iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51956

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Stingray Device for Cyber-Surveillance using a Software-Defined Radio as an IMSI Catcher

Aishwarya R[1], Sanjana Ramesh[2], V Viknesh Balaji[3], Yash Sikhwal[4], Dr. P V Bhaskar Reddy[5]
REVA University

Abstract: ***The Stingray or IMSI-catcher is a surveillance device for cellular phones that was initially developed by the Harris Corporation for military use. Nowadays, various local and state law enforcement agencies across countries such as Canada, the United States, and the United Kingdom use similar devices widely. The term Stingray has also become a general term for this type of device. The IMSI catcher has two modes of operation- active and passive. In the active mode, the device pretends to be a cell tower, tricking all nearby mobile phones and cellular devices to connect to it. It can be mounted on vehicles, low flying airplanes and helicopters, UAVs, etc. It broadcasts signals that seem stronger than the cell tower, and thus, it forces each compatible cellular device to disconnect from its service provider (e.g., Jio, BSNL, etc.) and establish a new connection with the device. Cellular communications protocols require mobile phones and cellular devices to connect to the strongest signal. We have used a Software Defined Radio (SDR) to replicate the Stingray device manufactured by the Harris Corporation. Although this device has a shorter range, it can still track the IMSI of all cellular devices around it. This project also demonstrates how fragile our privacy is concerning our devi***

I. INTRODUCTION

Cyber-Surveillance has been increasingly relied on by governments to carry out certain administrative tasks in the health, welfare, education and civil security sectors. Businesses keen toprotect certain information or to monitor the behavior of their employees or clients have also engaged in “cyber-surveillance” and corporate surveillance. Civil society and citizens'organizations may also use information technologies to monitor the words and deeds of authorities or businesses as part of strategies to publicly denounce conduct they deem to be unacceptable. Finally, delinquents and criminal groups may turn to cyber-surveillance in the pursuit of their objectives. The stingray device can be extremely beneficial to the government if used for the intended purpose, i.e. to hunt for criminals and national threats. If an approximate location of the threat is known, a stingray can be deployed near the region. The stingray will provide the phone numbers present in a particular radius around it. An even more advanced version can intercept the calls and messages being sent through the target’s device.

The motivation for this project was taken from the highly regarded Netflix documentary, “Web ofMake Believe.”

II. LITERATURE SURVEY

S.No	Title	Year	Pros	Cons	Methodology
1	Shahid, Z., Raza, M. A., Malik, A. W., & Khan, M. A. (2020). Software Defined Radio: An Overview, Technology and Its Applications. Journal of Electrical Engineering, 20(1), 175- 189.	2020	Provides a comprehensive overview of SDRtechnology andits applications invarious fields	Does not provide a critical evaluation of the limitationsof SDR or anynew research findings	The authorsused a literaturereview methodology.
2	Chabukswar, V. R., & Patil, S. K. (2019). Cyber Surveillance using Stingray Device. International Journal of Engineering and Advanced Technology,8(4), 81-85.	2019	Presents a new method for cyber-surveillance using a Stingray device, which could potentiallybe useful for lawenforcement and intelligence agencies	Does not discuss any potential ethical or legalconcerns associated with using Stingray devices forcyber surveillance	The authors describe the technical detailsof the Stingraydevice and how it can be used forcyber surveillance

3	NIST (National Institute of Standards and Technology). (2019). Guidelines for the use of cell site simulator technology. NIST Special Publication 800-146.	2019	Provides detailed guidelines and recommendations for the use of cell site simulator technology by law enforcement and other authorizedentities	Does notprovide an in-depth evaluation ofthe effectiveness of cell sitesimulator technology forlaw enforcement purposes	NIST developedthese guidelines through a collaborative process thatincluded input from stakeholders in government, law enforcement, industry, academia, andcivil liberties organizations
4	Yan, H., Qian, Y., & Wang, W. (2019). 5G mobile networks: Vision, requirements and challenges. Science China Information Sciences,62(2), 210301.	2019	Provides a detailed overviewof the vision andrequirements for 5G mobile networks, including their technical capabilities and potential applications	The paper is focused primarily on the technical aspects of 5G technology, and does not address broader societal or economic implications	The authorsused a literaturereview methodology to gather information from academic databases, technical journals, andindustry reports
5	Reimann, F., & Stöver, R. (2017). An SDR-based system for detection and tracking of UAVs in the ISM bands. In 2017 IEEE International Conference on Microwaves, Antennas, Communications andElectronic Systems (COMCAS) (pp. 1-6). IEEE.	2017	Presents a new system for detecting and tracking unmanned aerial vehicles (UAVs)using software-defined radio (SDR) technology	The proposed system has only been tested in a laboratory environment, and its performance in real-world conditions is not yet known	The authors describe the design and implementation of an SDR-based system forUAV detection and tracking in the ISM bands. They conducted experiments to evaluate the system's performance, including its ability to detectand track multiple UAVs simultaneously

