DESIGN OF AN ANTI THEFT SECURITY GADGET FO R MONITORING

BY

MARUF SODIQ AYOFE

ND/23/ MCT/ FT/0001

A PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF MECHATRO

NICS ENGINNERING, INSTITUTE OF TECHNOLOGY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF N ATIONAL DOIPLOMA IN MECHATRONIC ENGINEERING TECHNOLOGY ILO RIN, NIGERIA

JULY, 2025

CERTIFICATION

The undersigned certify that this project report prepared by MARUF SO DIQ AYOFE **ND/23/ MCT/ FT/0001** Entitle: **Design of an Anti-Theft Security Gadget f or Monitoring**

meets the requirement of the Department of Mechatronics Engineering for the awar d National Diploma [ND] in Mechatronics Engineering, Kwara State Polytechnic, Ilorin.

_____ _____

ENGR. RAJI Idowu Adebayo **DATE**

Project Supervisor

_____ _____

ENGR. RAJI Idowu Adebayo **DATE**

Head of Department

_____ _____

EXTERNAL EXAMINER **DATE**

Name & Signature

DECLARATION

I hereby declare that this research project title **Design of an Anti-Theft Security Gadget for Monitoring** is my work and has not been submitted by any other person for any degree or qualification at any higher institution, I also declare that the information provided therein is mine and those that are not mine are properly acknowledged.

_____ _____

Student Name **Signature and Date**

DEDICATION

I also dedicate to my Parents Mr. and Mrs. MARUF for their moral and fi nancial support towards the completion of this program, I pray may u live long to eat the fruits of your labor Inshallah.

ACKNOWLEDGEMENT

All praise and adoration belong to Almighty Allah, the most high, the ever first and infi nite last, the most supreme, the ever living and the giver of life. I thank Him for His im measurable love, care, blessings, joy, and protection on me from the beginning of my life. To Him is the glory forever.

I appreciate my supervisor ENGR. RAJI IDOWU ADEBAYO for his support and his guid ance toward this success of this project. May the peace of Almighty God be upon you and your family all the time. I also tender my sincere appreciation to the head of depa rtment (H.O.D) in person of ENGR. RAJI IDOWU ADEBAYO. God's mercy will always be with you (Amen). I must not forget all the staff and lecturers of the Mechatronic Engi neering Technology Department of Kwara State Polytechnic for their understanding a nd professional teaching in their various lectures in class. May the Almighty continue to strengthen you.

My special gratitude goes to MR. YUNUS MARUF, for his expert guidance and mentor ship throughout this project and to my lovely parents for their unwavering support an d encouragement throughout my academic pursuits.

I cannot forget my project members, for their collaboration and dedication to our shar ed objectives, am truly grateful for the collective efforts and contributions that made t his project possible. Thank you all for your support!

ABSTRACT

This project presents the design and implementation of a cost-effective, portable, an d reliable anti-theft security gadget for real-time monitoring and alerting. The system aims to address the increasing demand for accessible security solutions, particularl y in areas lacking advanced infrastructure or internet connectivity. The device integra tes a Passive Infrared (PIR) motion sensor for intrusion detection, an Arduino Uno mi crocontroller for control logic, , and a buzzer for audible deterrence. The gadget oper ates autonomously and is powered by a 9V battery, making it suitable for deploymen t in garden perimeter yard from the entrance gates. When motion is detected within t he sensor's range, the system triggers an immediate alarm and simultaneously send s an alert to the users. The entire setup is low-cost, easy to install, and does not requ ire internet access, making it ideal for rural and low-income users. Performance eval

uation showed that the system responds within specific duration programmed (i.e 1 0:00pm night-time–6:00am morning) of motion detection, operates reliably for over 5 hours on battery, and demonstrates high accuracy with minimal false alerts. The pr oject concludes that with additional features like remote control, solar charging, and GPS integration, the system can be further enhanced for broader applications. This work contributes toward improving localized security systems through the use of si mple, efficient, and affordable technologies.

