SmartSeal: IoT based-Smart Anti-Tampering Solution for Secure Deliveries

---

ENSURING PACKAGE INTEGRITY AND TRANSPARENCY FROM WAREHOUSE TO DOORSTEP

Presented by:

Achyuth Mukund - 22011102005

Haneef Ahmad - 22011102019

SHIV NADAR UNIVERSITY
CHENNAI

CONTENTS

OVERVIEW

The Tamper-Proof IoT-Based Package Security System is an innovative solution designed combination of sensors and communication modules to enhance the security of e-commerce deliveries by detecting tampering attempts.

It continuously monitors package integrity, detecting any unauthorized openings or unusual movements, and sends real-time alerts to users via buzzer alerts, cloud platform or mobile app. By providing immediate notifications of potential tampering, this system helps ensure the safe delivery of packages, adding an extra layer of trust and security for online shoppers and e-commerce providers alike.

- **Objective:** Create an IoT solution to monitor and detect tampering with e-commerce packages during delivery.
- **Functionality:** Monitors package integrity in real-time by detecting unauthorized openings or unusual motion.
- **Alert System:** Sends immediate alerts to the user’s cloud platform or app if tampering occurs.
- **Connectivity:** Uses Wi-Fi to enable remote monitoring.
- **Ease of Use:** Designed for simple setup with easy-to-read alerts for package status.
- **Application:** Adds an extra security layer to online deliveries, improving customer trust and satisfaction.

PROJECT OBJECTIVES

1. Detect Unauthorized Access: Identify if the package is opened or tampered with during delivery.

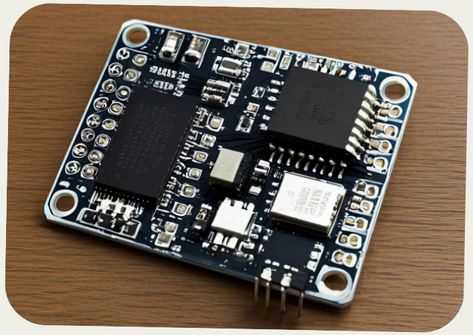
2. Real-Time Alerts: Notify the recipient and/or e-commerce provider in real time if any suspicious activity is detected.

3. Verification Before Opening: Provide a secure confirmation system so that only authorized individuals can open the package upon delivery.

CORE COMPONENTS

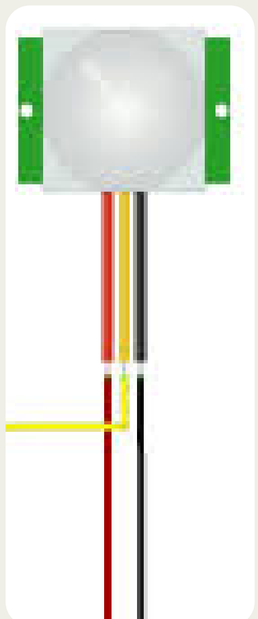
Microcontroller

NODE MCU ESP8266 or ESP32 (Wi-Fi Module), for communication and sensor control.



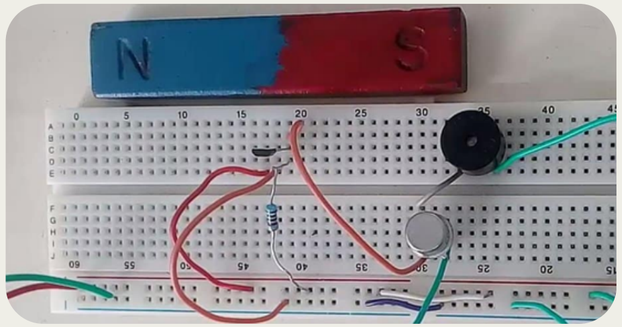
Motion Sensor

Detects any unexpected movements or impacts, which could indicate tampering.



Magnetic Sensor

Checks if the package has been opened by detecting changes in the magnetic field when the package lid or flap is moved.

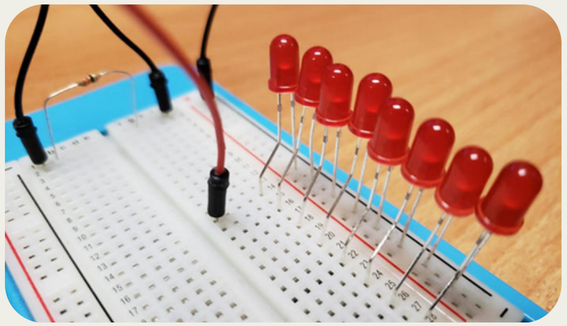


GPS Module (Optional)

Tracks the package's location throughout the delivery.

