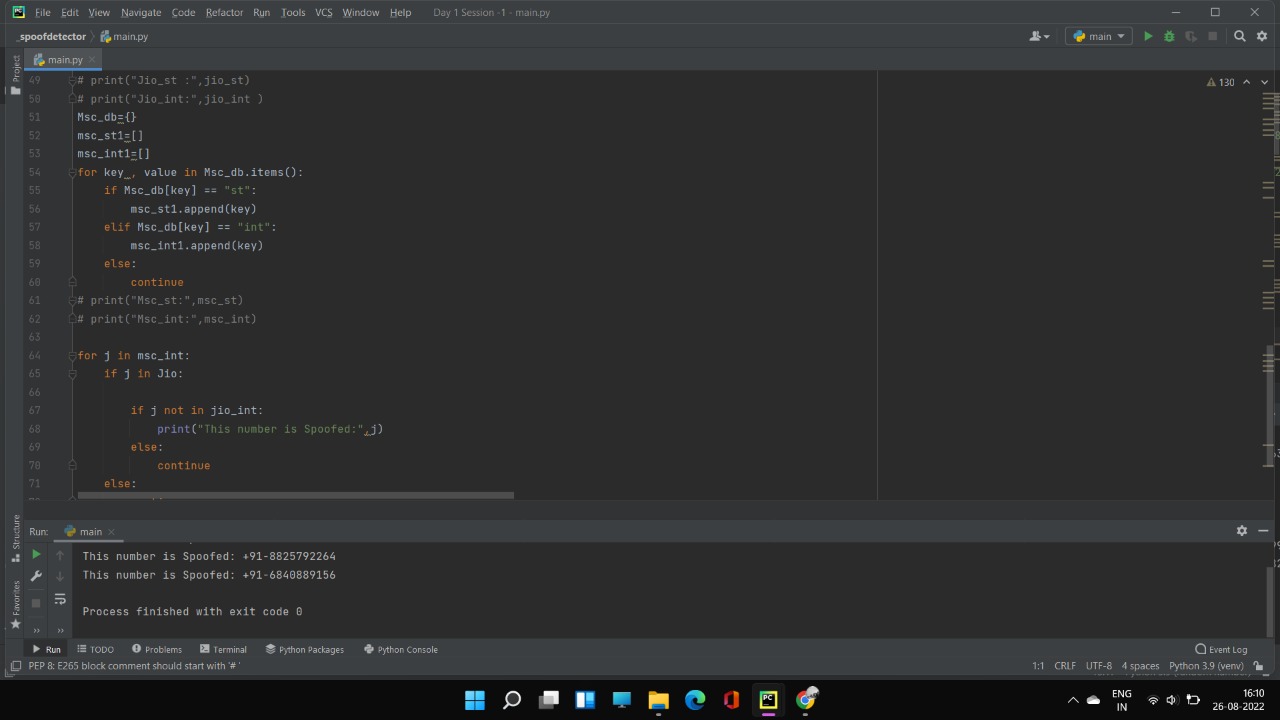
#st-State Roaming

#int - International Roaming

#Msc-Mobile Switching centre

#Database of Bsnl and VI are considered to be its VLR(Visitor location Register)