TABLE OF CONTENT

LIST OF TABLES

CHAPTER ONE

1.0 Introduction

The increasing incidence of theft, burglary, and unauthorized access in homes, offices, and public institutions has led to a growing demand for more efficient and intelligent security systems. Traditional mechanical locks and basic alarm systems, while still in use, often fail to provide timely alerts or deter sophisticated intrusions (Adebayo & Yusuf, 2020). In response, there has been a shift toward automated, sensor-based anti-theft systems that leverage advancements in technologies through the use of microcontrollers, wireless communication, and the Internet of Things (IoT).

Anti-theft security gadgets typically incorporate components such as motion detectors (PIR sensors), vibration sensors, magnetic door contacts, and microcontroller-based control units. These systems are capable of detecting unusual activity and responding in real-time by triggering alarms or sending notifications to users through mobile phones or cloud platforms (Olaoye et al., 2021). The integration of GSM, Wi-Fi, and Bluetooth modules has further enhanced the functionality of these gadgets, allowing for remote access and monitoring—a key requirement in modern security applications.

According to Ahmed and Bello (2019), the application of embedded systems in security gadgets improves responsiveness and reliability, making them suitable for residential and small business use. Similarly, Adekunle et al. (2022) emphasize that low-cost microcontrollers such as Arduino and ESP32 have made it easier for students, engineers, and entrepreneurs to develop custom security solutions that are both scalable and user-friendly.

Recent studies have also explored the use of mobile applications for interfacing with security gadgets, enabling users to monitor their properties from anywhere in the world (Idowu & Eze, 2023). These developments highlight the evolving landscape of security technologies, with a focus on real-time intelligence, low power consumption, and multi-platform accessibility.

In light of these trends, this study seeks to design and implement a smart, cost-effective anti-theft security gadget for monitoring. The goal is to create a prototype system that combines hardware components (sensors, alarms, microcontrollers) and software (embedded code, alert system) to provide effective intrusion detection and user notification.

1.2.1 Aim

The aim of this study is to design an efficient, cost-effective anti-theft security gadget capable of monitoring and alerting users in real-time about unauthorized access or intrusion attempts.

1.2.2 Objectives of the Study

The specific objectives of the study are to:

1. Design a functional electronic security gadget using microcontroller technology for detecting unauthorized movement or access.

2. Integrate various sensor modules (e.g., motion, vibration, and door contact sensor

s) for effective intrusion detection.

3. Evaluate the performance of the designed gadget in terms of responsiveness, reli ability, and ease of use in a real-world environment.

4. Ensure the gadget is portable, scalable, and energy-efficient, making it suitable fo r homes, offices, and small businesses.

1.3 Justification of the Study

The increasing rate of theft, burglary, and unauthorized access to personal an d commercial property has created a critical need for more efficient and intelligent se curity systems. In many developing countries, including Nigeria, security remains a m ajor challenge due to the high cost of advanced surveillance systems, the limited rea ch of law enforcement, and the lack of affordable technological solutions for the aver age citizen. This project is therefore justified by its aim to develop a low-cost, practic al, and effective anti-theft security gadget that can serve the needs of households, s mall businesses, and institutions. For real-time monitoring of their properties from un authorized access.

1.4 Scope of the Study

This project is limited to the design and implementation of an anti-theft securit y gadget specifically intended for monitoring physical intrusions in a confined enviro nment such as garden perimeter yard from the entrance gates. The gadget is designe d to detect unauthorized movement or tampering and respond by activating an alar m. This is within a specific duration programmed (i.e 10:00pm night-time to 6:00am morning).

CHAPTER TWO

2.0 LITERATURE REVIEW

The development of anti-theft security gadgets has attracted growing interest i n recent years due to the increasing need for efficient and intelligent surveillance syst ems. Modern technologies such as microcontrollers, sensors, wireless communicatio n modules, and mobile applications are being combined to create responsive, reliable, and cost-effective security solutions.

