Signal analysis

In this project, we adopted an integrated, practical methodology that begins with analyzing radio frequency (RF) signals and recognizing patterns, and receive it through a receiver and filter the signal to get the correct transmission.

Multi-purpose IoT Security Guard Edge Node

Graduation Project for CyberSecurity

The Team

Sami Saad

IoT Specialist - Cyber Security

Graduate Cyber security student

Ahmad Jamhour

Penetration testing - Cyber Security

Graduate Cyber security student

Introduction

Our project is a specialized device designed to emulate threat types of radio frequency and Wi-Fi attacks , with the ultimate goal of developing and innovating effective protection techniques against them.

Why did choose this project?

We chose this project due to the lack of security in many RF and Wi-Fi-based systems, and the growing number of real-world attacks targeting them.

📌 **Examples of real incidents:**

- **RF replay/cloning** – open garage doors and smart home devices.
- **Signal jamming** – disable car remotes and alarms with no alert.
- **Wi-Fi deauth attacks** – disconnect users and hijack sessions.
- **Drone hijacking** – take control of unprotected RF signals.

🎯 Our goal: Emulate these threats and build smart defenses.

Problem

What problem is the project trying to solve?

The problem in our project is trying to protect smart cars and homes from attacks via over-the-air wireless networks.

Objectives

Radio frequency analysis and detection

Development of an integrated defense device using Raspberry Pi

Real-time Emulation of attacks to understand and stop these attacks

Methodology

In this project, we adopted an integrated, practical methodology that begins with analyzing radio frequency (RF) signals and recognizing patterns, then building an integrated device to test and execute attacks, and finally developing intelligent protection mechanisms based on detecting abnormal behavior and interference.