III. POSITIONING

1) *Problem Statement:* Cell-Site Simulators are advanced tracking and snooping devices used by several developed countries, previously unheard of in pertinence Indian law enforcement. Also called StingRays/IMSI catchers, through this project we research and implement a small scale model of this device so as to demonstrate its valuable assistance to legal agencies in matters of great public safety and national security.
2) *Product Position Statement:* Our product is an IMSI catcher designed to be used bylaw enforcement authorities and individual corporations alike. These devices can be used in tracking members of crime organizations as well as help in tracking down the exact locations of missing persons or devices.

IV. PROJECT OVERVIEW

A. *Objectives*

1) Capture GSM signals using an SDR and be able to track IMSI numbers of nearby cellulardevices.
2) Decrypt the GSM signals and intercept/read data packets.
3) Provide an encryption means for data captured using IMSI catcher

B. Goal

The main goal of this project is to build a working IMSI tracker using a software defined radio (RTL-SDR) and a PC, and provide said device to law enforcement agencies to be used in regulation.

V. PROJECT SCOPE

The scope of the Stingray Device using a RTL-SDR as an IMSI catcher is to capture GSM signalsaround the devices and obtain the IMSI numbers of the devices. This will in turn allow us to triangle the location of the said device.

VI. METHODOLOGY

A. PC with Linux

Linux is a free and open-source OS. It is well-known for its resilience, security, and adaptability. It is commonly used for servers, desktop computers, and mobile devices. It delivers a sophisticated command-line interface as well as a large collection of open-source software tools to users. It is highly modifiable and can be adjusted to the requirements of the user. It is made up of several small, specialized components that may be joined in a variety of ways to create a personalized operating system. Hence, Linux is a robust and versatile operating system that has emerged as a significant component of the computing environment.

Tested with:

1) Ubuntu 20.04: Ubuntu 20.04 is a popular open-source OS that is based on the Linux kernel. It is well-known for its stability, ease of use, and security. It comes with a slew of pre- installed software, including productivity tools, web browsers, multimedia apps, anddevelopment tools. It also contains a robust package management system that makes installing, updating, and deleting software packages simple. Ubuntu 20.04 offers a modern and configurable user interface that can be readily tailored to the demands of the user. It isuseful in various applications, including desktops, servers, and cloud-based systems. Furthermore, it is a Long-Term maintenance (LTS) release, which means it will receive upgrades and maintenance for the next five years.
2) Kali 2020+: Kali Linux 2020+ is a well-known open-source OS that was created primarily for penetration testing and digital forensics. It is based on Debian Linux and comes with avariety of pre-installed tools for ethical hacking and network testing. It offers a configurable and powerful interface that can be readily tailored to the demands of the user. It also contains a robust package management system that simplifies the installation, updating, and removal of software applications. It is extremely flexible and may be readilytailored to the needs of the user and is frequently used to examine and test the security of computer systems and networks by security professionals, network administrators, and ethical hackers.

B. SDR receiver

An SDR (Software Defined Radio) receiver is a form of radio receiver that processes radio signals using software rather than traditional hardware circuitry. It enablesversatile and efficient signal processing, making it suitable for a variety of applications such as communication, signal analysis, and research. They are typically made up of two parts: radio hardware and software that runs on a computer. The radio hardware digitizes and captures the radio signal, while the software processes it and provides a user interface for controlling the radio and studying the signal. They have various advantages over standard radio receivers, including increased flexibility, enhanced performance, and lower cost. They are easily adaptable to multiple frequencies and modulation types, making them suitable for a wide range of applications. Furthermore, the use of software for signal processing enables advanced signal processingtechniques, such as digital signal processing, that are not achievable with traditional radioreceivers.