LED Indicator

Provides a visual/audible alert if tampering is detected.



Battery

Power source for the components.

HOW IT WORKS

Tamper Detection:

The magnetic sensor is placed at the opening edge of the package. If the package is opened or tampered with, the sensor registers this change.

The motion sensor detects unusual movements or impacts that might indicate rough handling or unauthorized access.

Real-Time Alerts:

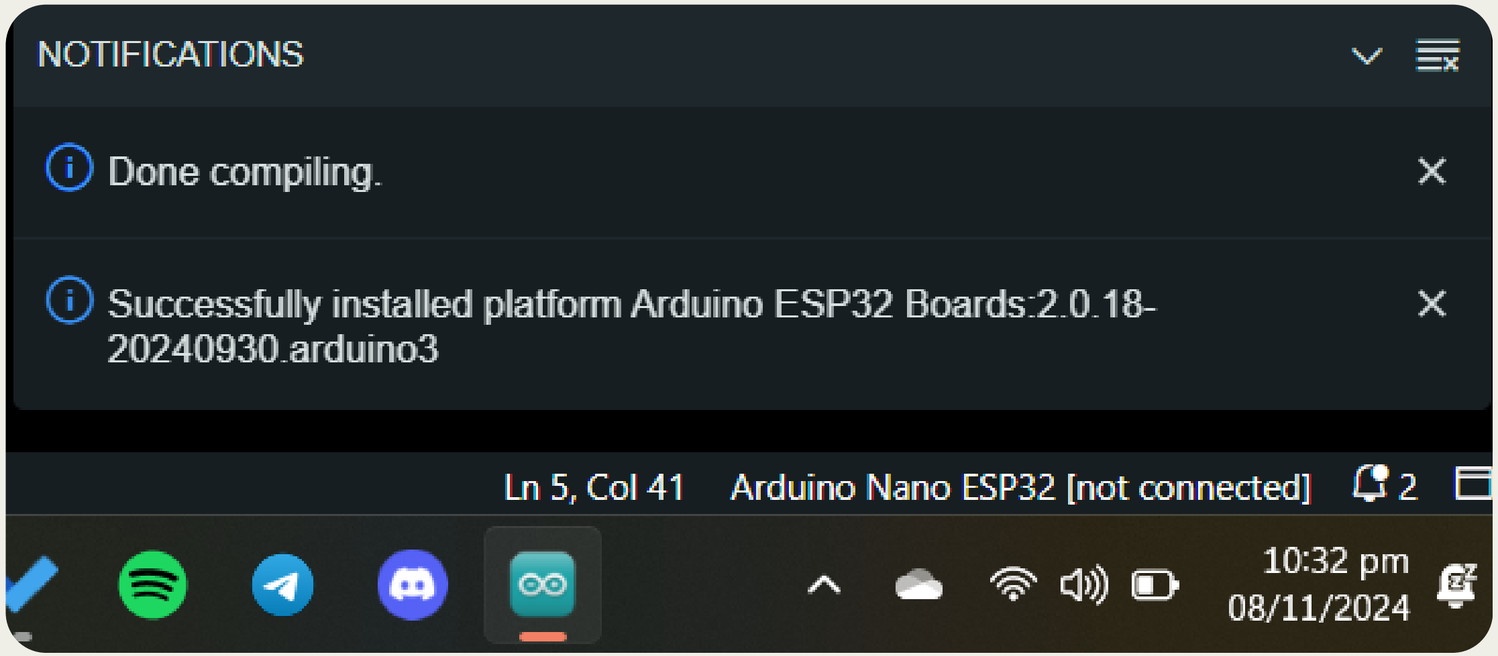
When tampering is detected, the microcontroller triggers the Wi-Fi module to send a real-time alert to a mobile app or cloud-based dashboard, notifying the e-commerce provider or the recipient about the issue.

An optional GPS module can track the package's location, allowing for easy tracing and accountability.

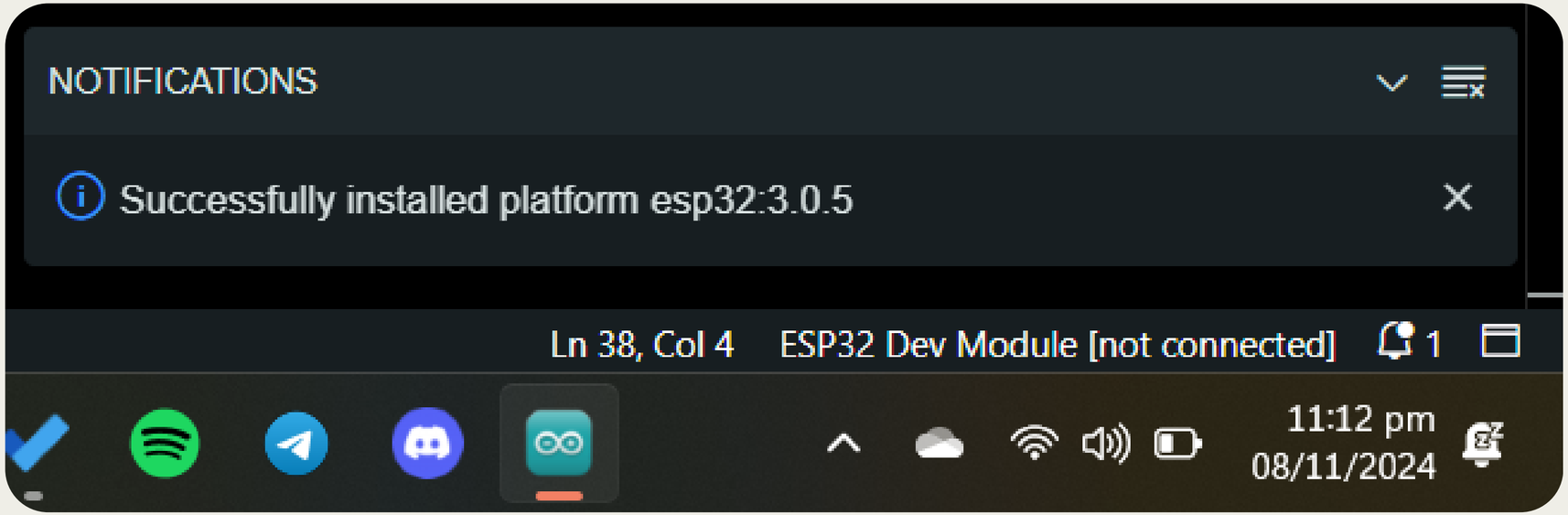
Secure Delivery Confirmation:

Once the package reaches the recipient, they can use an app-based verification system (e.g., a QR code or OTP) to confirm they are the rightful recipient before opening.

If no tampering has been detected, they are authorized to open it, logging the successful delivery.



Package Installation in Arduino IDE



PROCESS FLOW

STEP 1

At the warehouse, the package is carefully sealed, and embedded sensors (such as tamper sensors, motion sensors, or environmental sensors) are activated.

This ensures that from the moment it leaves the warehouse, any suspicious activity or damage will be detected. The package's information is then registered in the cloud or app, initiating tracking.

STEP 2

During transit, the sensors monitor the package for any abnormal events, such as unauthorized opening, rough handling, or exposure to unfavorable conditions (like high temperatures or humidity).

If any of these events occur, an instant alert is sent to the cloud/app. This alert can be reviewed in real-time by logistics managers, providing an opportunity to intervene or address issues with delivery personnel.

STEP 3

Upon arrival, the delivery personnel verifies the recipient’s identity, typically through the app, ensuring the package reaches the correct person.

Once identity verification is complete, the recipient can confirm the package’s integrity via the app and proceed to open it.

If all checks are successfully completed, the delivery is logged as secure, building a record of safe and verified delivery for both the customer and the provider.

Practical Implementation

Arduino IDE 2.3.3

Data/Power Exchange
USB to B-Type Cable

Node MCU ESP Wroom-32
(WiFi Enabled Module)

Magnetic Hall Sensor

Buzzer Module
(Low Level Trigger)

SPIoT | Arduino IDE 2.3.3

File Edit Sketch Tools Help

DOIT ESP32 DEVKIT V1

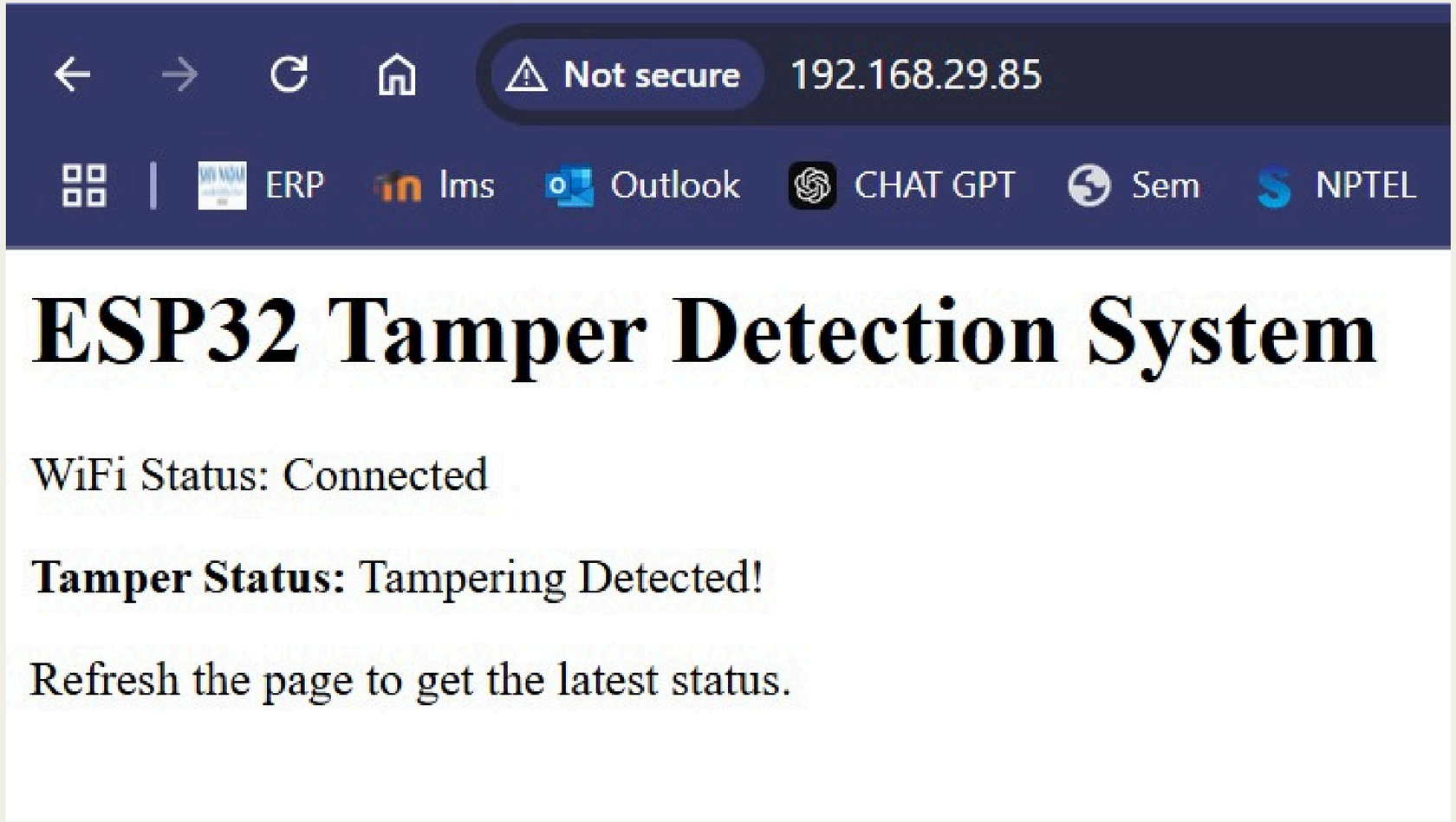
SPIoT.ino

```
#include <WiFi.h>
#include <WebServer.h>

// WiFi credentials
const char* ssid = "Achuu2308";
const char* password = "Kungfupanda2";

// Pin definitions
#define VIBRATION_PIN 27   // GPIO for Vibration sensor
#define ALERT_PIN 16       // GPIO for LED/Buzzer

// Web server on port 80
WebServer server(80);

// Variables to track tamper status
String tamperStatus = "No Tampering Detected";

// Function to send an alert to the cloud (can be customized)
void sendAlert() {
  Serial.println("Sending alert to user...");
  // Insert your alert service code here
}

// Function to handle web page requests
void handleRoot() {
  String html = "<html><head><title>ESP32 Tamper Detection</title></head><body>";
  html += "<h1>ESP32 Tamper Detection System</h1>";
  html += "<p>WiFi Status: Connected</p>";
  html += "<p><strong>Tamper Status:</strong> " + tamperStatus + "</p>";
  html += "<p>Refresh the page to get the latest status.</p>";
```

Output

```
Sketch uses 938733 bytes (71%) of program storage space. Maximum is 1310720 bytes.
Global variables use 45344 bytes (13%) of dynamic memory, leaving 282336 bytes for local variables. Maximum is 327680 bytes.
```

OUTPUT SNAPSHOT



PRACTICAL APPLICATIONS

Package Security

The system ensures that packages remain untampered with throughout delivery, giving customers peace of mind.

Accountability

It provides e-commerce providers with detailed tracking of deliveries, enhancing accountability for delivery personnel.

Enhanced Customer Trust

Transparency in the delivery process helps build trust with customers, who can feel more confident in the integrity of their shipments.

Damage Prevention

By tracking package conditions, such as handling impact or environmental exposure, the system can help identify and prevent damage, ensuring that items arrive in good condition.

FUTURE SCOPE

Integration with E-commerce Platforms:
Enable direct communication between the package and e-commerce systems.

Tamper-Evidence Tracking for High-Value Items:
Can be scaled up for expensive or sensitive goods like electronics and luxury items.

Delivery Analytics:
Collect data on delivery times, handling quality, and locations where tampering attempts occur most frequently.

WHY THIS PROJECT?

This IoT system uses simple, readily available components to address a real-world issue of package tampering.

It provides a straightforward yet effective solution that can be scaled and customized according to various e-commerce security needs.

1.

Reference	Understanding	Implementation in Project	Result
Ali, S. (2022), *IoT-Based Intelligent Systems for Package Tracking and Security*	Discusses intelligent IoT systems for secure package tracking to prevent unauthorized access during transit.	Integrated tamper detection with magnetic and vibration sensors to track and secure package status in real-time.	Achieved real-time tamper alerts to the user, ensuring package integrity.
Alkadi et al. (2021), *Enhancing IoT Network Security with Blockchain*	Explores blockchain in IoT to prevent data tampering, ensuring secure package handling records.	Not directly implemented, but concept inspired alert system that prevents tampering and logs detection for secure deliveries.	Demonstrates a system inspired by blockchain principles for secure tracking of package condition changes.
Chen, L. (2020), *Smart Package Security and Tracking Systems*	Smart tracking using sensors (GPS, vibration) for secure package monitoring and unauthorized access detection.	Combined magnetic and vibration sensors to detect any tampering attempts and alert the user instantly.	Successful tamper detection with low power consumption for prolonged usage in IoT setups.

2.

Kim, S. & Li, Y. (2020), *Intrusion Detection Systems for IoT*	Emphasizes intrusion detection in IoT, using machine learning models to identify unauthorized activity.	Implemented simple real-time alert for tamper attempts, leveraging intrusion principles for small-scale tamper detection.	Provided user notifications instantly upon detecting physical interference with packages.
Nguyen, H. (2023), *Machine Learning Approaches in Package Security*	Explores deep learning applications in tamper detection, improving security alert accuracy.	Simplified machine learning not implemented here due to complexity; inspired overall tamper detection with real-time response instead.	Focused on real-time response over complex algorithms for effective tamper detection.
Patel, R. (2022), *Secure Package Delivery Solutions in E-Commerce*	Discusses IoT applications in e-commerce to improve package security and prevent tampering.	Applied direct alert system without complex components, keeping costs low and improving accessibility of solution for e-commerce packages.	Produced a cost-effective, scalable package security system.
Rao, K. (2021), *IoT for Tamper-Resistant Package Delivery*	Highlights IoT-based tamper-resistant packaging to monitor packages through cloud alerts.	Integrated with Wi-Fi-enabled ESP32 to send tamper alerts over the internet for real-time access by users.	Enabled remote package monitoring for user peace of mind.

3.