Signal analysis

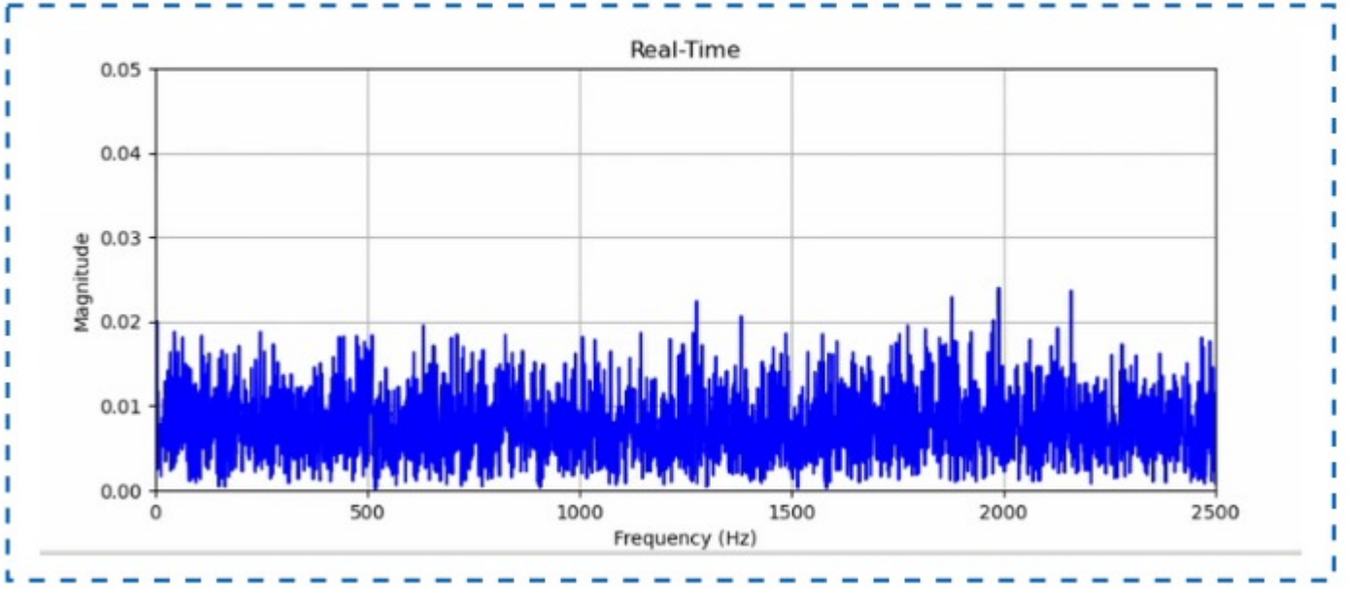
Hardware design

Attack Emulation

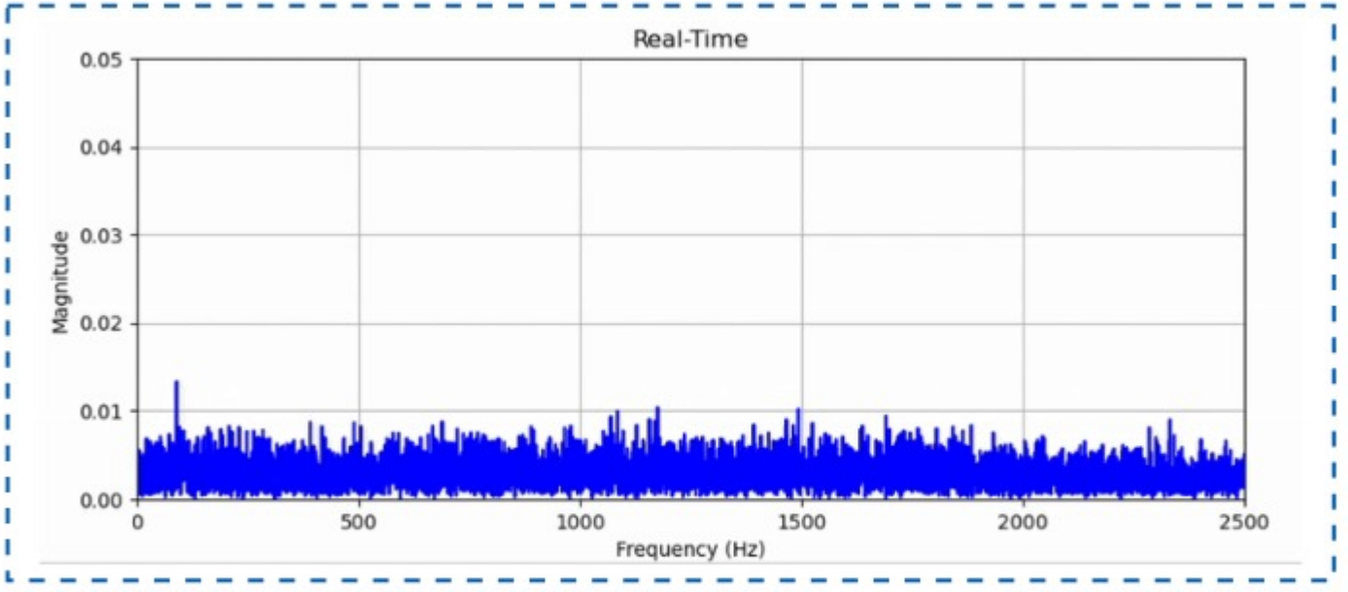
Defense Implementation

Environmental Noise: Before vs. After Filtering

The **raw environmental noise** spectrum captured without any filtering. The graph shows a high density of random peaks distributed across the frequency range, making it difficult to distinguish between real signals and background interference.



The **same environment after applying filtering by using Temporal-Statistical RF Frame Filtering.** As seen, the background noise level has significantly decreased, and the spectrum became flatter and more stable, indicating a much cleaner signal space.



What is Temporal-Statistical RF Frame Filtering technique

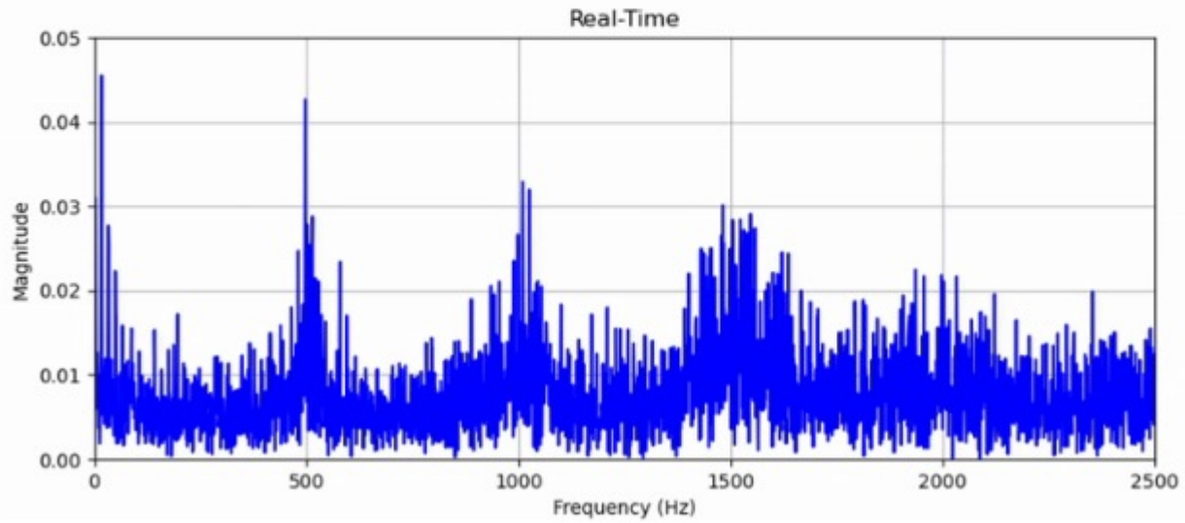
A hybrid signal filtering technique that combines time-domain analysis, statistical consistency checks, and bit-pattern validation to isolate valid RF transmissions from environmental noise.

The filtering process depends on the values of the following thresholds :

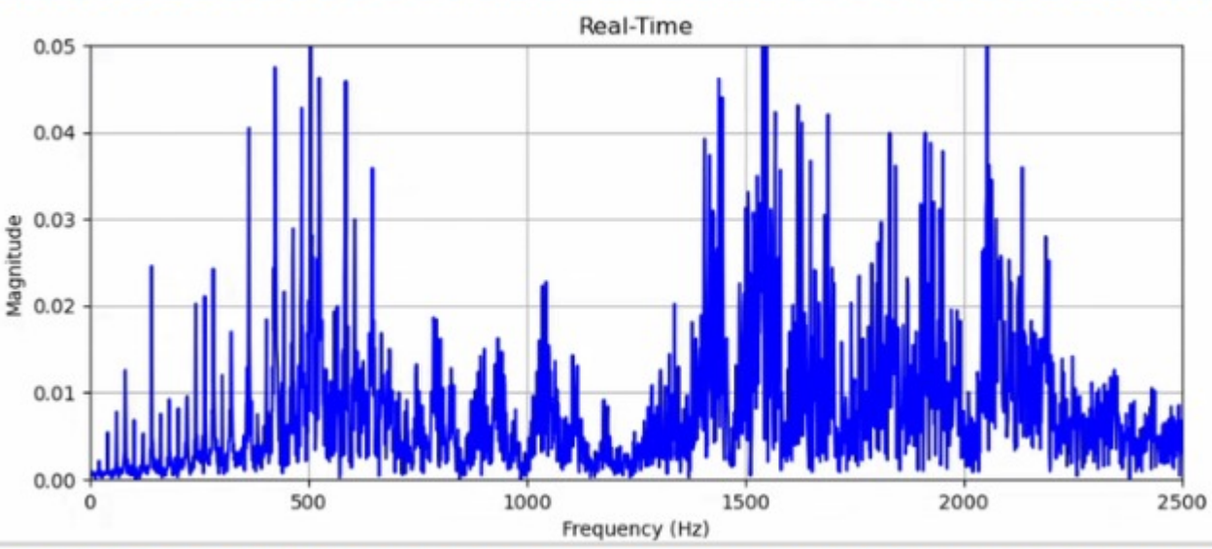
Parameter	*Purpose*	*Example Value*
MIN_PULSES	*Minimum number of edges to consider "a frame"*	*20*
MAX_STD_DEV	*Max allowed µs variation among pulse intervals (noise filter)*	*200 µs*
MIN_BITS_LEN	*Minimum bit-pattern length after conversion*	*24 bits*
MAX_BITS_LEN	*Maximum bit-pattern length*	*96 bits*
REPEAT_SUPPRESSION_MS	*Ignore duplicate frames within this time*	*500 ms*

Car Key Signal: Before vs. After Filtering

The raw frequency spectrum of the car key signal before noise filtering. The signal contains many sharp peaks, but they are partially buried under background noise and overlapping components, which makes the signal harder to analyze not entirely correct.