Tested with:

1) *USB DVB-T key (RTL2832U) with Antenna:* A USB DVB-T key is a compact and portable device that allows users to receive digital terrestrial television (DTT) signals on acomputer or other device having a USB connection. DVB-T is an abbreviation for Digital Video Broadcasting - Terrestrial, which is the standard for broadcasting digital television signals over the air. It is typically comprised of a small USB dongle with an integrated tuner and antenna. It connects to the computer through USB and is powered by the USB port. The device collects the DTT signal and converts it to a digital version that can be seenon a computer. They are a popular solution for those who do not have a TV with a built-inDTT tuner to watch digital television on a computer. They have a number of advantages over standard television receivers, such as mobility, flexibility, and the ability to record and time-shift programmes. They are also usually less expensive than dedicated DTT receivers or set-top boxes.

2) *HackRF:* HackRF is a software-defined radio (SDR) platform that enables users to explore,analyze, and manipulate a wide range of wireless signals. It is an open-source hardware platform that is designed to be affordable and accessible to users of all levels of expertise.The HackRF platform consists of a small and portable hardware device that connects to a computer via USB. The device includes a wide-band RF transceiver and supports a range of modulation schemes and frequency bands. It can be programmed and controlled using arange of open-source software tools, including GNU Radio, SDR#, and GQRX. HackRF is used for a wide range of applications, including wireless network security testing, reverseengineering of wireless protocols, and development of custom wireless communication systems. It is particularly popular in the field of cybersecurity and is used by security professionals, researchers, and hobbyists to analyze and manipulate wireless signals for various purposes.

VII. MODULES IDENTIFIED

1) *Obtain Hardware:* RTL SDR, PC with Kali/Linux installed.
2) *Install Required Dependencies:* Python 3.7, gr-gsm, GQRX, kalibrate-rtl and Wireshark.
3) *Calibrate the RTL-SDR:* Calibrate and find the offset value for your RTL-SDR by tuningit to a local FM Radio station using GQRX.
4) *Identify Active Frequency:* Find the active GSM downlink frequency in the area usingthe mobile device and kalibrate-rtl tool. (Generally between 925MHz - 960MHz)
5) *Capture GSM Signals:* Start gr-gsm and set the offset value, and tune in to the identifiedfrequency until you receive hex-values in the terminal.
6) *Observe GSM Packets:* Meanwhile open Wireshark, where the encrypted GSM packetscan be observed.

