Sniffer: Smart Device Proximity Mapping

Fairer Examinations for the New Generation

Madhan Kumar S 20BEC1112
Abhishek Sebastian 20BEC1118
Pragna R 20BLC1104

Current Scenario : Online Exams

Tab Switch* Has Not Checked the Usage Of Multiple Devices to Copy During Exams.

Sniffer: Smart Device Proximity Mapping

- **Sniffer is a conceptual framework for Smart Device Proximity Mapping, enabling real-time tracking and visualization of connected devices.**

- **It utilizes Bluetooth Low Energy (BLE) and signal strength measurements to estimate the distances between devices.**

- **The framework consists of a central scanning module that continuously scans for nearby devices and a visualization interface that represents devices as dots on a map.**

- **Sniffer can be implemented in examination environments to enhance security and integrity. By monitoring the proximity of devices during exams, it can help detect potential cheating attempts, such as unauthorized collaboration or the presence of additional devices. This can provide a valuable tool for maintaining the fairness and integrity of examinations.**

Concept:

Proposed Methodology
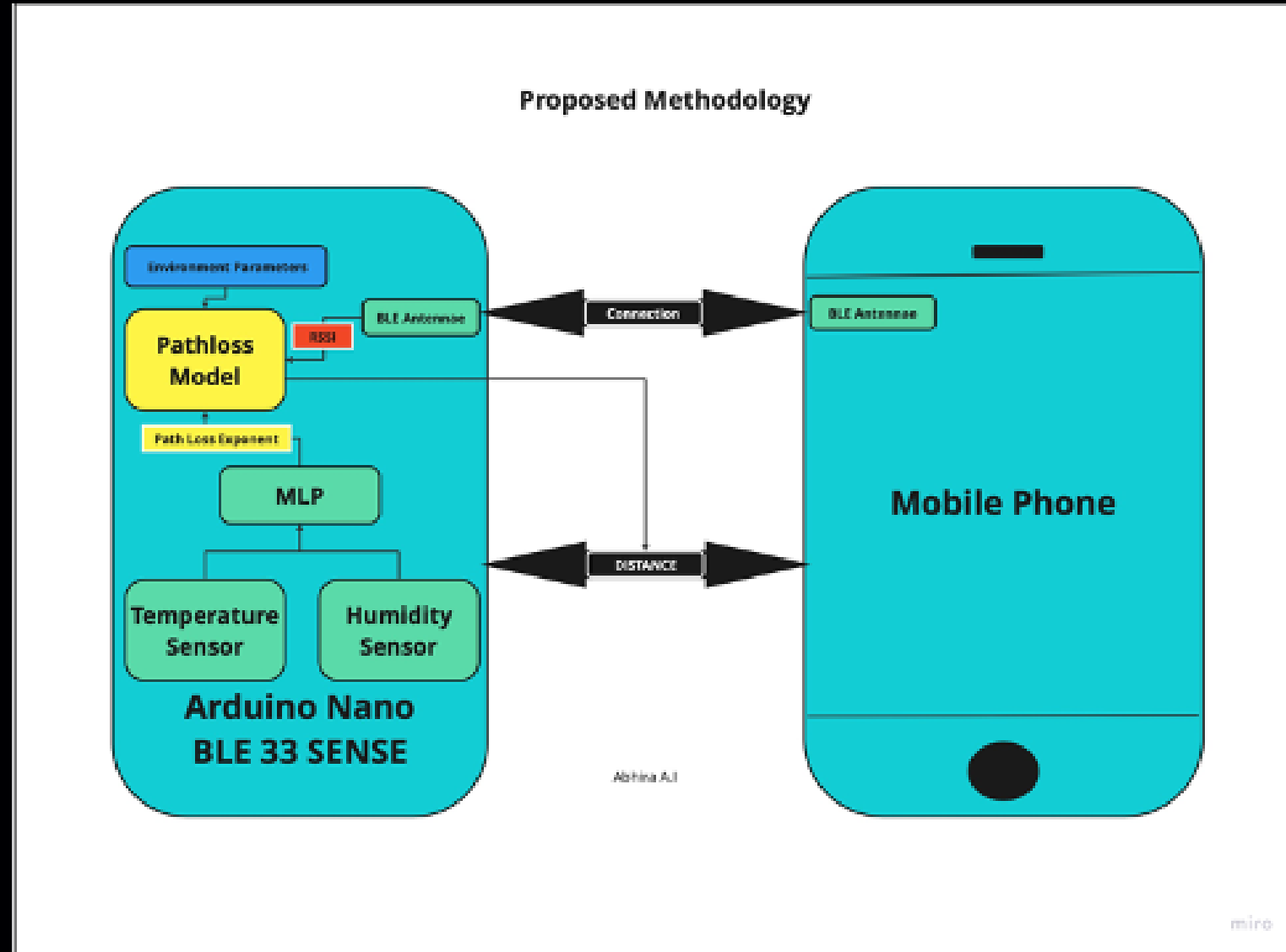
- **Firstly, we use the Received Signal Strength Indicator (RSSI) metric to estimate the distance between the devices based on signal strength, propagation, and attenuation effects caused by the environment**