Presents the same signal after applying noise reduction and outlier filtering. The spectrum becomes much clearer, with more distinct, well-separated peaks, allowing us to better understand the structure and frequency components of the original RF signal entirely correct.



Jamming Signal Spectrum – Real Execution

In this figure, we can see the result of a real RF jamming attack executed using our custom Python script on a Raspberry Pi. The jamming works by sending fast, random pulses continuously across a wide frequency range.

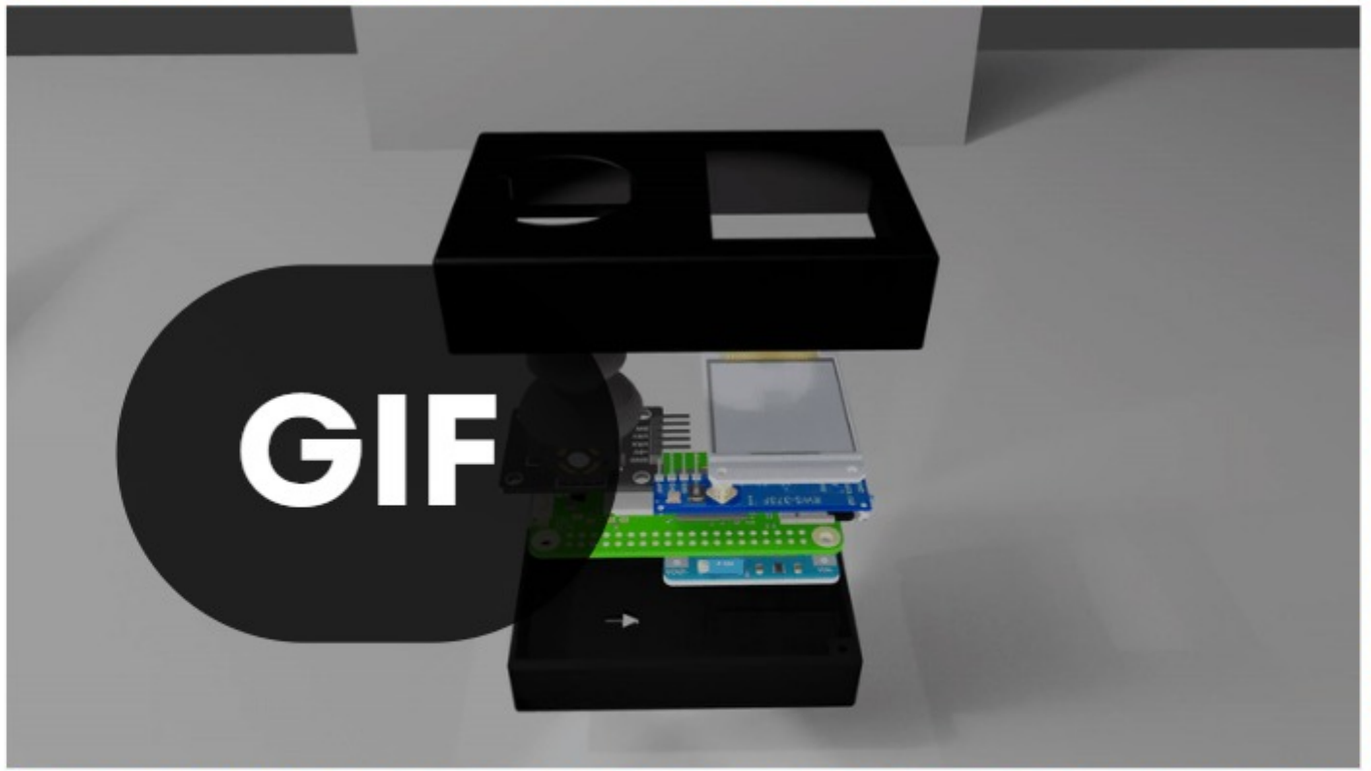
Unlike normal signals, this one doesn't have clear patterns — instead, it fills the spectrum with strong and chaotic energy, making it hard for any real device (like a car key) to communicate.

This means the jamming is:

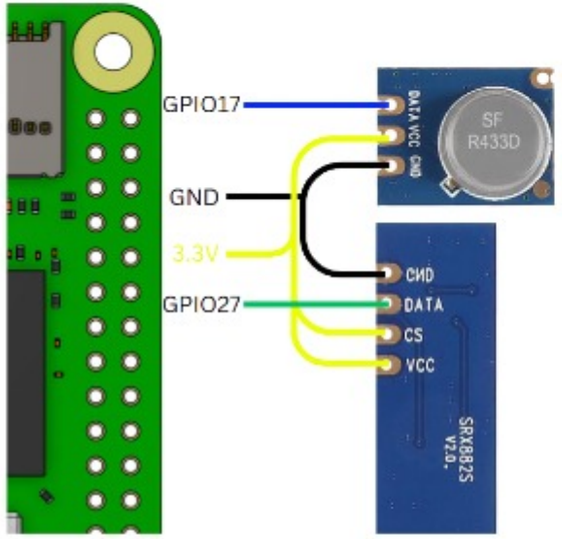
- Fast (50-500 Microseconds)
- Long-lasting (10 milliseconds)
- Wide (50-500 Microseconds)

Hardware design

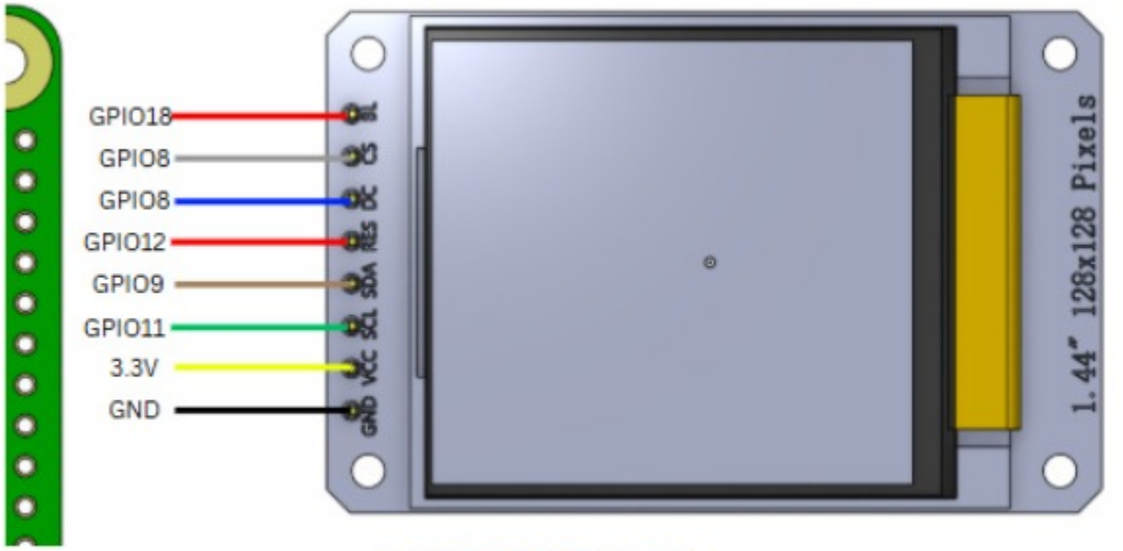
Here we show how the hardware was designed and built.



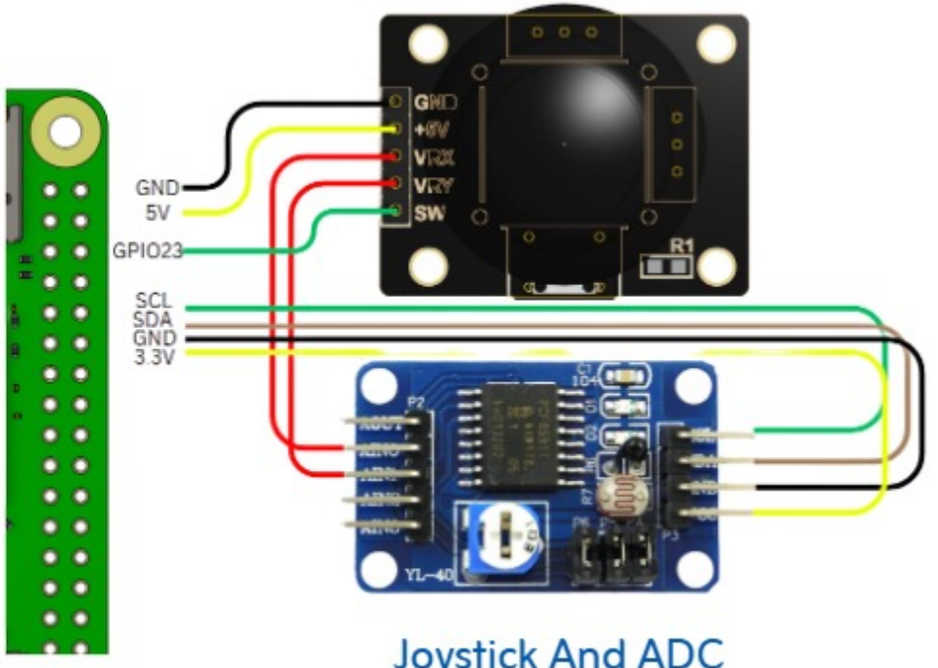
Hardware Wiring



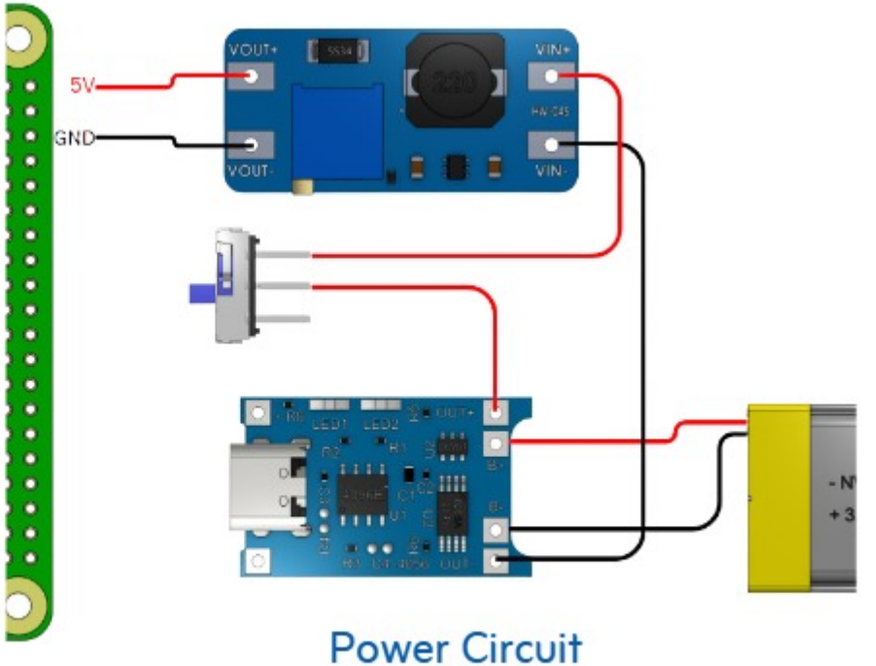
STX882 Transmitter
and
SRX882 Receiver



TFT 128*128 SPI

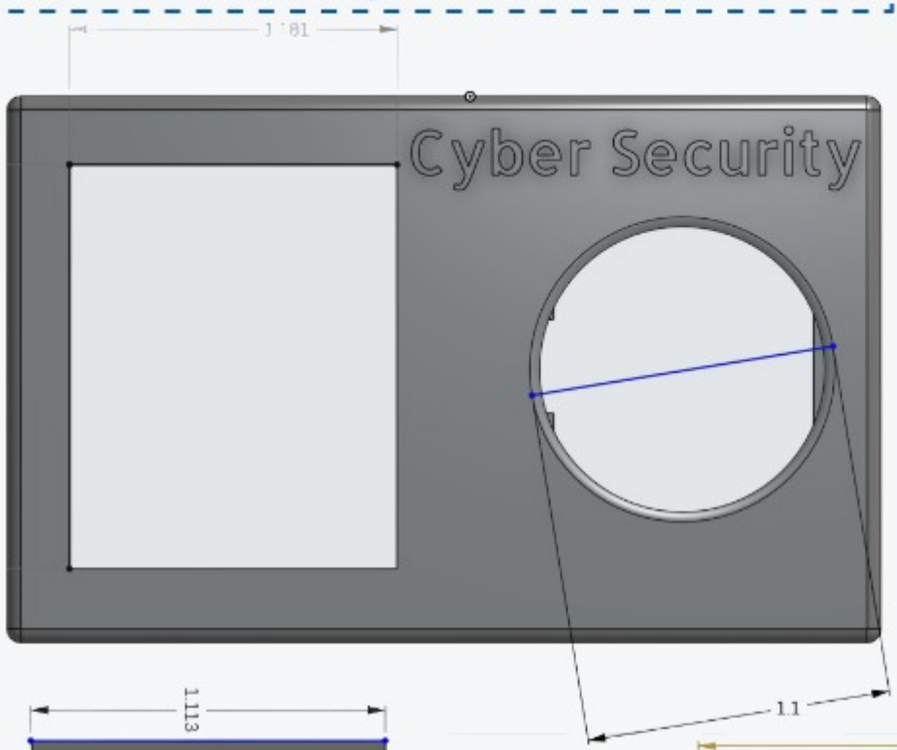


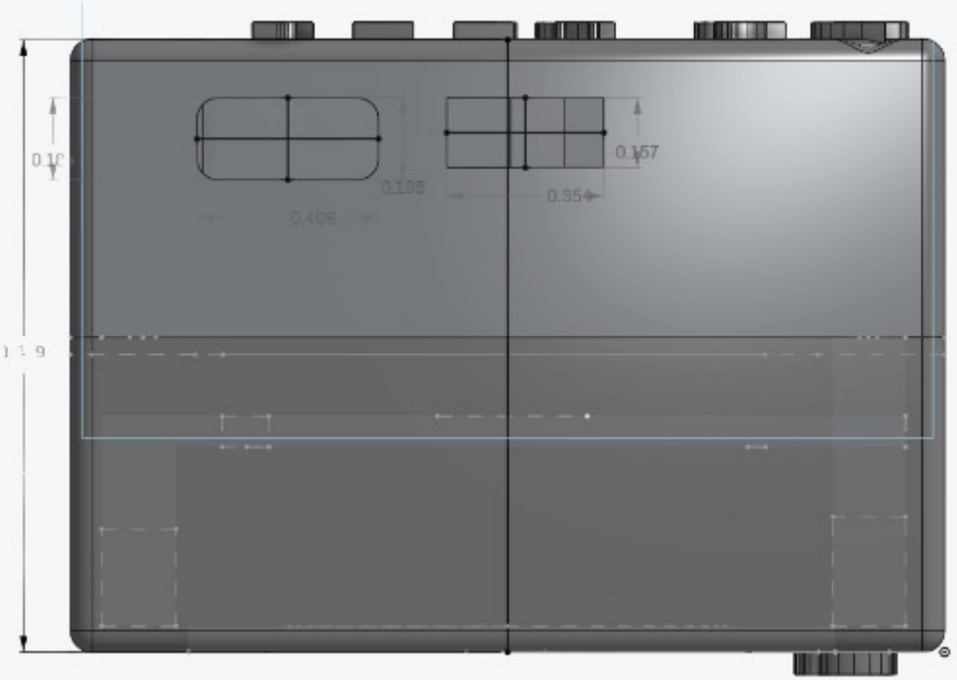
Joystick And ADC

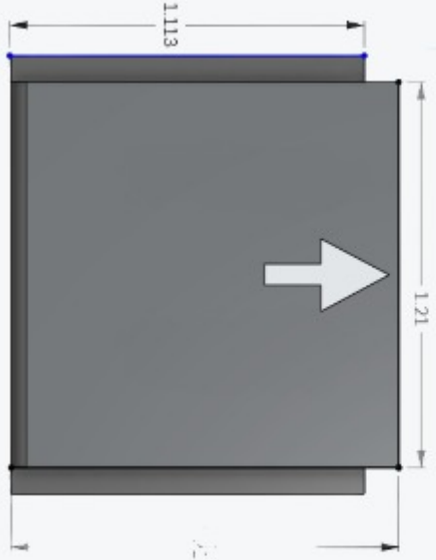


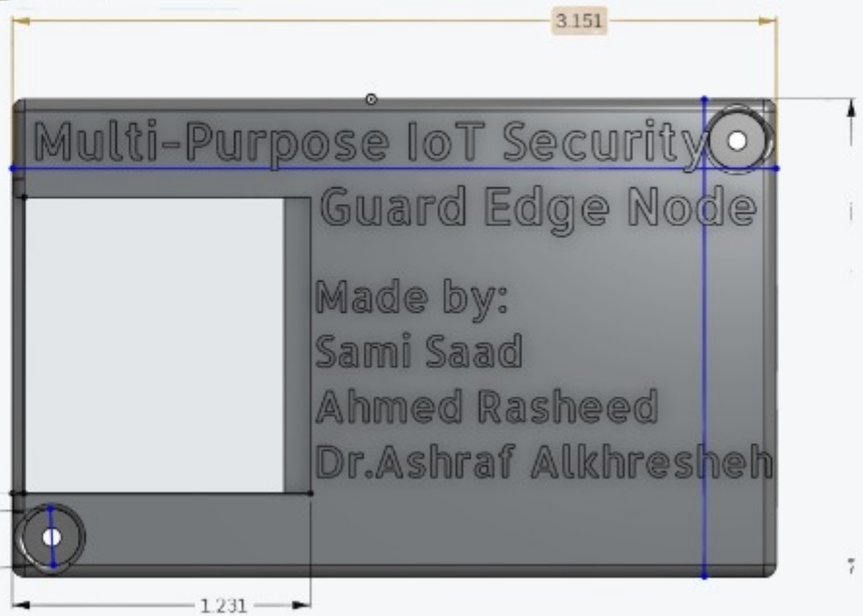
Power Circuit

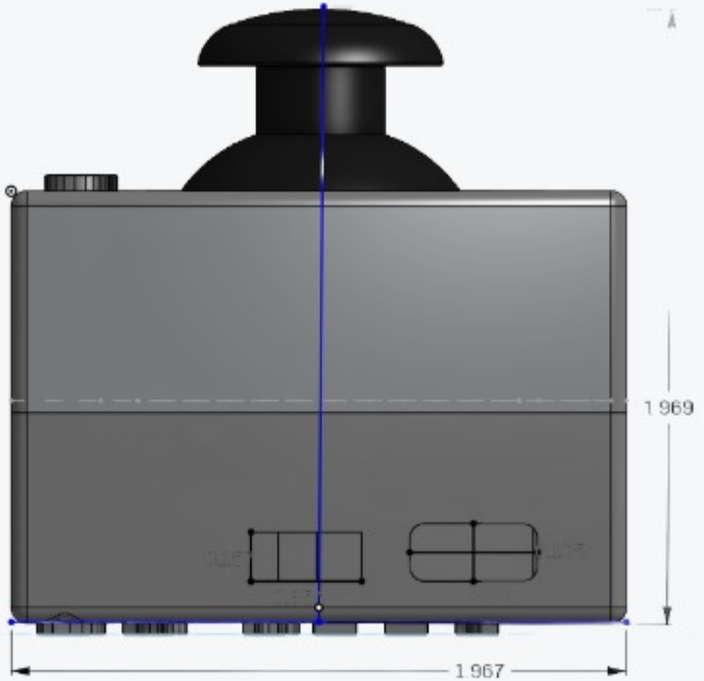
Device Design – 3D CAD View





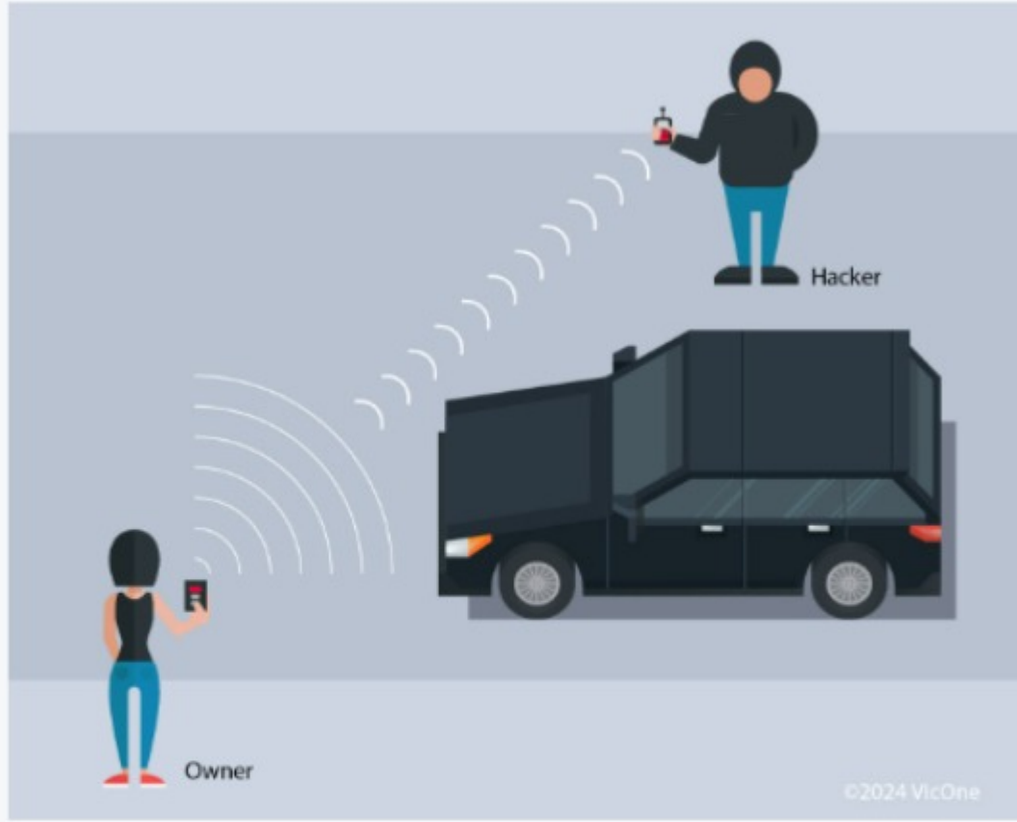






FIXED CODE CLONING ATTACK

- Many devices using 433 MHz rely on static (fixed) codes for access control (e.g., remotes, garage doors).
- The device captured a complete transmission from a real key fob.
- The signal showed a repeatable and identical waveform each time the button was pressed.
- Once recorded, the same signal was replayed using the transmitter, successfully triggering the target system.
- This confirms a critical vulnerability in fixed-code systems.



Jamming

Jamming is a type of **wireless denial-of-service attack** where an attacker **deliberately transmits radio frequency (RF) signals** on the same frequency used by legitimate devices.

The goal is to **interfere with communication**, causing **signal disruption or complete communication loss.**

Rolling key

A Rolling Key changes the code with every press using a shared algorithm and counter, preventing replay attacks by making old codes invalid.

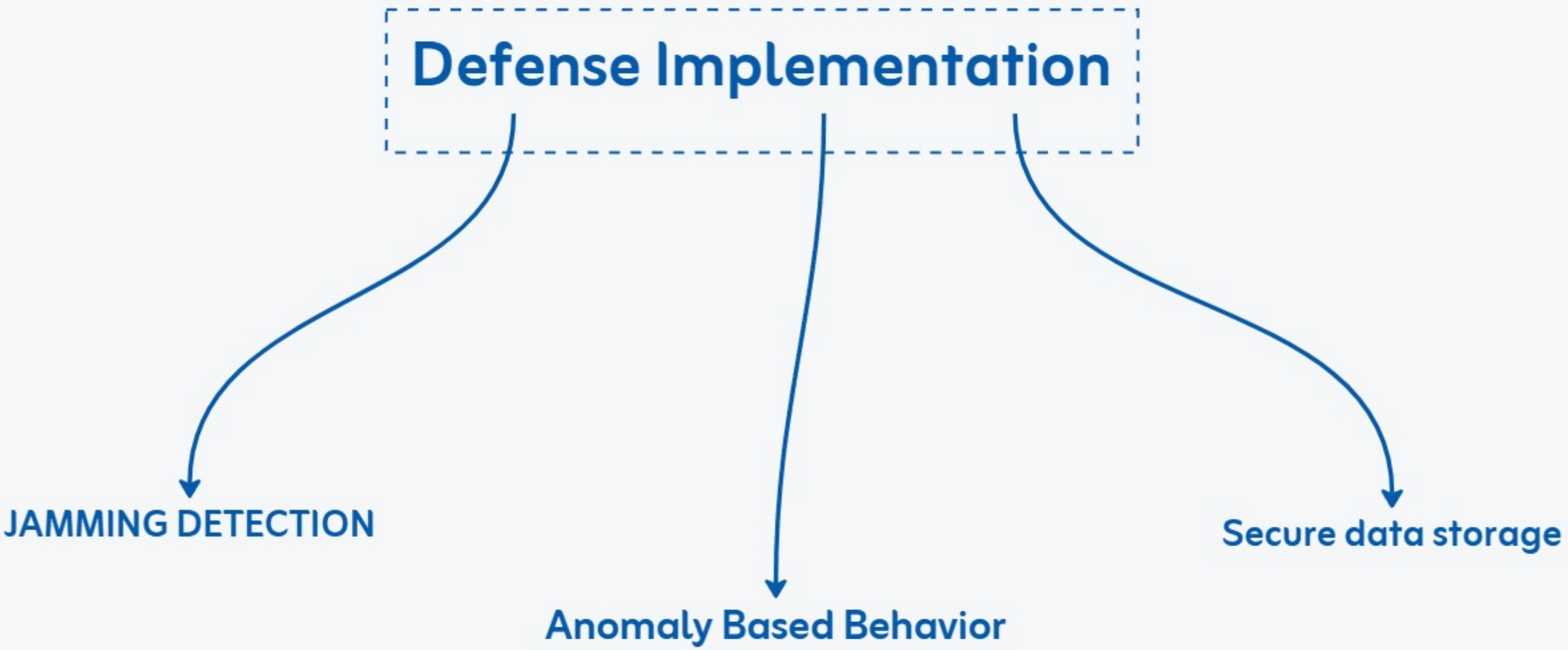
Hopping1 & Hopping2

Hopping1 uses predictable code jumps (like +1), while Hopping2 adds more variation to make code prediction harder.

Wi-Fi Security Assessment

In our project, we implemented a dedicated module for analyzing Wi-Fi security by simulating real-world attack scenarios and evaluating the resilience of wireless networks. This section of the device performs:

1. Scanning for available WPA/WPA2 networks.
2. Executing De-authentication attacks, forcing clients to reconnect and exposing the handshake process.
3. Performing offline password cracking using dictionary-based techniques rockyou.txt.


Defense Implementation
JAMMING DETECTION
Anomaly Based Behavior
Secure data storage

JAMMING DETECTION

- The device monitors RF signals for signs of continuous interference or abnormal silence, indicating jamming activity.
- During testing, a jamming signal was emitted in the 433 MHz band to simulate an attack.
- The system detected:
- Unusual signal patterns (flat/noise-heavy)
- Blocked legitimate transmissions
- Spike in RF energy without valid packet structure
- A visual alert is triggered when jamming is detected to prevent command injection or DoS.

anomaly based behavior

What is Anomaly-Based Behavior?

Anomaly-based detection is a technique that monitors the normal behavior of RF signals and then triggers alerts when any unexpected or unusual pattern occurs.

This approach allows us to:

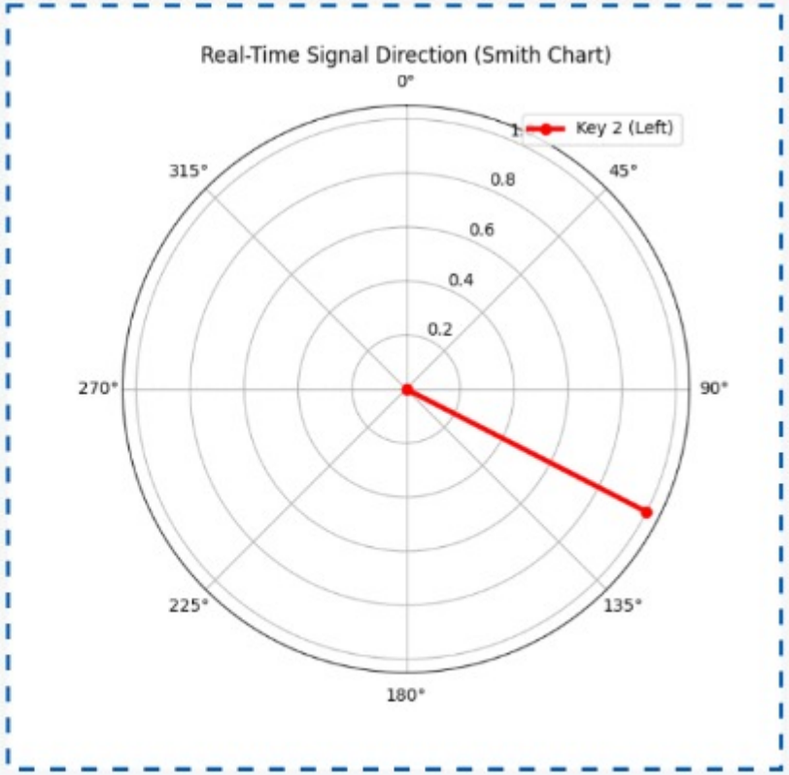
Detect cloned or tampered signals.

Identify spoofing or replay attacks.

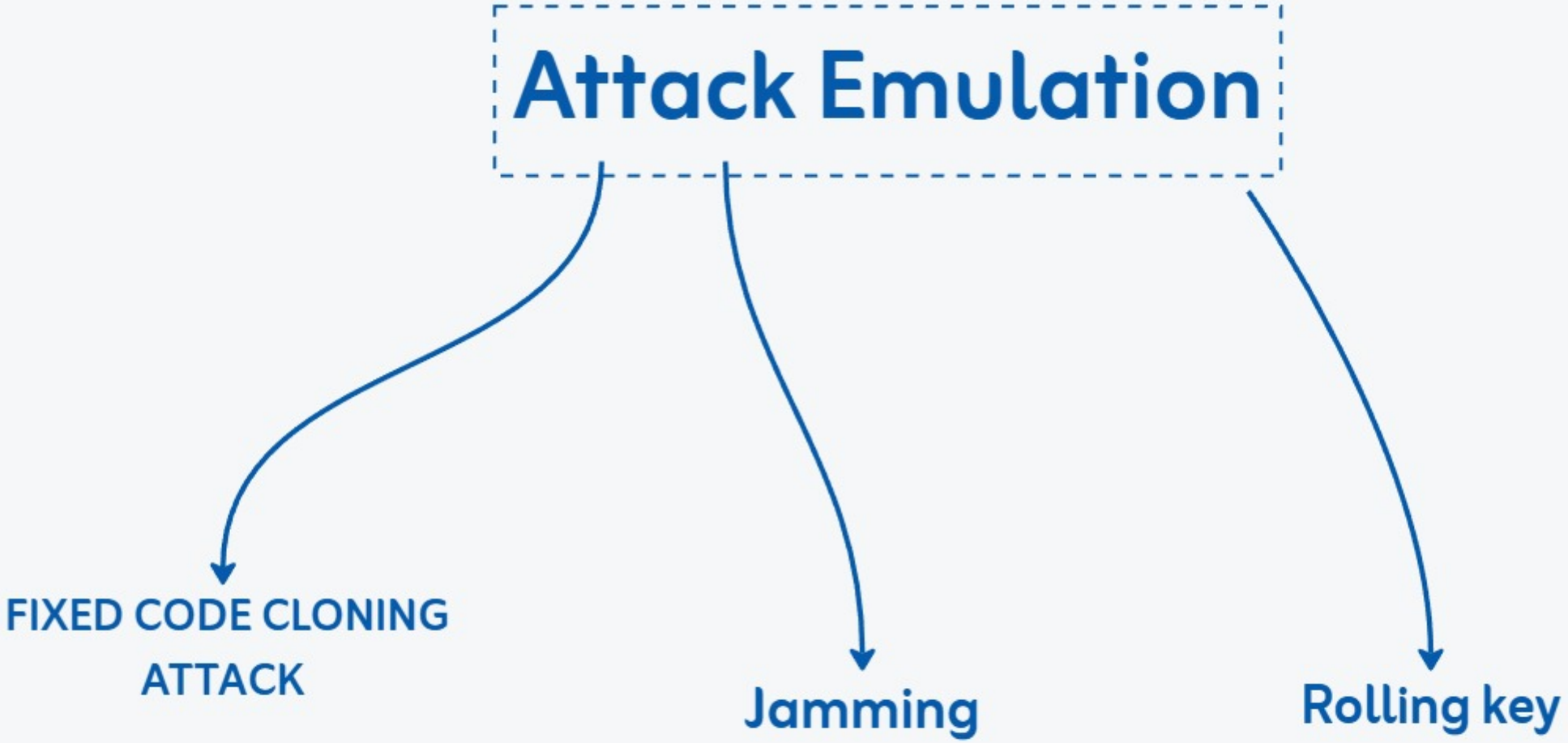
React dynamically to unknown or evolving threats.

Real-Time Signal Direction Detectiona

In this figure, we show a Smith chart representing the directional behavior of a real RF signal.
The red arrow represents a signal coming from a specific direction (e.g., "Key 2 – Left side").
By tracking angle, amplitude, and consistency,
we can tell whether a signal is expected or suspicious.



If a signal suddenly comes from a new direction or with unusual behavior, we consider it an anomaly and trigger a security response.


Attack Emulation
FIXED CODE CLONING ATTACK
Jamming
Rolling key

Secure data storage

To ensure our captured RF data and test results are safely stored and accessible, we implemented secure cloud storage.
We used Google Drive as our storage solution. After capturing data such as RF keys, signal logs, and jamming detections, the system uploads the files automatically to our protected Google Drive folder.

Backup protection in case the device is lost or damaged
Remote access to data anytime from anywhere
Data confidentiality, since only authorized users can access the folder
Our device ensures that all sensitive files are stored in the cloud safely and encrypted during transmission.

Demo

Thanks