VIII. PROJECT IMPLEMENTATION

A. *Architectural Design*

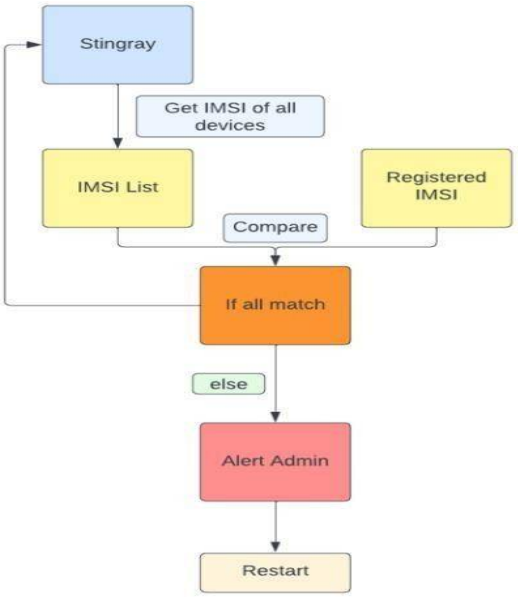


Fig. 8.1.1

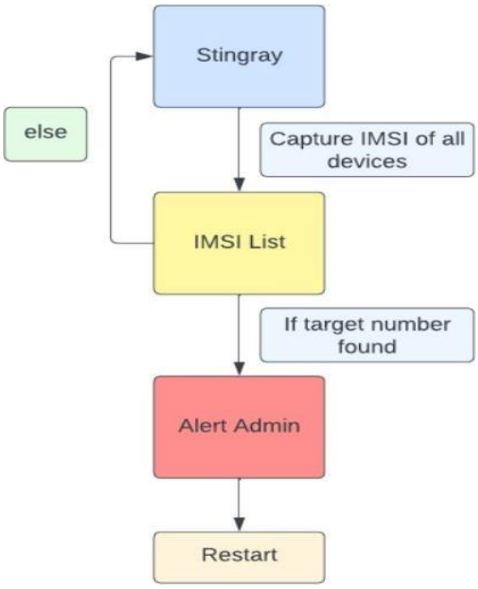


Fig. 8.1.2

Design-Workflow of the Stingray Device

1) *Figure 8.11:* Stingray in corporations- In this use case the Stingray device can be used to keep track of the devices being used inside a corporation based on the IMSI numbers of these devices. Hence it canhelp in identifying and alerting the admin upon the entry of unauthorized devices.
2) *Figure 8.12:* Stingray for law enforcement- In this use case the Stingray device can be used by law enforcementto trace the IMSI numbers within a certain vicinity of the device and hence can track a particular 'target' IMSI to its exact location. This favors national security, helps finding missing persons andmaintain general law and order.

B. Class Diagram

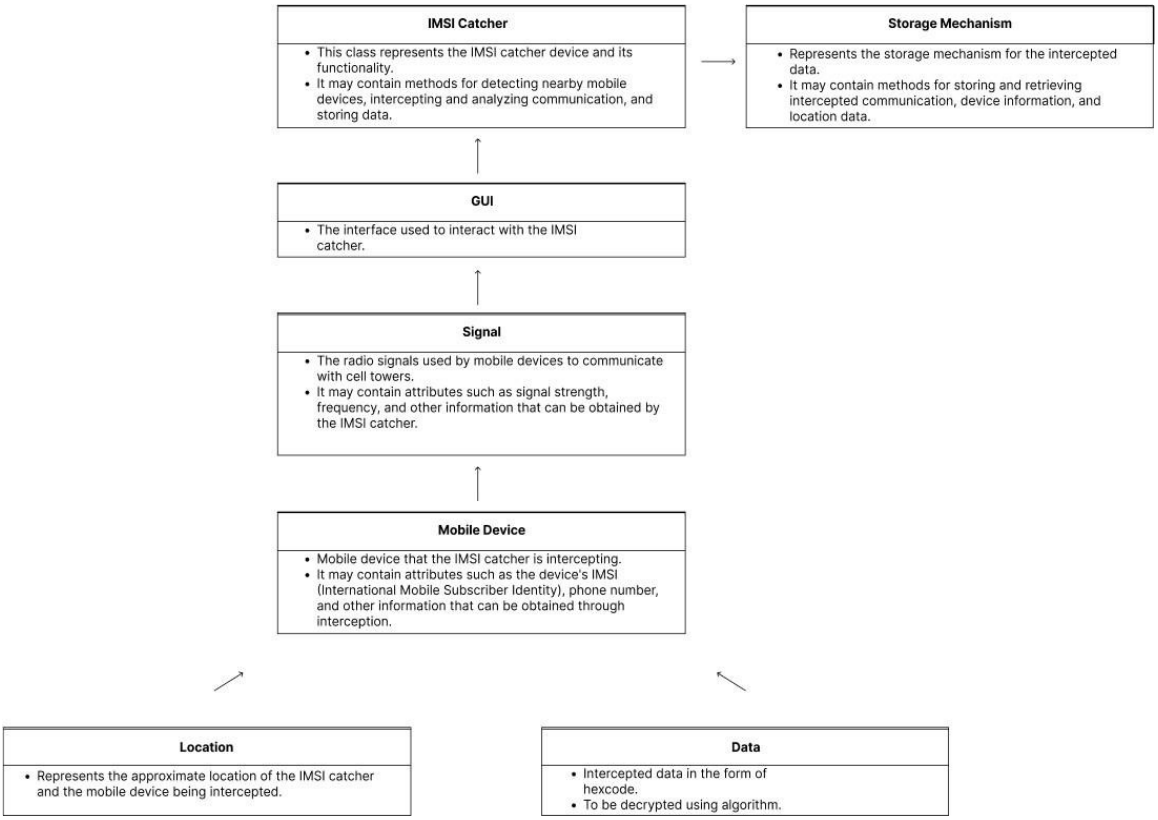


Fig 8.2.1 Class Diagram

C. Entity Relationship Model

1) In the case of a Stingray device, we can identify several entities and their relationships:

2) IMSI Catcher Entity: The Stingray device itself can be considered an entity. It has attributes such as the device ID, firmware version, and hardware specifications.