- **Predicting path loss exponent with temperature and humidity is important to improve accuracy of BLE proximity detection in varying environments, as environmental factors * affect the propagation of RF waves.**

- **With accurate distances , We will be able to identify Devices with Closer Proximity to the Test Device**

*For example, in an air-conditioned room, the density of cold air can significantly affect the propagation of RF waves, leading to changes in the path loss exponent. By using temperature and humidity data to predict the path loss exponent, our proposed approach can account for these environmental factors and improve the accuracy of proximity detection between BLE devices.

useCase1:
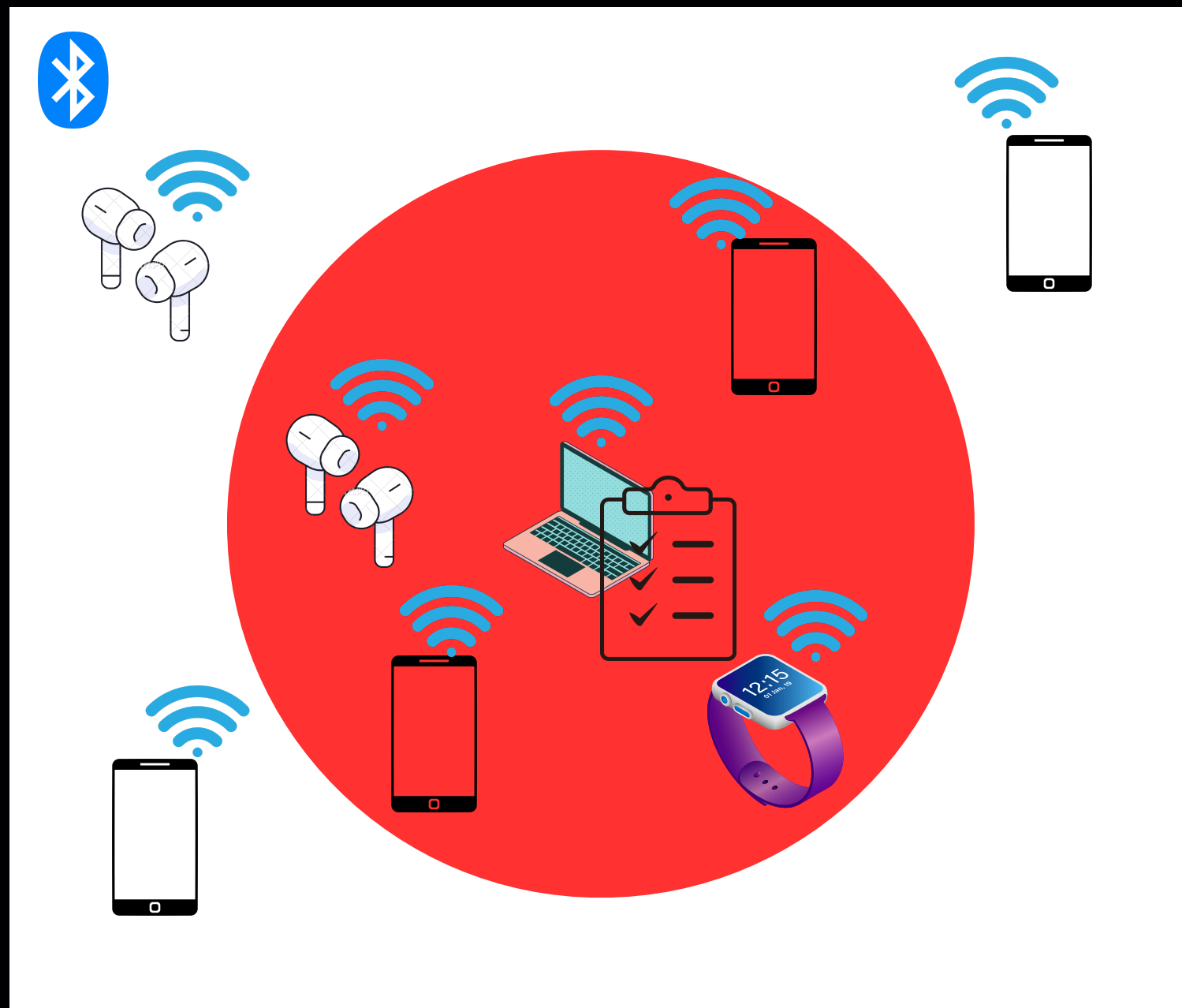
- Let's Consider a Usecase , If We Include this In a Online Proctoring System.