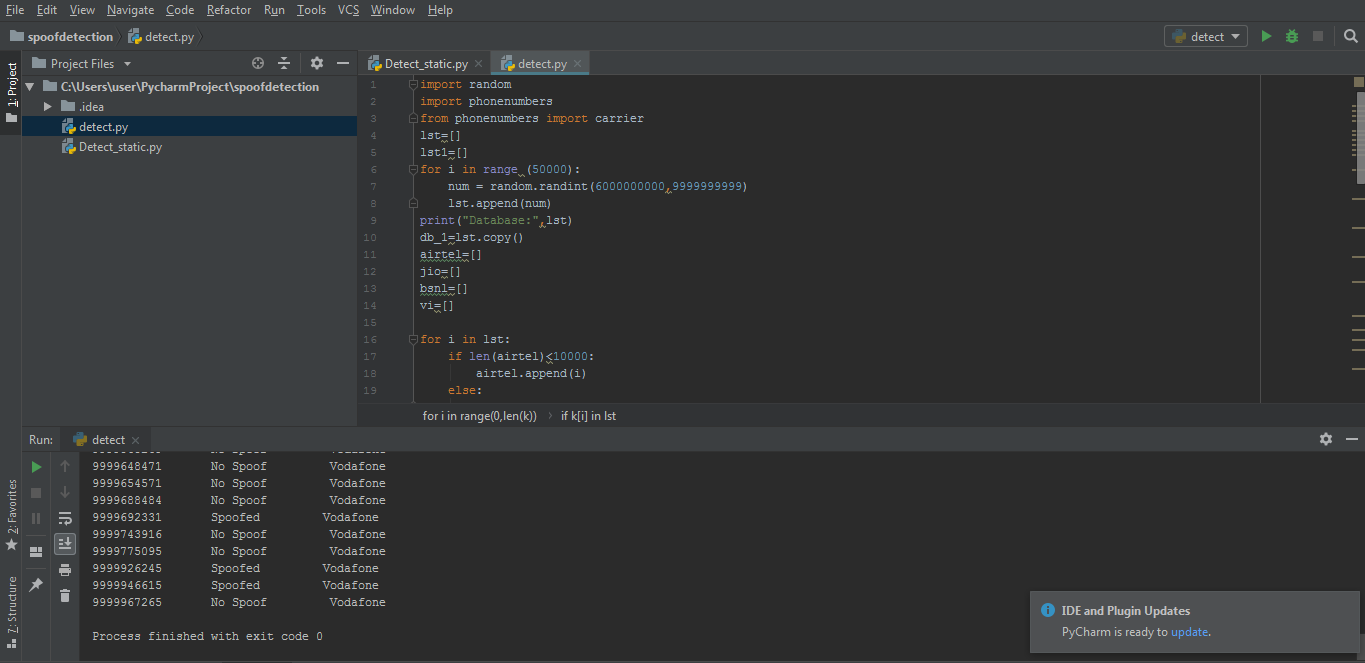
OUTPUT:



RANDOMIZED DATA:

In this code,we are generating random numbers from series 6000000000 to 9999999999 and identifying whether the number passing through the International Gateway is a spoofed call or not.

OUTPUT:



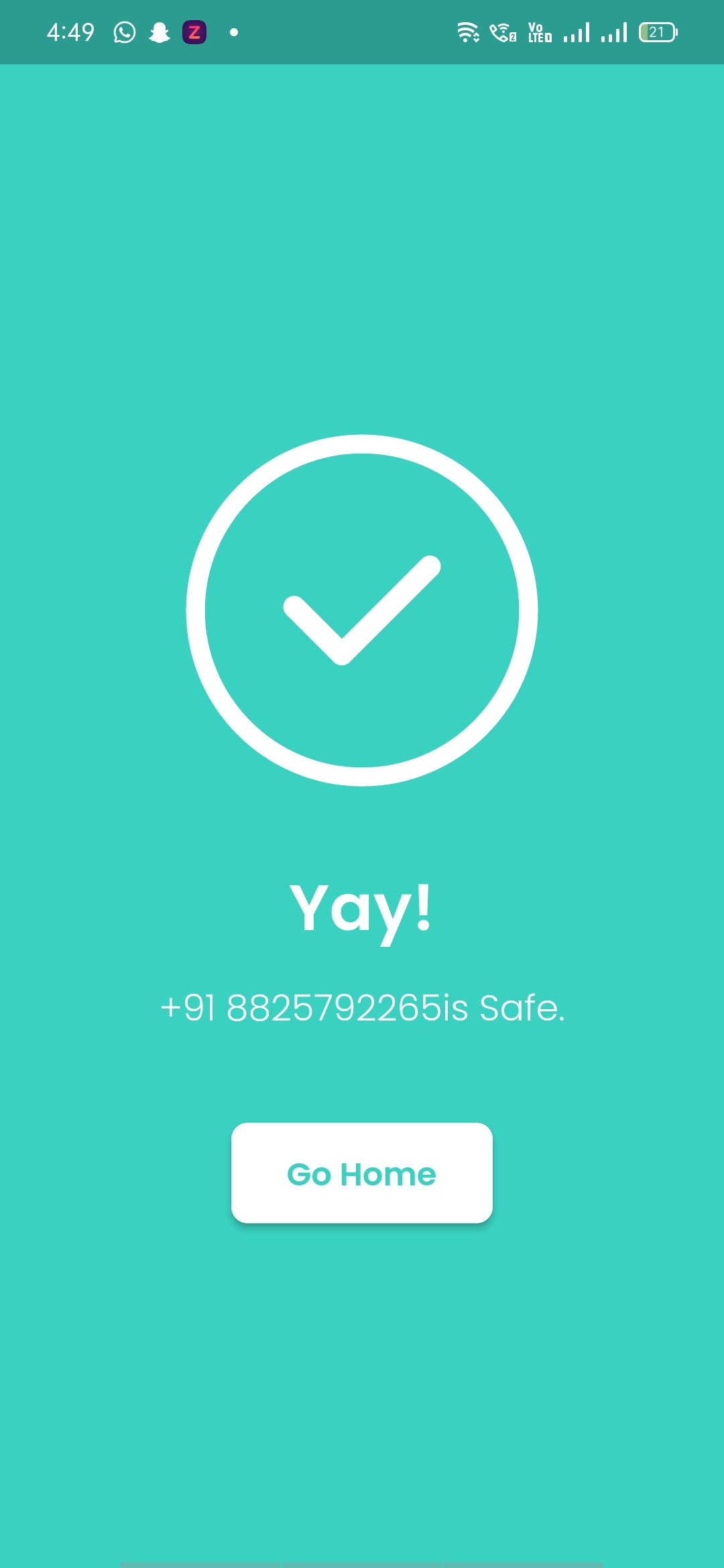
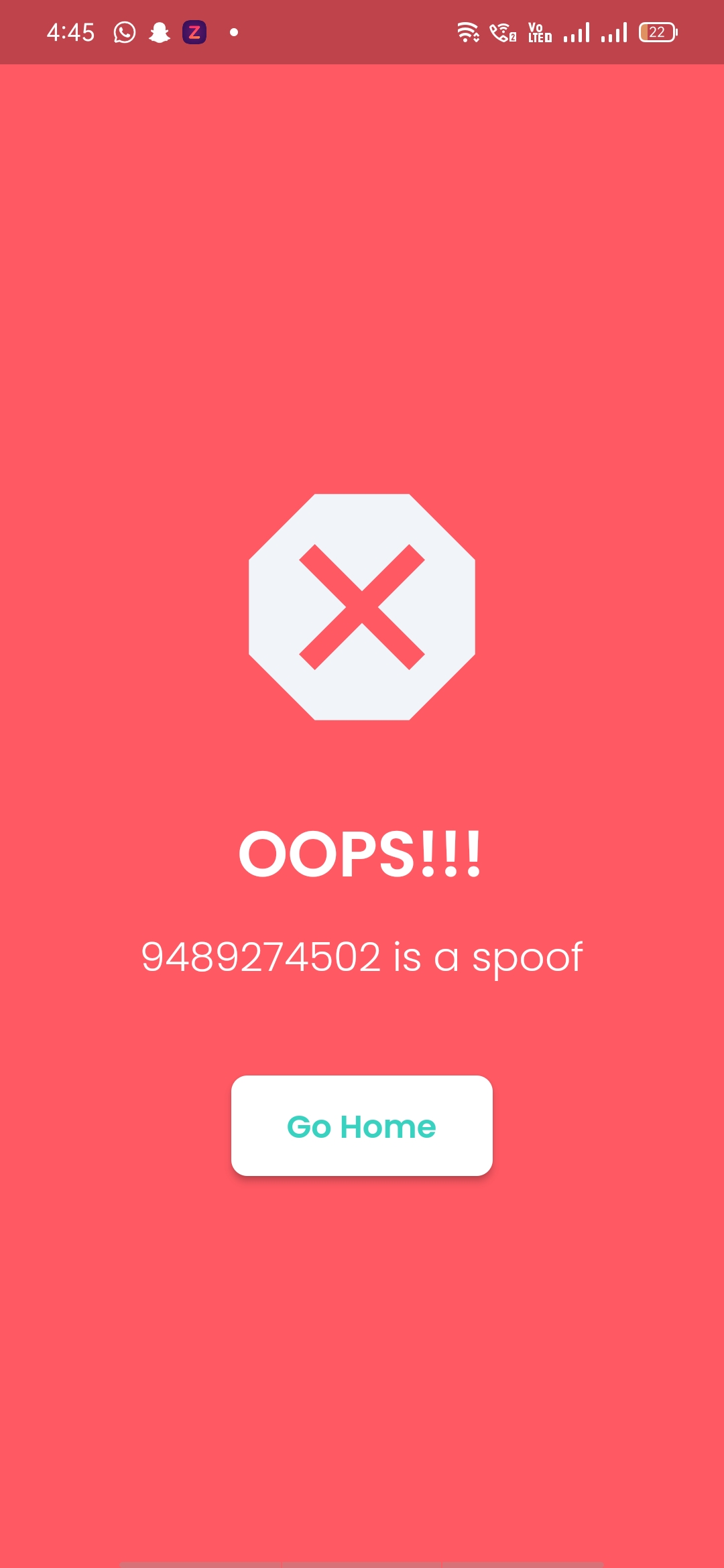
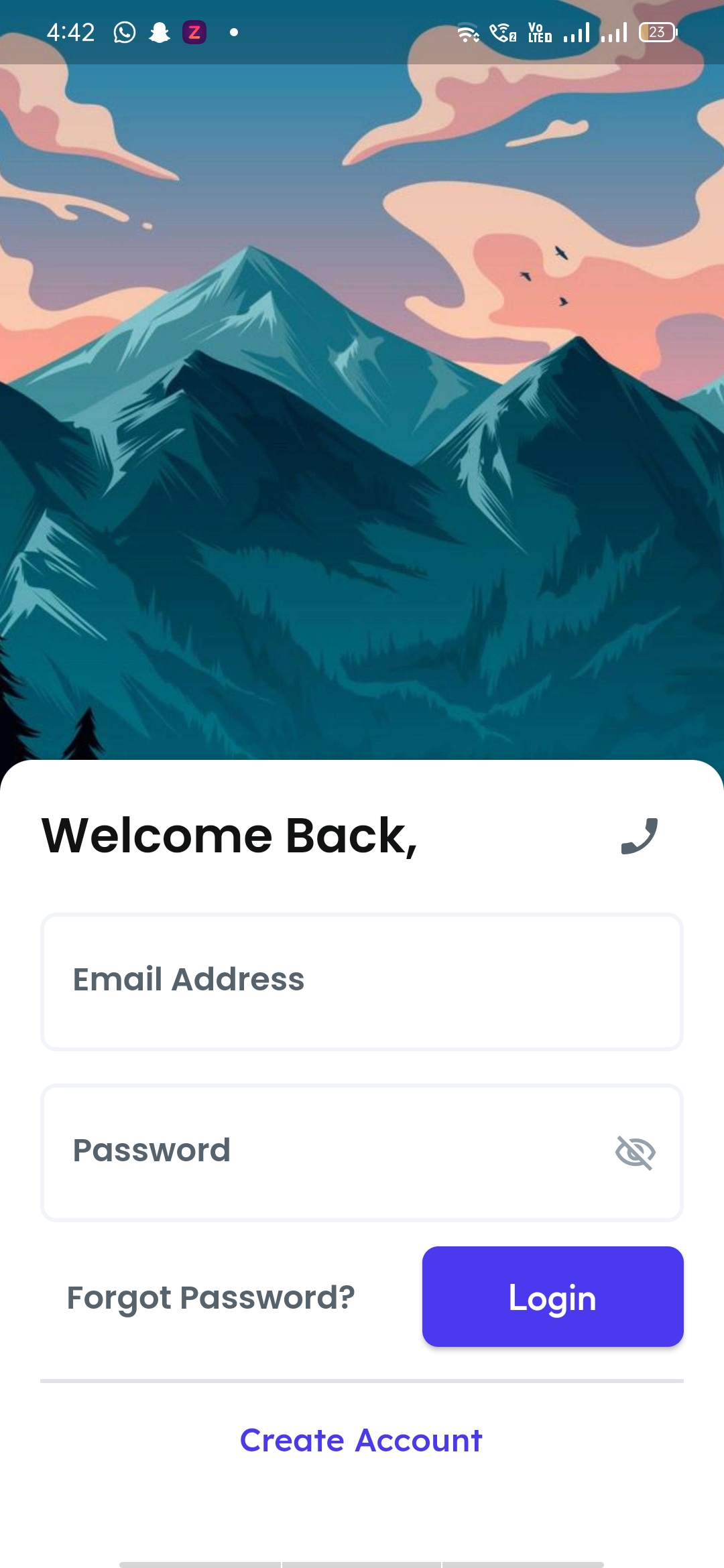
Application:

Flutter is a free and open-source mobile UI framework created by Google .In a few words, it allows us to create a native mobile application with only one codebase. This means that you can use one programming language and one codebase to create two different apps (for iOS and Android).

Flutter consists of two important parts:

* An SDK (Software Development Kit): A collection of tools that are going to help you develop your applications. This includes tools to compile your code into native machine code (code for iOS and Android).
* A Framework (UI Library based on widgets): A collection of reusable UI elements (buttons, text inputs, sliders, and so on) that you can personalize for your own needs.
* Dart is a typed object programming language.

**SPOOF DETECTOR APPLICATION:**





Contributors:

* SAJITH.M
* U.SHIVA RAMA KRISHNAN
* YUVANESH.G
* SRINIVASAN.S
* MADHUMITHA.G
* S.JANET RAJAJOTHI
* Dr. Jeneetha Jebanazer. J
* Feel free to drop a mail at [sajucools01@gmail.com](mailto:sajucools01@gmail.com) regarding any queries.
* Special thanks to the Department of Telecommunication of India.