3) Law Enforcement Entity: The law enforcement officer who operates the device can be considered as a user entity. The officer has attributes such as badge number, name, and contact information.

4) Target Device Entity: The person or group being investigated can be considered as a suspect/target device entity. The suspect has attributes such as name, date of birth, and contact information.

5) Location Attribute: The location where the Stingray device is deployed can be consideredas a location entity. It has attributes such as the address, longitude, and latitude.

6) Data Attribute: The communication data collected by the Stingray device can be considered as a communication entity. It has attributes such as the phone number, message content, and call duration.

The relationships between these entities can be described as follows:

a) IMSI Catcher-Law Enforcement Relationship: One user can operate multiple Stingray devices, but one Stingray device can only be operated by one user.

b) IMSI Catcher-Target Device Relationship: One user can investigate multiple suspects, butone suspect can be investigated by multiple users.

The ER model for a Stingray device can be represented in a diagram that shows the entitiesand their relationships, such as the one below:

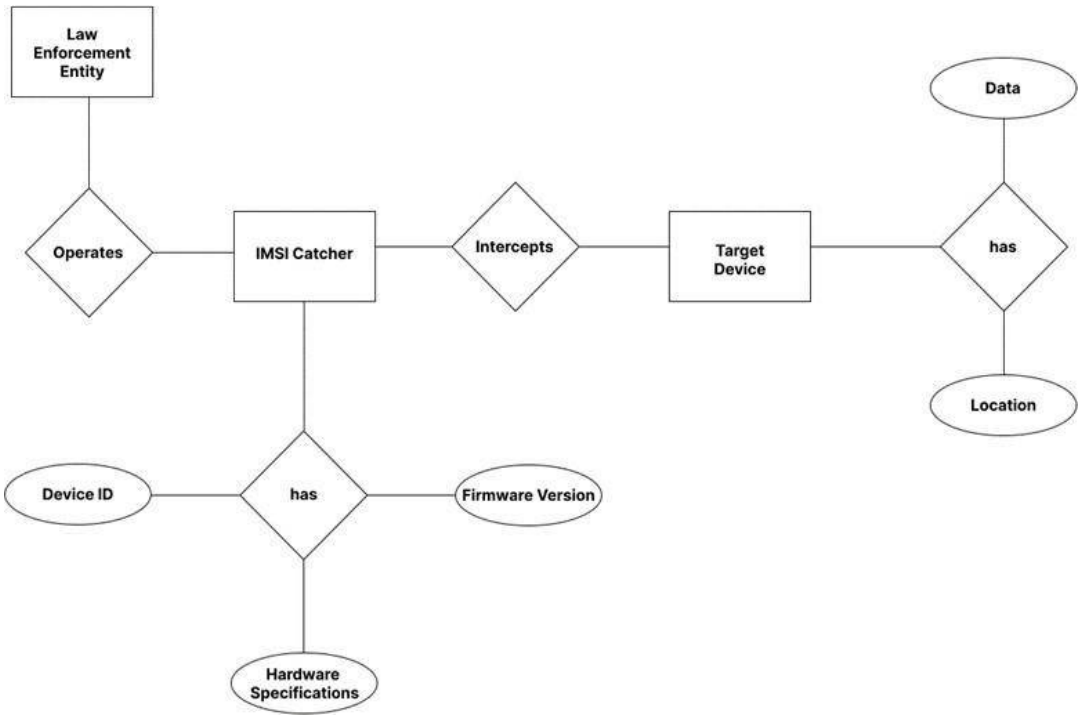


Fig 8.3.1 Entity Relationship Diagram

D. Sequence Diagram

Here are some possible object interactions for the major use case scenarios for cyber-surveillance using Stingray devices with an SDR:

1) Deploying the Stingray Device

a) User: authenticates()
b) User: authorize(location)*
c) Location: provides location data to Device
d) Device: start()
e) Device: collects communication data from Communication

2) Gathering Communication Data

a) Device: collects communication data from Communication
b) Communication: provides call duration, phone number, and message content toDevice
c) Analyzing communication data
d) Device: sends communication data to Analysis module
e) Analysis: analyzes communication data to identify suspicious activity
f) Analysis: sends analysis results to User

3) Investigating a Suspect

a) User: receives analysis results from Analysis
b) User: retrieves suspect information from Suspect
c) User: authorizes location of suspect
d) Device: collects communication data from Communication
e) Device: provides communication data to Analysis
f) Analysis: analyzes communication data to provide evidence against suspect
g) Analysis: sends evidence to User

4) Upgrading firmware

a) User: retrieves firmware upgrade from Upgrade module

b) Device: upgrades firmware using Upgrade module

These are just some possible object interactions for the major use case scenarios for cyber-surveillance using Stingray devices with an SDR. The specific interactions may vary depending on the implementation details of the system.

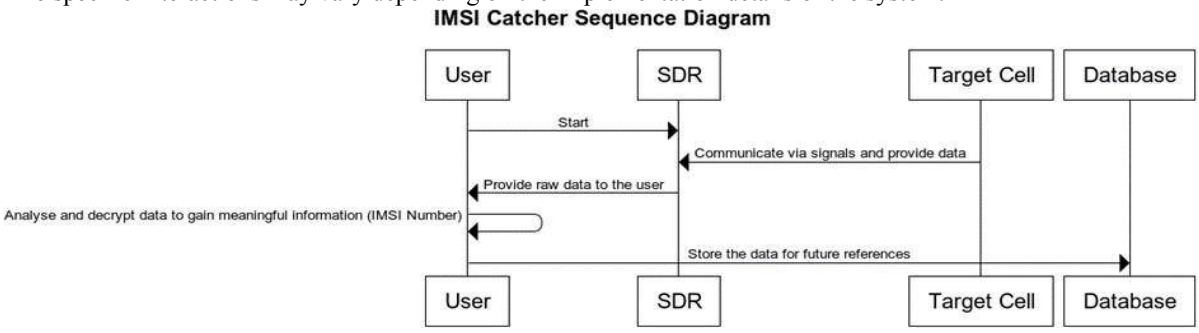


Fig. 8.4.1 Sequence Diagram

E. Description of Technology Used

A Stingray device is a type of surveillance equipment used by law enforcement agencies to intercept and analyze cellular communications. It works by simulating a cell tower andtricking nearby mobile devices into connecting to it, thereby allowing the device to intercept and monitor the communications of the targeted mobile devices. Software- defined radio (SDR) technology is often used to build Stingray devices, as it allows for a flexible and programmable approach to wireless communication. Here are some of the technologies commonly used to build a Stingray device using an SDR:

1) *SDR Hardware:* The radio frontend, analog-to-digital converter (ADC), and digital signal processor (DSP) are all physical components of an SDR Stingray device. The SDR hardwarereceives and converts analogue radio signals into digital signals that the SDR software can process.
2) *SDR Software:* The most significant component of the Stingray gadget is the SDR software. It is incharge of impersonating a cell tower and intercepting cellular communications. The software analyses intercepted signals and extracts relevant information from them using various signal processing methods. Frequency hopping, signal modulation, signal demodulation, signal filtering, signal amplification, and signal decoding arejust a few of the functionalities that can be coded into the software.
3) *GNU Radio:* GNU Radio is a free and open-source SDR toolkit that provides a foundation for developing SDR applications. It comes with a set of signal processing blocks that can be used to create custom signal processing pipelines for a variety of wireless communication standards. GNU Radio is compatible with a wide range of SDR hardware platforms and offers a versatile programming environment for developingcustom SDR applications.
4) *LTE Protocol Stack:* Cellular networks communicate with mobile devices using the Long-Term Evolution (LTE) protocol stack. To impersonate a cell tower and intercept cellularconversations, the Stingray device must comprehend the LTE protocol. The LTE protocol stack is usually implemented in software and can be used to create customLTE base stations using SDR technology.
5) *RF Amplifiers and Antennas:* RF amplifiers and antennas are utilized to extend the Stingray device's range and sensitivity. RF amplifiers are used to boost received signals, whereas antennas areused to pick up signals in the air. The antenna and amplifier to be used are determined by the frequency ranges and communication standards to be used.