Sun, X. (2021), *IoT-Enabled Tamper Detection for Goods in Transit*	Focuses on IoT and tamper detection for monitoring goods in transit to prevent unauthorized handling.	Used similar concept of real-time tamper detection with an alert system, without location tracking for simplicity.	Effective transit monitoring and user notification.
Li, W., et al. (2019), *Blockchain in IoT Security Systems*	Examines blockchain to secure IoT data transmission, prevent unauthorized modifications, and add reliability.	Adopted a secure alert and response system for tamper detection, although blockchain wasn't directly implemented due to project scope.	System focused on real-time notifications, ensuring timely user intervention when tampering is detected.
Xiao, Z. (2020), *Real-Time Tamper Detection Systems for IoT*	Describes real-time tamper detection systems to secure goods against unauthorized openings or rough handling.	Implemented an immediate response system using a combination of motion and magnetic sensors for direct user alerts.	Achieved high responsiveness and user engagement for tamper-proof package monitoring.

Literature Survey:

- IoT Security and Privacy: Research on IoT applications in security has grown, addressing challenges in maintaining data integrity and privacy in interconnected environments. A review discusses the use of security protocols to safeguard IoT data and prevent tampering incidents. IEEE Xplore

- Intrusion Detection in IoT Networks: A study on machine learning and blockchain in intrusion detection systems (IDS) for IoT networks demonstrates enhanced detection of security breaches, including unauthorized access and tampering attempts, highlighting the need for robust tamper detection in package delivery systems The Science and Information Organization

- Real-Time Package Tracking and Security Systems: Research has explored using IoT sensors like GPS and motion detectors to ensure the secure transport of goods, providing real-time data on package handling and location AISSMS IOIT Research

- Wireless Sensor Networks for Tamper Detection: IoT solutions using wireless sensor networks offer real-time alerts for any tampering attempts, detecting sudden movements or breaches. These systems ensure that security measures remain effective and responsive to threats. IEEE Xplore

- Advanced Machine Learning Models for Package Security: Leveraging deep learning algorithms has improved the predictive accuracy of tamper detection, enhancing security protocols and making real-time adjustments to safeguard packages from interference. The Science and Information Organization

REFERENCES

- Ali, S., “IoT-Based Intelligent Systems for Package Tracking and Security,” International Journal of IoT, 2022.
- Alkadi et al., “Enhancing IoT Network Security with Blockchain,” International Journal of Advanced Research in Computer Science, 2021, The Science and Information Organization
- Chen, L., et al., "Smart Package Security and Tracking Systems," IEEE Transactions on Consumer Electronics, 2020.
- Kim, S. & Li, Y., “Intrusion Detection Systems for IoT,” Journal of Network and Computer Applications, 2020 AISSMS IOIT Research
- Nguyen, H., et al., “Machine Learning Approaches in Package Security,” Sensors, 2023.
- Patel, R., "Secure Package Delivery Solutions in E-Commerce," International Conference on IoT Security, 2022.

- Nguyen, H., et al., “Machine Learning Approaches in Package Security,” Sensors, 2023.
- Patel, R., "Secure Package Delivery Solutions in E-Commerce," International Conference on IoT Security, 2022.
- Rao, K., "IoT for Tamper-Resistant Package Delivery," Journal of Applied IoT Research, 2021.
- Sun, X., “IoT-Enabled Tamper Detection for Goods in Transit,” IEEE Internet of Things Journal, 2021.
- Li, W., et al., "Blockchain in IoT Security Systems," Computer Communications, 2019.
- Xiao, Z., “Real-Time Tamper Detection Systems for IoT,” Internet Technology Letters, 2020 IEEE Xplore

RESULT:

The system effectively detects tampering through real-time monitoring using the ESP32, reed switch, and vibration sensor. Unauthorized openings or sudden impacts trigger instant alerts sent to users via Wi-Fi, with local LED or buzzer alerts for additional deterrence. It's energy-efficient, suitable for extended use, and adaptable to different package sizes. This initial design demonstrates a scalable and secure IoT-based solution for safeguarding e-commerce deliveries, with potential for GPS integration in future implementations.

- **Scalability and Versatility:** The successful implementation highlights the system's scalability for various e-commerce applications. By connecting multiple sensors, the system can be adapted to different types and sizes of packages, making it versatile and widely applicable.

- **Future Potential:** Given the modular nature of the design, additional components such as GPS modules can be integrated to provide location tracking. This makes the system flexible for future enhancements aimed at offering more comprehensive tracking and security options for high-value packages.

Thank you!