- Where The Student Takes the Exam in a Laptop , And Uses a Nearby Mobile Phone to Check For answers.
- With Our Proposed System We Will be able to Identify any Electronic devices that is bluetooth enabled.
- Providing a Added Security to the Existing Online Proctoring System Which includes (Tab Switch , Copy paste Disabled)

useCase2:
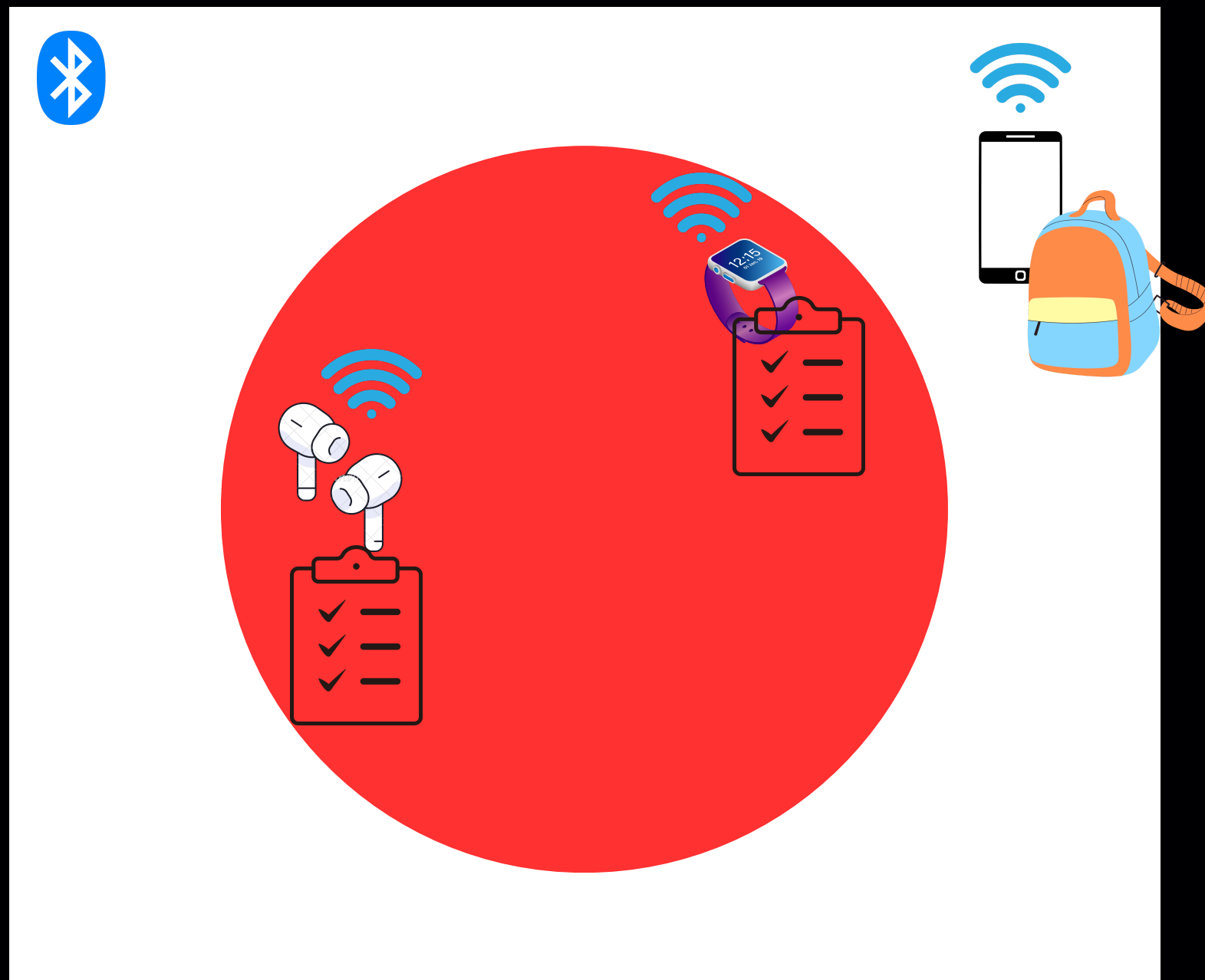
- **Let's Consider a Usecase , If We Include this In a Normal Clasroom Examination System.**

- **Where The Student Takes the Smaller Devices like BT Earphones , Smart Watches And Uses a Nearby Mobile Phone to Check For answers or have some kind of Communication with the Outer world.**
- **The proposed system will be able to check if there are any BT devices are used in the classroom**
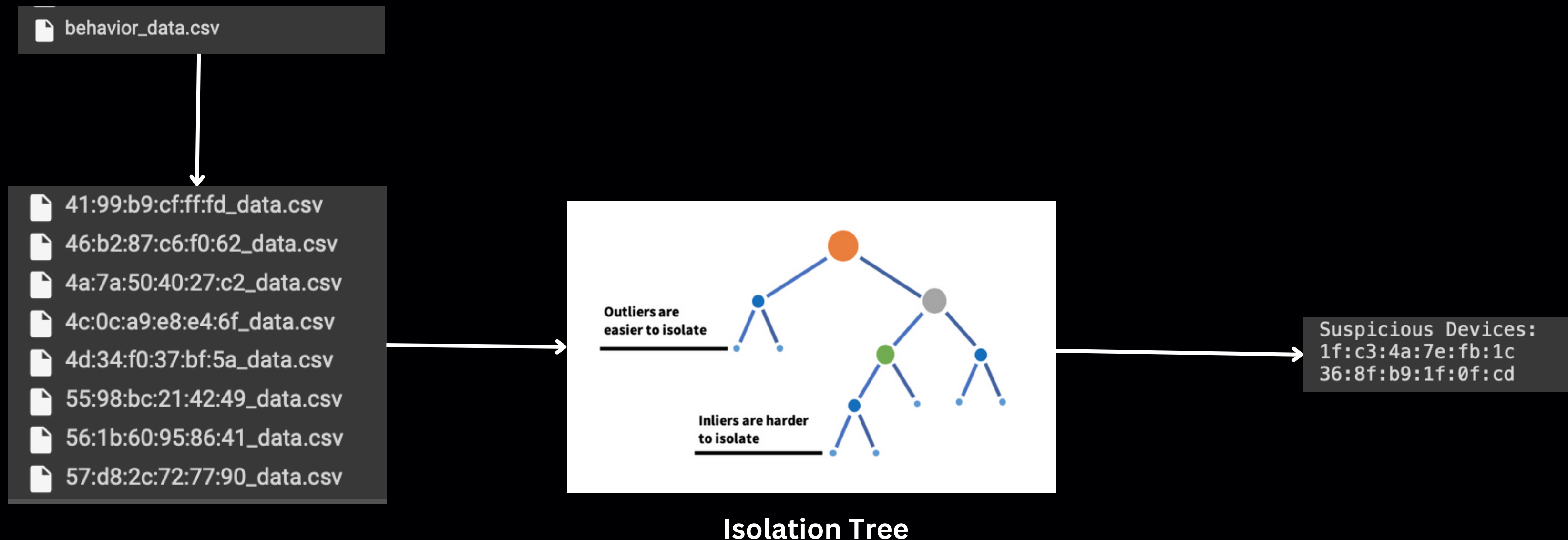
Working: Radar
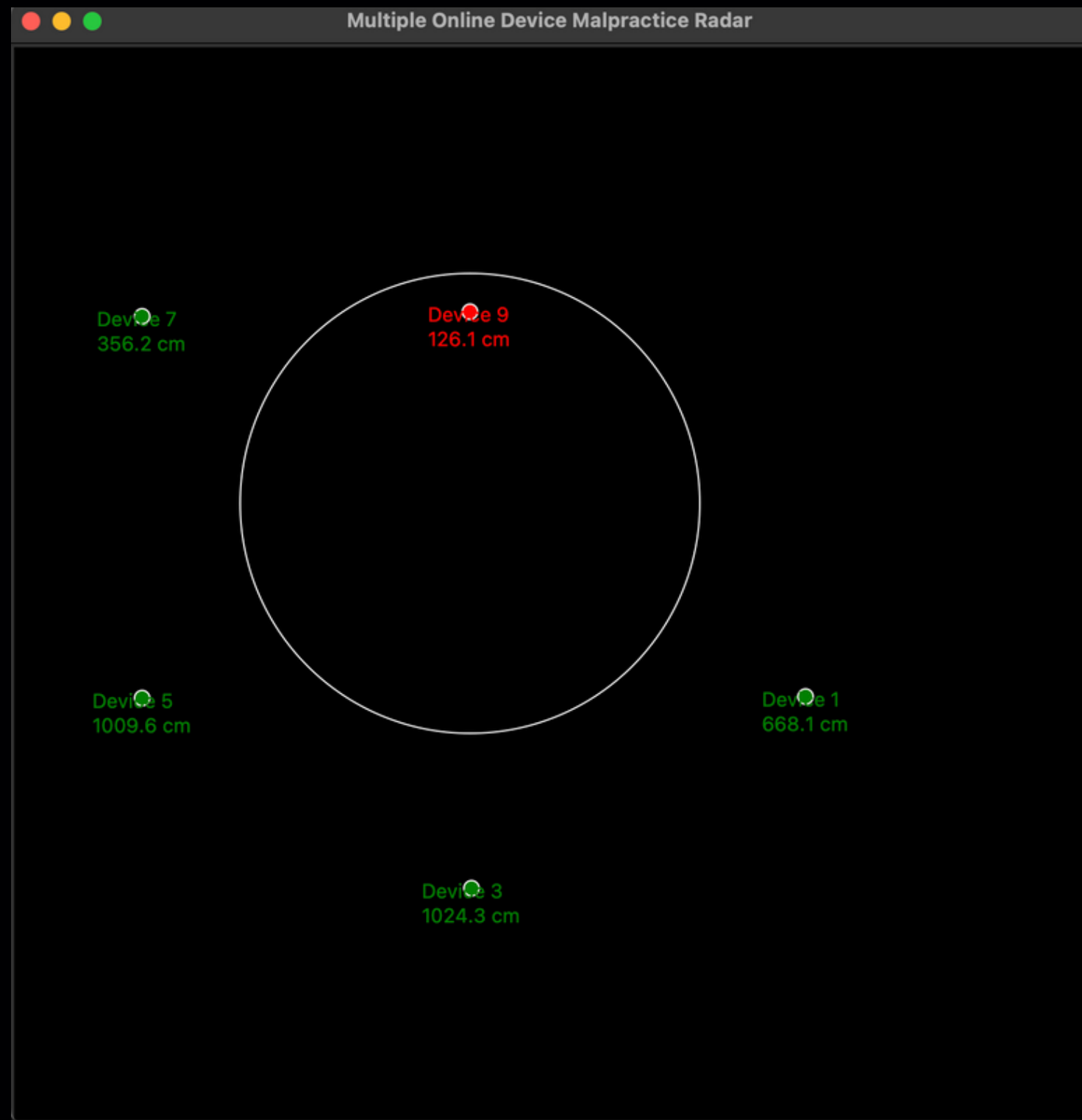
- **This is a GUI Implementation of The Radar.**