Overall, the combination of SDR hardware, SDR software, GNU Radio, LTE protocol stack, RF amplifiers, and antennas provides a robust and versatile foundation for developing Stingray devices for cyber-surveillance. It is crucial to emphasize, however, that the usage of such devices must be done in accordance with applicable rules and regulations.

IX. FINDINGS / RESULTS OF ANALYSIS

So far, through our project we are able to obtain hexadecimal values in the terminal whichindicate the packets being transmitted from the base station to the device (Downlink). These packets can be visualized in a more organized way in Wireshark. However, decrypting these packets to obtain IMSI numbers is still under progress. Also, the stingraydevice is limited to capturing only GSM frequencies.

X. COST OF THE PROJECT

A. Requirements

Kali Linux with gr-gsm, GQRX and WiresharkPython 3.7+
4 GB RAM+
i3 processor

B. Cost Analysis

Internet connection - Rs.2500Photocopies - Rs.500
RTL-SDR Dongle with antenna - Rs. 4000

XI. CONCLUSION

Creating Stingray devices with software-defined radio (SDR) technology offers a flexible and configurable way to wireless communication. These devices, which can impersonatea cell tower and intercept cellular conversations, have become a significant tool for law enforcement organizations in combating cybercrime and terrorism.

The project on Stingray devices made using SDR has offered a thorough understanding ofthe technologies and techniques used in their development. The project has emphasized the significance of SDR hardware, SDR software, GNU Radio, LTE protocol stack, RF amplifiers, and antennas in the development of Stingray devices.

The study has also emphasized the importance of adhering to existing laws and regulations when deploying Stingray devices for surveillance purposes. When deploying Stingray devices, ethical and legal factors must be taken into account, as with any technology.

In conclusion, the study established the value and efficacy of leveraging SDR technology to develop Stingray devices for cyber-surveillance objectives. As technology advances, we may expect more developments in the development of Stingray devices, and it is critical that we continue to balance the requirement for security with the preservation of privacy and individual rights.