This chapter presents already existing literature related to this study. The review has been done under the following sub heading:

Overview of Security Systems

Security systems are designed to protect assets, property, and lives from unauthorized access, theft, and other criminal activities. Over the past few decades, these systems have evolved from simple manual mechanisms to advanced electronic and automated solutions that utilize sensors, microcontrollers, and wireless communication for real-time monitoring and alerts.

Modern security systems consist of interconnected components such as sensors (motion, vibration, and magnetic contacts), control units (microcontrollers or programmable logic units), alarm systems, and communication modules that facilitate alert delivery via GSM, Wi-Fi, or Bluetooth. These technologies work together to detect intrusions and immediately notify users, thereby reducing response time and enhancing safety (Olaoye et al., 2021).

There are two main categories of security systems based on their operation:

1. **Wired Systems**: These involve physical connections between the sensors, control units, and alarms. Though often reliable, they require extensive installation and are le ss flexible.

2. **Wireless Systems**: These use RF or Wi-Fi to connect components, allowing for ea sier setup, scalability, and integration with mobile and IoT technologies (Idowu & Eze, 2023).

Additionally, systems can be:

- **Passive**, where they only alert users after detecting an intrusion.

- **Active**, where they initiate a defensive response, such as locking doors or activati ng lights (Adekunle et al., 2022).

The growing prevalence of smart security systems is driven by the affordabilit y and accessibility of microcontrollers like Arduino and ESP32, along with open-sourc e platforms. These systems support the integration of sensors, GSM modules, and mobile applications to provide remote surveillance and alerts. For instance, GSM-bas ed anti-theft systems can send SMS alerts to users in real-time, improving their situat ional awareness and response (Ahmed & Bello, 2019).

Another significant advancement is the integration of IoT into security system s. IoT-enabled devices allow for continuous data transmission and monitoring over cl oud platforms, making it possible for users to access their systems remotely via sma rtphones. This functionality has proven vital in both residential and commercial cont

exts, where 24/7 surveillance is necessary (Adebayo & Yusuf, 2020).

Security systems have become increasingly important in regions with high cri me rates, unreliable public policing, or limited infrastructure. For example, in Nigeria a nd similar developing countries, there is a growing demand for low-cost, effective sol utions that can help prevent theft and burglary in homes and businesses (Oyetunji et al., 2022).

In modern security systems are transitioning from simple alarm-based mecha nisms to smart, interconnected gadgets capable of real-time monitoring and respons e. These systems combine hardware and software innovations to provide flexible, sc alable, and effective security solutions tailored to the needs of different environment s.

2.2 Anti-Theft Technologies

Anti-theft technologies are specialized systems and devices designed to detec t, deter, and respond to unauthorized attempts to access, steal, or damage property. T hese technologies are integral to modern security systems and have become increasi ngly sophisticated with the advent of digital electronics, microcontroller-based syste ms, and wireless communication.

Anti-theft systems can be broadly categorized based on their detection mecha nisms, response capabilities, and communication methods. These technologies have found applications in homes, vehicles, retail environments, offices, and warehouses.

2.2.1 Key Anti-Theft Technologies:

Motion Detection Sensors: Passive Infrared (PIR) sensors are widely used to d etect human movement within a secured area. When a person enters the sens or's range, it triggers an alert. PIR sensors are cost-effective and energy-efficie nt (Akinlabi & Umar, 2020).

Vibration and Shock Sensors: These sensors detect physical disturbances suc h as window breaking or forced entry through doors. They are often installed o n safes, windows, or lockers and are sensitive to changes in vibration patterns (Adeyemi et al., 2021).

Magnetic Contact Sensors: Used primarily on doors and windows, these sens ors trigger an alarm when the magnetic connection is broken. They are simple and highly effective for perimeter monitoring (Eze & Salami, 2019).

RFID-Based Access Systems: Radio Frequency Identification (RFID) systems r estrict access to authorized users through electronic tags or cards. RFID is co mmonly used in vehicle theft prevention and in access-controlled buildings (C hukwuma et al., 2022).

GSM and SMS Alert Systems: One of the most widely implemented technolog ies in modern anti-theft devices, GSM modules can send SMS or call alerts to a predefined number when an intrusion is detected. This allows **for** real-time n otification and off-site monitoring, even without internet access (Olatunji & Uc

he, 2020).

IoT-Based Anti-Theft Systems: Integration of the Internet of Things (IoT) allo ws for remote access, control, and monitoring of anti-theft systems via smartp hones or web platforms. These systems often include mobile apps for arming /disarming and logging intrusion events (Adebayo & Yusuf, 2020).

Camera-Based Surveillance (CCTV): While not a direct deterrent in many low-cost systems, integration of video surveillance enhances evidence collection a nd monitoring capabilities. When combined with motion detection, cameras c an automatically record when movement is detected.

Alarms and Buzzers: Audible alarms serve as immediate deterrents to intruder s. When triggered, they can alert occupants or passersby and potentially scare off would-be thieves.

2.2.2 Applications and Advancements

Recent developments have led to multi-layered systems that combine several of the above technologies into one compact gadget. For example, an Arduino or ESP 32-based device can integrate motion sensors, GSM modules, and an RFID reader to create a smart, interactive anti-theft solution (Olaoye et al., 2021).

Moreover, advancements in low-power microcontrollers, long-range communic ation (LoRa, GSM, Wi-Fi), and mobile application development have made it possible to create highly efficient systems that are also affordable and scalable, especially im

portant for deployment in developing countries.

2.3 Related Works and Existing Systems

Over the years, several researchers and developers have contributed to the evol ution of anti-theft and security systems by integrating microcontrollers, sensors, and communication modules. This section reviews related projects and existing systems, highlighting their design approaches, functionalities, and limitations.

2.3.1 GSM-Based Intruder Alert Systems

Olaoye et al. (2021) developed a GSM-based anti-theft system for domestic us e, which employs a PIR motion sensor connected to a microcontroller. Upon detecting motion, the system triggers a buzzer and sends an SMS alert to the user's phone via a GSM module. The system demonstrated a high level of reliability in a controlled en vironment but lacked remote control capability and required manual arming/disarmin g.

Chukwuma et al. (2022) designed an RFID-enabled access control system that grants or denies entry based on a valid RFID card scan. The system, based on an Ard uino UNO, proved useful in office environments where access needed to be restricted. However, it was not equipped to handle forceful entry or tampering without RFID use.

Idowu & Eze (2023) created a smart home security system using NodeMCU an d cloud services. The system allowed users to monitor their homes remotely using a smartphone application. It combined motion detection, camera surveillance, and real

-time push notifications. While the system offered scalability and user convenience, it depended heavily on internet availability and cloud server uptime.

Adeyemi et al. (2021) proposed a system that utilized vibration sensors and PI R sensors to detect both movement and tampering. This hybrid approach increased t he detection sensitivity of break-ins and unauthorized handling of property. However, the system was found to be prone to false alarms caused by environmental vibration s (e.g., wind, nearby traffic).

Adebayo & Yusuf (2020) built a security locker system using keypad entry, ma gnetic lock, and GSM alert. When an incorrect password was entered multiple times, an SMS alert was sent to the owner, and an audible alarm was activated. Though eff ective for secure storage, the design was primarily suited for lockers and not scalable to full-room surveillance.

Beyond academic works, companies like Ring, Xiaomi, and Hikvision have rele ased advanced anti-theft systems featuring motion-detecting cameras, cloud storag e, smartphone integration, and AI-based activity recognition. However, these systems are often costly, rely on constant internet access, and require subscriptions for full fu nctionality—factors that may limit adoption in developing regions (Olatunji & Uche, 2 020).

Table 1: ***Summary of Key Features in Reviewed Systems***

Core Technologies	Alert Type	Strengths	Limitations	Alert Type

RFID, Arduino	Access Denial	Access management	No tamper detection	Access Denial
IoT, Cloud, NodeMCU	App Notification	Remote access	Internet dependent	App Notification
Vibration, PIR	Local Alarm	Multi-trigger detection	Prone to false alarms	Local Alarm

2.4 Comparative Analysis of Monitoring Gadgets

Monitoring gadgets play a vital role in security systems by enabling real-time observation, detection, and reporting of unusual activities. These gadgets include sensors, microcontroller-based systems, GPS trackers, surveillance cameras, and smart alert systems. This section presents a comparative analysis of commonly used monitoring gadgets in terms of technology, features, and effectiveness, particularly for anti-theft security applications.

PIR Motion Sensors

Technology: Detects infrared radiation emitted by warm objects (e.g., humans, animals).

Features: Low power consumption, simple interface with microcontrollers, quick response.

Effectiveness: Good for indoor use; limited in harsh outdoor environments.

Limitations: Prone to false positives from pets, heat sources, and moving curt ains.

Vibration/Shock Sensors

Technology: Detects physical disturbances or impact.

Features: Useful in safes, windows, doors.

Effectiveness: Good for detecting tampering or forced access.

Limitations: Sensitive to environmental vibrations; may need calibration.

GSM Modules (SIM800L, SIM900A)

Technology: Sends SMS/calls when triggered via microcontroller (e.g., Arduin o).

Features: Long-distance communication, works without internet.

Effectiveness: Highly effective in regions without Wi-Fi.

Limitations: Depends on GSM signal; SMS delays possible.

GPS Trackers

Technology: Provides real-time location tracking.

Features: Ideal for vehicle security and mobile asset monitoring.

Effectiveness: High; allows tracking even after theft.

Limitations: Expensive; requires GSM and sometimes subscriptions.

RFID Systems

Technology: Uses radio frequency for access control.

Features: Grant or deny access via tags/cards.

Effectiveness: Excellent for managing entry; poor for intrusion detection.

Limitations: Cannot detect unauthorized physical breaches.

IoT-Based Monitoring (NodeMCU, ESP32)

Technology: Wi-Fi-enabled boards for remote access and cloud monitoring.

Features: Supports mobile apps, automation, real-time alerts.

Effectiveness: Excellent for tech-savvy users with internet access.

Limitations: Internet-dependent; less reliable in rural areas.

CCTV/Smart Cameras

Technology: Visual monitoring, sometimes with AI recognition.

Features: Real-time video, storage, facial/object detection.

Effectiveness: Very effective; acts as deterrent and evidence collector.

Limitations: High cost, requires continuous power and storage.

The comparative analysis shows that while CCTV and IoT systems offer advanced functionalities, they are costlier and require internet infrastructure. In contrast, GSM modules, PIR sensors, and RFID systems offer cost-effective solutions suitable for low-resource environments. Choosing the right gadget depends on budget, environment, and level of monitoring required.

2.5 Theoretical Framework

The theoretical framework provides the foundational theories that guide the design and implementation of the anti-theft security gadget. It helps to justify the rationale behind the system architecture, components used, and user interaction with the device. In this study, the following theories are applied:

1. Routine Activity Theory (RAT)

This theory states that the likelihood of a crime occurring increases when thre e elements converge: a motivated offender, a suitable target, and the absence of a ca pable guardian.

A p p l i c a t i o n

The anti-theft security gadget serves as a capable guardian by providing real-time m onitoring and alerts, thereby reducing the opportunity for crime. Its presence alone m ay deter offenders.

2. Crime Prevention Through Environmental Design (CPTED)

CPTED suggests that the built environment can be structured in a way that reduces cr iminal behavior. It emphasizes natural surveillance, territorial reinforcement, and acce ss control.

A p p l i c a t i o n :

The gadget uses visible sensors, audible alarms, and proactive notification systems t o enhance perceived surveillance, which deters unauthorized access and theft.

3. General Systems Theory

This theory explains how complex systems can be understood as a whole made of in terrelated parts that work together to achieve a goal.

A p p l i c a t i o n :

The gadget functions as a system, where components such as sensors, microcontrollers, and communication modules interact in a coordinated way to detect threats and alert users effectively.

4. Technology Acceptance Model (TAM)

TAM explains how users come to accept and use a technology based on two key factors: perceived usefulness and perceived ease of use.

Application:
The gadget is designed to be affordable, user-friendly, and reliable to ensure widespread acceptance and usage, especially in low-tech or residential environments.

5. Signal Detection Theory (SDT)

Overview: This theory, from the field of psychophysics, focuses on the ability to discern between information-bearing patterns (signal) and random patterns (noise).

Application:
In the context of the anti-theft system, SDT helps in calibrating the sensors to reduce false alarms while maintaining high sensitivity to actual intrusion signals.

Table 2: Theoretical Applications

Theory	Focus Area	Relevance to the Study

Routine Activity Theory	Crime causation and deterrence	Justifies the gadget as a preventive guardian against intrusion
CPTED	Environmental design	Guides physical design and placement for deterrence
General Systems Theory	System interaction	Supports modular integration of gadget components
Technology Acceptance Model	User behavior and design	Ensures usability and accessibility for end-users
Signal Detection Theory	Detection accuracy	Improves reliability of alert and sensor systems

The integration of these theories provides a multidisciplinary foundation for the research, supporting both the technical design and the social relevance of the anti-theft security gadget. It ensures that the project addresses real-world problems effectively, both functionally and behaviorally.

CHAPTER THREE

SYSTEM DESIGN AND METHODOLOGY

3.1 Design Requirements and Specifications

The design of the anti-theft security gadget is driven by the need to create a co mpact, efficient, and reliable system capable of detecting unauthorized access or the ft attempts and promptly notifying the user. The system integrates mechanical, electr onic, and software components in a typical framework. Below are the detailed design requirements and specifications.

3.1.1 Functional Requirements

Motion Detection: The gadget must detect motion within a specified range us ing sensors such as PIR (Passive Infrared) or ultrasonic sensors.

Intrusion Detection: The system must identify unauthorized access or tampering thr ough vibration or door contact sensors.

Real-Time Monitoring: The device must support real-time monitoring for imme diate notification acquisition through a user interface.

Alert System: Upon detecting an intrusion, the system should send instant aler ts via second alarm.

Power Supply: The system should operate on a rechargeable battery with sola

r charging options and include a power-saving mode.

Sound Alarm: A loud buzzer or siren must be activated during intrusion events to deter theft attempts.

3.1.2 Non-Functional Requirements

Portability: The device must be compact, lightweight, and easy to install on va rious objects or locations on the fence/a mounted pole.

Durability: The housing should be resistant to environmental conditions like d ust, moisture, and temperature fluctuations.

Low Power Consumption: Energy efficiency is crucial to ensure long-term oper ation on battery power.

User-Friendly Interface: The control and monitoring interface should be intuiti ve for end-users, whether it is a mobile app, LCD screen, or web interface.

Cost-Effective: The components should be affordable to ensure mass product ion and scalability for consumer markets.

3.1.3 System Specifications

Table 3: Showing the component parts of the system

Parameter	Specification
Power Supply	5V–12V DC, rechargeable Li-ion battery supported

Motion Sensor	PIR Sensor, Range: 5–7 meters
Vibration Sensor	Piezoelectric or SW-420 vibration module
Microcontroller	Arduino Uno / ESP32 / Raspberry Pi (as applicable)
Communication Module	GSM Module (SIM800L) or Wi-Fi (ESP8266/ESP32)
Alert Mode	SMS, Call, App Notification, Buzzer
SUser Interface	Mobile App / Web Interface / LCD (16x2)
Alarm Sound Output	≥ 85 dB Buzzer/Siren
Enclosure Material	ABS Plastic or Aluminum Casing
Operating Temperature Rang e	-10°C to 50°C
System Response Time	≤ 1 second

3.1.4 Compliance and Safety

EMC Compliance: Ensure electromagnetic compatibility to avoid interference with nearby devices.

Electrical Safety: Protect circuits with fuses and ensure insulation of high-curr ent paths.

User Safety: No exposed conductive parts or sharp edges; warning labels for b attery charging.