  - **We are able to see That there are 4 devices outside the range, and one device within the proximity of the Test Device**

  - **So there Are probabilities of it being a device used for malpractice.**

  - **Examiners Can Use this System to Scan Rooms Inbetween Exams , to monitor Usage of any bluetooth devices present inside the Exam Hall.**

Working:Behavior_Analysis

- **Behavior_Analysis is a Technique Used to analyse devices that have suspicious behaviour will be tagged**

- **Workflow**

SCAN--> Combined Log File --->Address Specific Log File ---> Anomaly Detection --> Suspicious Devices

behavior_data.csv

41:99:b9:cf:ff:fd_data.csv
46:b2:87:c6:f0:62_data.csv
4a:7a:50:40:27:c2_data.csv
4c:0c:a9:e8:e4:6f_data.csv
4d:34:f0:37:bf:5a_data.csv
55:98:bc:21:42:49_data.csv
56:1b:60:95:86:41_data.csv
57:d8:2c:72:77:90_data.csv

Outliers are
easier to isolate

Inliers are harder
to isolate

Isolation Tree

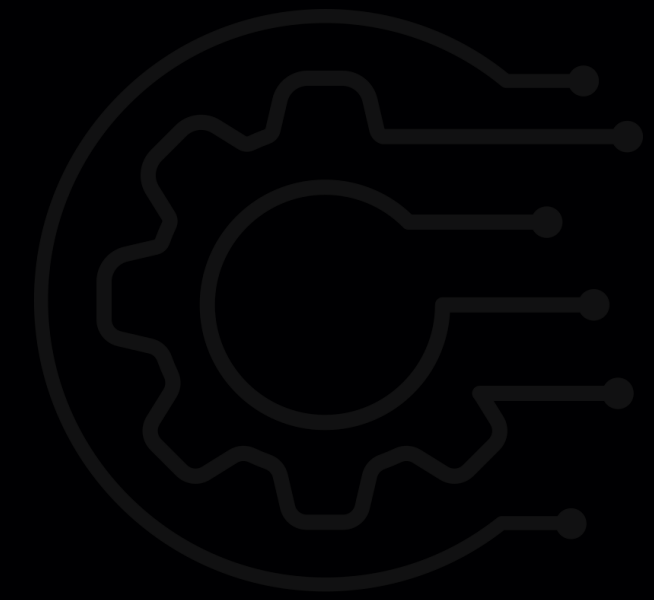Suspicious Devices:
1f:c3:4a:7e:fb:1c
36:8f:b9:1f:0f:cd

Conclusion

- **Real-time Tracking and Visualization:** Sniffer tracks and visually represents device proximity in real time, allowing prompt identification of cheating attempts during exams.

- **Proactive Cheating Detection:** Sniffer accurately estimates device distances, enabling early detection of unauthorized collaboration or additional devices during exams.

- **Enhanced Exam Security:** Sniffer provides an additional layer of security, ensuring fairness and integrity in exams by mitigating the risks associated with cheating.

- **Effortless Implementation:** Sniffer is easy to deploy and integrate into existing exam processes, leveraging widely available Bluetooth technology.

- **Addressing Online Learning Challenges:** Sniffer combats academic dishonesty by actively monitoring device proximity, discouraging copying from external sources and promoting an honest learning environment.

Thank You