XII. PROJECT LIMITATIONS AND FUTURE ENHANCEMENTS

A. Limitations

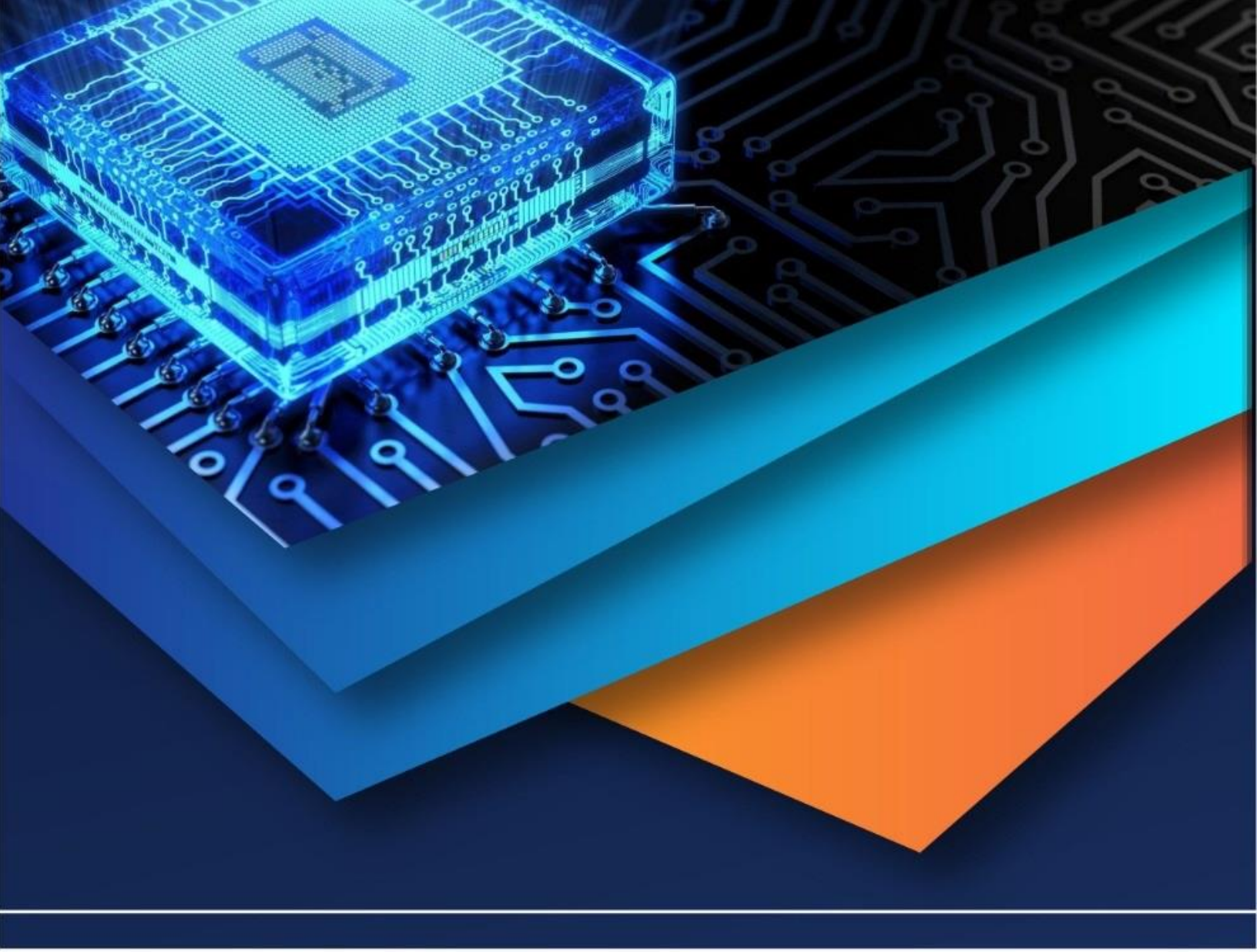
1) *2G Detections:* The stingray device exclusively operates on GSM frequencies and is not capable of detecting signals beyond 3G, 4G, and 5G. Additionally, intercepting and deciphering 4G signals is more challenging.
2) *Lack of Concrete Decryption Method:* The device is incapable of monitoring phone callsand text messages as all communication channels are typically encrypted with a stream cipher (A5), which is used to ensure privacy in the GSM cellular telephone standard. Theencryption key is saved in the SIM card and is never transmitted over the network, makingit impossible to capture encryption keys over the airwaves. Furthermore, the encryption key changes with each call setup, implying that every call has a distinct encryption key.

B. Enhancements

1) *Data Decryption:* The encryption provided by the older A5 cipher can be broken through brute force with more powerful computational resources, as demonstrated by researchers who cracked A5/1 encryption using a cloud setup with extensive computational capabilities. There is a Github repository called GSM Decryption (Kraken) that can be used for this purpose.
2) *Intercepting Higher Frequencies:* As for newer technologies, such as 4G and 5G, they use higher frequency bands that can be intercepted using software-defined radio (SDR) technology, which can receive higher frequencies. Further investigation is needed to determine how to decrypt the intercepted information from these newer technologies.

REFERENCES

[1] Shahid, Z., Raza, M. A., Malik, A. W., & Khan, M. A. (2020). Software Defined Radio: An Overview, Technology and Its Applications. Journal of Electrical Engineering,20(1), 175-189.
[2] Chabukswar, V. R., & Patil, S. K. (2019). Cyber Surveillance using Stingray Device.International Journal of Engineering and Advanced Technology, 8(4), 81-85.
[3] NIST (National Institute of Standards and Technology). (2019). Guidelines for the useof cell site simulator technology. NIST Special Publication 800-146
[4] Yan, H., Qian, Y., & Wang, W. (2019). 5G mobile networks: Vision, requirements and challenges. Science China Information Sciences, 62(2), 210301.
[5] Reimann, F., & Stöver, R. (2017). An SDR-based system for detection and tracking ofUAVs in the ISM bands. In 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) (pp. 1-6). IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY