

**KWARA STATE UNIVERSITY, MALETE**

**THE GREEN UNIVERSITY FOR COMMUNITY DEVELOPMENT**

# FACULTY OF ENGINEERING AND TECHNOLOGY

**IMPROVEMENT ON THE DESIGN & CONSTRUCTION OF AN IOT-BASED DISTRIBUTION TRANSFORMER ANTI-VANDALISM MONITORING AND CONTROL SYSTEM**

Submitted by

**OLUWADAMISI VICTOR SEUN  
19/67EC/00922**

Submitted to

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

In partial fulfillment for the Award of Bachelor of Engineering Degree in Electrical and Computer Engineering.

**January 2024**



**IMPROVEMENT ON THE DESIGN & CONSTRUCTION OF AN IOT-BASED DISTRIBUTION TRANSFORMER ANTI-VANDALISM MONITORING AND CONTROL SYSTEM**

**(A Case Study of KWASU Library 500KVA Transformer)**

**BY**

**OLUWADAMISI VICTOR SEUN**

**19/67EC/00922**

**A CONSTRUCTION PROJECT SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING, KWARA STATE UNIVERSITY, MALETE, IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF ENGINEERING (B.NG) DEGREE IN ELECTRICAL AND COMPUTER ENGINEERING.**

**SUPERVISED BY DR. LAMBE M. ADESINA**

**JANUARY, 2024**

# DECLARATION

I hereby declare that this project titled **“Improvement on the design & construction of an IOT-based distribution transformer anti-vandalism monitoring and control system”** is my own work and I am making further improvements from the work of the previous graduated set in the higher institution. I also declare that the information provided are mine and those that are not mine are well acknowledge.

Oluwadamisi Victor Seun

Name of Student Signature and Date

# CERTIFICATION

This is to certify that this project titled **“IMPROVEMENT ON THE DESIGN & CONSTRUCTION OF AN IOT-BASED DISTRIBUTION TRANSFORMER ANTI-VANDALISM MONITORING AND CONTROL SYSTEM”** was carried out by **“Oluwadamisi Victor Seun”.** This project has been read and approved as meeting the requirements for the award of the Bachelor of Engineering degree (B.Eng) in Electrical and Computer Engineering, Faculty of Engineering and Technology, Kwara State University, Malete.

**………………………. ……………………**

**Engr. DR. Lambe. M ADESINA Date**

**( Project supervisor)**

**………………………. ……………………**

**Engr. DR. Abdulwaheed Musa Date**

**(Head of Department)**

**………………. …………………….**

**External Examiner Date**

# DEDICATION

This work is dedicated to God Almighty who made this possible. Also, to my Parents Mr. and Mrs. Oluwadamisi for making this achievable with your love and full support.

# ACKNOWLEDGEMENTS

My appreciation goes to God almighty for choosing Electrical and Electronics Engineering as my discipline and also for guiding me throughout this project work.

Actually, there are so many people to appreciate. However, I sincerely express my deep sense of gratitude to my respected supervisor Engr. Dr. Lambe M. Adesina for his valuable guidance, profound advice, persistent encouragement and help during the completion of this work. His time-to-time helpful suggestions boosted us to complete this task successfully. He has helped me in all possible ways right from gathering the materials to report preparation.

To my Institution, Kwara State University, the Faculty of Engineering and to all the academic and non-academic staff of the Department of Electrical and Electronics Engineering. Most especially Engr. Dr. Abdulwaheed Musa, Engr. Dr. Balogun Monsurat, Engr. Dr. Olalekan Olabiyi, Tgst. M. Abolaji. I say thank you all. I am sincerely grateful.

I would also like to acknowledge my entire family, for their support all through this project.

Also, thanks to my friends who support, encourage, motivate and advise me throughout the project.

**TABLE OF CONTENTS**

[**ABSTRACT** i](#_Toc95337743)

[**CHAPTER ONE** 1](#_Toc95337744)

[**1.1 Background of the study** 1](#_Toc95337745)

[**1.2 Motivation** 2](#_Toc95337746)

[**1.3 Problem statement** 3](#_Toc95337747)

[**1.4 AIM and objective** 3](#_Toc95337748)

[**1.4.1 AIM** 3](#_Toc95337748)

[**1.4.2 Objectives** 3](#_Toc95337748)

[**1.5 Scope of the project** 4](#_Toc95337749)

[**1.6 Significance** 5](#_Toc95337749)

[**1.7 Outline** 6](#_Toc95337749)

[**CHAPTER TWO** 7](#_Toc95337750)

[**2.1 Vandalism of distribution transformer** 8](#_Toc95337751)

[**2.2 What to know about IoT** 9](#_Toc95337752)

[**2.3 Sensors** 1](#_Toc95337752)0

[**2.3.1 Types of Sensors** 1](#_Toc95337752)0

[**2.3.2 Determining a Good Sensors** 1](#_Toc95337752)0

[**2.4 Alarm Systems** 1](#_Toc95337752)1

[**2.4.1 Introduction to Alarm Systems** 1](#_Toc95337752)1

[**2.4.2 Components of an Alarm Systems** 1](#_Toc95337752)1

[**2.4.3 Key Features and Functionality of an Alarm Systems** 1](#_Toc95337752)1

[**2.4.4 Types of Alarm Systems** 1](#_Toc95337752)1

[**2.5 Micro-controller** 1](#_Toc95337751)2

[**2.5.1 Components of a Micro-controller** 1](#_Toc95337752)2

[**2.5.2 Key Characteristics of a Micro-controller** 1](#_Toc95337745)2

[**2.5.3 Applications of a Micro-controller** 1](#_Toc95337746)2

[**2.5.4 Types of Micro-controller** 1](#_Toc95337747)2

[**2.5.5 Features of a Micro-controller** 1](#_Toc95337748)2

[**2.6 Review of related works** 1](#_Toc95337749)3

**LIST OF FIGURES**

[**Figure: 3-1: ESP32-PIN OUT** 14](#_Toc95337751)

[**Figure: 3-2 GSM module** 15](#_Toc95337752)

[**Figure: 3-3 Microwave sensor** 1](#_Toc95337752)6

[**Figure: 3-4 ATMEGA328P** 1](#_Toc95337752)7

[**Figure: 3-5 Arduino software**  1](#_Toc95337752)8

[**Figure: 3-6 System block diagram**  1](#_Toc95337752)9

[**Figure: 3-7 System flowchart** 20](#_Toc95337752)

[**Figure: 3-8 System circuit diagram** 21](#_Toc95337752)

# ABSTRACT

Electricity holds a vital role in our daily routines. A crucial component in the transmission and distribution of electric power is the transformer. Given the widespread deployment of transformers in current electric systems, there is a notable increase in complaints about vandalism directed towards these devices. This growing trend of transformer vandalism not only imposes a substantial financial burden on electricity distribution companies but also necessitates frequent replacements of stolen components. The ensuing power failures cause considerable inconvenience to consumers. Recognizing the escalating need for global transformer protection, an innovative system is currently under development.

This forward-thinking system integrates several advanced technologies, including a micro-controller, a sophisticated camera, a microwave sensor for motion detection, an RF module for transmitting radio signals to the nearest security post, and a GSM module for identifying potential vandals. This comprehensive solution places emphasis on factors such as cost-effectiveness and mobility, aiming to provide an efficient shield against acts of vandalism. The goal is to safeguard transformers effectively, contributing to the resilience and integrity of the global electrical grid.

**CHAPTER ONE: INTRODUCTION**

* 1. **Background of Studies**

Throughout the nation, the power generation, transmission, and distribution sectors experience various types of losses, including technical, non-technical, and commercial. These losses inflict significant damage on the country’s economy and lead to a decline in the quality of power supplied to consumers. Distribution transformers, serving as the primary access point for electricity consumers, are particularly vulnerable to vandalism. The surge in demand for copper and transformer oil on the black market has substantially escalated the incidence of vandalism.

According to a recent update from the Eket/Port Harcourt Electricity Distribution Company, 11 transformers were damaged in various locations within the local government area of the state between July and the present. Despite extensive awareness campaigns and customers interactions, the report highlights that vandals continue to undermine electrical installations in the region.

The destruction incurred by these acts of vandalism results in financial losses for both consumers and distribution company. The expense of installing new components after each vandalism incident adds to the financial burden. Consumers also face security concerns as the frequent attacks lead to power outages in affected areas. Additionally, the vandals themselves are at the risk of electrocution, risking their lives in the process.

**1.2 Motivation**

The issue of vandalism targeting distribution transformers is a grave concern, causing substantial financial losses for power utilities and posing a safety risk to the public. The objective of this project is to develop and implement a robust anti-vandalism system, with the aim of thwarting unauthorized access to distribution transformers and mitigating the occurrence of vandalism.

**1.3 Problem Statement**

Vandalism of distribution transformers in Nigeria manifests in various forms, each exacerbating the challenges faced by the power distribution system. One prevalent issue is the theft of valuable components, such as copper coils and other metallic elements. This not only leads to operational disruptions but also results in substantial financial burdens for utility companies tasked with replacing and repairing the damaged transformers.

Additionally, wanton destruction and sabotage of distribution transformers contribute to the depletion of critical infrastructure. Vandals often target these transformers for various reasons, including the illegal extraction of oil, which further compromises the operational integrity of the transformers. The susceptibility of transformers to these

**1.4 Aim and Objectives**acts of vandalism raises concerns about the resilience of the power distribution network in Nigeria.

The impact of vandalism on power distribution in Nigeria is multifaceted, affecting different aspects of the electrical grid. Vandalized transformers lead to prolonged downtimes as utility companies grapple with the intricate process of repairs and replacements. The extended periods of inactivity contribute to frequent power outages, disrupting the daily lives of citizens and hampering industrial activities.

The financial ramifications of transformer vandalism are substantial. The costs associated with repairing or replacing damaged transformers, coupled with the expenses related to investigating and addressing security vulnerabilities, strain the already limited resources of utility companies. These financial losses have a ripple effect on the affordability and accessibility of electricity for consumers.

Vandalism introduces safety hazards into the power distribution landscape. Tampering with transformers can result in oil spills, fires, and electrocution risks. Such incidents not only endanger the lives of those involved in the vandalism but also pose threats to the broader community.

In conclusion, the pervasive vandalism of distribution transformers in Nigeria poses a severe threat to the efficiency and reliability of the power distribution infrastructure. Addressing this issue requires a comprehensive approach, including the development and implementation of advanced monitoring and control systems, as well as heightened security measures to deter potential vandals. Only through concerted efforts can Nigeria mitigate the negative impacts of vandalism and ensure the uninterrupted flow of electricity to its citizens.

**1.4.1 Aim**

The aim of this project is to further improve on the design and construction of a distribution transformer substation anti vandalism system and control. Using KWASU 500kva library transformer as a case study.

**1.4.2 Objectives**

The objective of the project includes:

1. To design the system to be scalable, allowing seamless integration with existing distribution infrastructure and enabling extension to cover a larger network of transformers as needed.

2. To incorporate diverse sensors and security devices into the system for detecting unauthorized access, triggering alarms, or sending notifications.

3. To evaluate the environmental sustainability of the anti-vandalism system and incorporate eco-friendly features into the design where applicable.

4. To build an anti-vandalism system and perform thorough testing and validation to guarantee its functionality and performance across diverse conditions and provide comprehensive guidelines for deploying and maintaining the system within the power industry.

**1.5 Scope of the project**

The project's scope revolves around enhancing the monitoring and control of distribution transformers by implementing an IoT-based system, with a specific emphasis on anti-vandalism measures. The key objective is to develop a system incorporating Internet of Things (IoT) technology for real-time monitoring of distribution transformers, achieved through the deployment of sensors and communication modules dedicated to data collection.

In addition to real-time monitoring, the project involves the implementation of anti-vandalism features. This includes the integration of intrusion detection sensors and security mechanisms designed to discourage and identify unauthorized access or tampering with distribution transformers. The project further facilitates swift responses to incidents by enabling remote control capabilities. This may entail designing a control interface that empowers operators to take necessary actions remotely, thereby enhancing the overall responsiveness of the system.

The project's subsequent focus is directed towards elevating the overall efficiency of distribution transformers by harnessing IoT data for predictive maintenance. This entails the analysis of performance data to proactively identify potential issues before they escalate. The system is designed to be scalable, allowing for seamless integration with existing distribution infrastructure. This design approach ensures that the solution can be easily extended to cover a larger network of transformers as necessary.

**1.6 Significance**

The project plays a pivotal role in enhancing safety by effectively addressing potential hazards associated with vandalism. The reduction in incidents of transformer tampering not only minimizes the risks of oil spills, fires, and electrocution but also bolsters the safety of both the infrastructure and the community it serves. Furthermore,

the project aligns seamlessly with the overarching objective of embracing technological advancements in the power sector. The incorporation of IoT technology not only showcases innovation but also underscores a commitment to modernizing infrastructure for improved service delivery.

The implementation of anti-vandalism measures goes beyond safety to significantly contribute to the security of distribution transformers. By acting as a deterrent to vandalism and facilitating swift responses to incidents, the project aims to safeguard

critical infrastructure against unauthorized access and tampering. The real-time monitoring capabilities of the IoT-based system play a crucial role in promptly identifying potential issues, enabling proactive maintenance. Consequently, this proactive approach reduces downtime by addressing problems before they escalate into transformer failures.

In essence, the ultimate goal is to contribute to the establishment of a more reliable power distribution network. The secure and efficiently monitored system ensures the consistent delivery of electricity to end-users, providing support to both residential and industrial consumers.

**1.7 Outline**

Chapter Two delves into the literature review, comparing prior works and conducting a comprehensive review. In Chapter Three, the focus shifts to the project's design, encompassing the system's flow description, process explanation, and system setup. This section incorporates a system block diagram, schematic diagram, as well as design specifications, requirements, and the methodology of system design.

Moving forward to Chapter Four, the discussion centers on the implementation and testing phases, featuring figures that elucidate and illustrate the system's functionality. Lastly, Chapter Five encapsulates the project's conclusion and suggests potential enhancements for future iterations.

**CHAPTER TWO: LITERATURE REVIEW**

**2.1 Vandalism of distribution transformer**

Vandalism of distribution transformers encompasses a range of destructive activities, including unauthorized access, tampering, theft of valuable components, and deliberate damage. Incidents of vandalism can lead to oil spills, fires, and electrical malfunctions, posing risks to both the infrastructure and the surrounding community.

Distribution transformer vandalism has far-reaching consequences, significantly impacting the power infrastructure. Acts of vandalism pose threats to the safety of nearby communities and the integrity of critical infrastructure. Furthermore, they can result in service disruptions, affecting businesses, residences, and essential facilities that rely on a continuous and reliable power supply. Financially, the repair and replacement costs associated with vandalized transformers place a substantial burden on utility companies, contributing to increased operational expenses. The cumulative effect of these impacts underscores the urgent need for comprehensive measures to address and prevent distribution transformer vandalism, ensuring the resilience and functionality of the power distribution network.

Distribution transformer vandalism poses a multifaceted challenge, impacting the safety, reliability, and financial stability of power distribution networks. Proactive measures, including the implementation of advanced monitoring systems and community engagement, are essential to mitigate these risks and ensure the continued reliability of the power infrastructure. Through a concerted effort from stakeholders, it is possible to reduce the incidence of vandalism and safeguard the integrity of the distribution transformer network. This review of literature centers on the current understanding of the design and development of anti-theft mechanisms intended for distribution transformers.

**2.2 What to know about IoT**

The Internet of Things (IoT) refers to a network of interconnected devices that communicate and exchange data with each other through the internet. These devices, often embedded with sensors, actuators, and communication hardware, can collect and share information, enabling them to interact with the environment and other connected devices.

The Internet of Things (IoT) is a paradigm that involves the interconnection of devices through the internet, enabling them to communicate and share data. In IoT, devices are equipped with sensors and actuators to collect and respond to information from the physical world. These devices can be connected wirelessly or through wired networks, using communication protocols like Wi-Fi, Bluetooth, Zigbee, or cellular networks.

The collected data from IoT devices is processed either locally on the device or transmitted to cloud-based servers for analysis. Data processing may involve advanced analytics, machine learning, and artificial intelligence to extract meaningful insights.

Interoperability is a fundamental characteristic of IoT, promoting seamless communication and collaboration between devices. Common communication protocols, such as MQTT and CoAP, facilitate interaction among diverse IoT devices.

Security is a critical concern in IoT implementations. To safeguard data and devices, security measures like encryption, authentication, and secure communication protocols are employed to protect against cyber threats and unauthorized access.

IoT finds applications across a wide range of industries. Examples include smart homes, industrial IoT for optimizing manufacturing processes, healthcare for remote patient monitoring, agriculture through precision farming, and smart cities with applications like traffic and waste management.

Edge computing is a concept in IoT where data is processed locally at the edge of the network, reducing latency and minimizing the reliance on centralized servers.

Scalability is inherent in IoT systems, allowing for the easy addition of new devices to expand the network. This scalability is crucial for accommodating the increasing number of connected devices in various applications.

While IoT offers numerous benefits, it also faces challenges such as privacy concerns, security vulnerabilities, interoperability issues, and the need for standardized protocols. Addressing these challenges is essential for ensuring the widespread and secure adoption of IoT technologies. The ongoing evolution of IoT continues to influence and drive innovation in various aspects of technology and daily life.

It's crucial to emphasize that an individual device does not constitute an entire IoT system. Instead, the IoT ecosystem comprises a multitude of interconnected devices collaborating and functioning collectively.

**2.3 SENSORS**

Sensors are devices that convert physical quantities or environmental conditions into electrical signals or digital data that can be interpreted, displayed, or processed. They play a fundamental role in various applications, from industrial automation to consumer electronics, by providing crucial input for decision-making and control processes.

In the course of our daily lives, we frequently come across an array of sensor types, whether within our households, workplaces, or vehicles. These sensors play a crucial role in simplifying and enhancing our day-to-day activities through the facilitation of automation.

Serving as a vital link between the physical and logical realms, sensors hold particular significance in the realm of the Internet of Things (IoT). Their key function lies in enabling the collection and processing of data, contributing to more effective monitoring, management, and control of various systems.

Fundamentally, a sensor's primary objective is to identify shifts in the measured quantity and convey these alterations through its output. The categorization of sensors is contingent upon the specific type of energy they detect and the methodology employed to convert this energy into another form.

**2.3.1 Types of Sensors**

Here is a list of various sensor types frequently employed across diverse applications. These sensors serve the purpose of measuring physical attributes, including but not limited to temperature, resistance, capacitance, conductivity, heat transfer, and more.

1. **Gas Sensors:** This sensor detects the concentration of gases in the air. Carbon monoxide detectors and air quality monitors are examples. The carbon monoxide detectors specifically senses carbon monoxide levels. While the air quality monitors detects various gases for assessing overall air quality. Gas and smoke sensors are crucial components in ensuring safety. Smoke detectors, commonly found in workplaces and businesses, identify smoke resulting from fires and trigger alarms.

Gas sensors, utilized in industries, kitchens, and laboratories, have the capability to detect a range of gases like methane, propane, butane, and LPG. Smoke sensors, often equipped to identify both smoke and gas, are frequently installed in homes for enhanced safety. Affordable sensors, exemplified by those in the "MQ" series, possess the ability to detect various gases such as CO, CO2, CH4, alcohol, propane, butane, LPG, and others.

1. **Temperature Sensors:** This sensor measures the temperature of the environment or an object. Examples include thermocouples, thermistors, and infrared sensors.

- Thermocouples: Utilizes the Seebeck effect, where temperature differences between two different metals generate a voltage.

- Thermistors: Relies on the varying resistance of semiconductor materials with temperature changes.

- Infrared Sensors: Detects temperature by measuring the infrared radiation emitted by an object.

Temperature sensors are crucial components widely used in various applications such as computers, mobile phones, cars, air conditioning systems, and factories. They measure temperature changes by sensing variations in temperature. There are several types of temperature sensors, including Thermistors, Thermocouples, RTDs (Resistive Temperature Devices), and Temperature Sensor ICs like LM35 and DS18B20. Analog temperature sensors, such as the LM35, change physical properties like resistance or voltage in response to temperature variations, producing analog output. Digital temperature sensors, exemplified by the DS18B20, provide discrete digital values after converting analog data.

1. **Radiation Detector (IR Sensor):** Infrared sensors, or IR sensors, play a vital role in numerous applications, including proximity and object detection in mobile phones. They come in two main types: Transmissive and Reflective. The Transmissive Type consists of an IR Transmitter (usually an IR LED) and an IR Detector (typically a Photo Diode) positioned opposite to each other. When an object passes between them, the sensor detects it. Reflective Type IR Sensors have the transmitter and detector adjacent to each other, facing the object. These sensors find applications in mobile phones, robots, industrial assembly, automobiles, and more.
2. **Motion Sensors:** Detects movement or acceleration. Examples include accelerometers and gyroscopes commonly found in smartphones and gaming devices.

- Accelerometers: Measure changes in velocity and acceleration.

- Gyroscopes: Sense rotational motion and changes in orientation.

1. **Light Sensors:** Measures the intensity of light in the environment. Photodiodes, phototransistors, and light-dependent resistors (LDRs) are common types. Light sensors, including the Light Dependent Resistor (LDR), are essential components. LDRs exhibit a characteristic where resistance varies inversely with ambient light intensity. As light intensity increases, resistance decreases, and vice versa. Light sensors are crucial in various applications and industries.

- Photodiodes: Generate a current proportional to incident light intensity.

- Phototransistors: Amplify current in response to light.

- Light-Dependent Resistors (LDRs): Change resistance based on light intensity.

1. **Radar sensor:** A radar sensor is a technology that uses radio waves to detect the presence, location, distance, and movement of objects in its vicinity. The term "radar" stands for "Radio Detection and Ranging." Radar sensors emit radio waves, and when these waves encounter an object, they reflect back to the sensor. By analyzing the reflected signals, the radar sensor can determine the object's properties, such as its distance, speed, and sometimes even its direction.

Key features and aspects of radar sensors include:

1. Operating Principle: Radar sensors operate on the principle of sending out electromagnetic waves (commonly radio waves) and detecting their reflections from objects in the sensor's field of view.
2. Transmitter and Receiver: A radar sensor typically consists of a transmitter that emits radio waves and a receiver that captures the reflected signals.
3. Frequency Bands: Radar sensors operate in various frequency bands, including microwave and millimeter-wave bands. The choice of frequency depends on the specific application requirements.
4. Applications: Radar sensors find applications in diverse fields, including automotive systems (for collision avoidance and adaptive cruise control), industrial automation, surveillance and security, weather monitoring, and aerospace.
5. Types of Radar Sensors: - Continuous Wave (CW) Radar: Emits a continuous signal and relies on frequency changes in the reflected signal.

- Pulse Radar: Sends out short pulses of radio waves and analyzes the time delay between transmitted and received signals.

- Frequency-Modulated Continuous Wave (FMCW) Radar: Utilizes a continuous signal with a frequency that changes over time, providing accurate distance and speed measurements.

1. Range Resolution: Radar sensors can provide range resolution, allowing them to distinguish between objects at different distances.
2. Doppler Effect: Radar sensors often use the Doppler effect to detect the speed of moving objects. The frequency shift in the reflected signal helps determine the object's velocity.
3. Advantages: Radar sensors are effective in various environmental conditions, including darkness, fog, and precipitation, making them suitable for applications where other sensors might struggle.
4. Challenges: Radar sensors can face challenges related to interference, accuracy at short distances, and the potential for signal reflections from nearby objects.

Radar sensors play a crucial role in modern technology, particularly in applications that require accurate detection and tracking of objects, such as in autonomous vehicles, weather monitoring systems, and industrial automation.

Numerous other sensors include Proximity Sensors, Accelerometers, Pressure Sensors, Ultrasonic Sensors, Touch Sensors, Color Sensors, Humidity Sensors, Position Sensors, Magnetic Sensors (Hall Effect Sensors), Microphones (Sound Sensors), Tilt Sensors, Flow and Level Sensors, PIR Sensors, Strain and Weight Sensors, and more. Each type serves specific purposes in diverse applications.

**2.3.2 Determining a Good Sensor**

**1. Accuracy:** A good sensor provides accurate and reliable measurements within specified tolerances.

**2. Sensitivity:** The sensor's ability to detect small changes in the measured quantity. Higher sensitivity is often desirable.

**3. Resolution:** The smallest change in the input quantity that the sensor can detect. Higher resolution allows for more detailed measurements.

**4. Range:** The range of values over which the sensor can accurately measure. A good sensor should cover the required measurement range.

**5. Response Time:** The time it takes for the sensor to respond to a change in the measured quantity. Faster response times are beneficial in dynamic applications.

**6. Stability:** The sensor's ability to maintain its calibration and performance over time.

**7. Calibration:** A good sensor is calibrated to provide accurate measurements, and calibration should be maintained regularly.

**8. Durability:** Sensors should be able to withstand environmental conditions and physical stresses relevant to their application.

**9. Power Consumption:** Depending on the application, low power consumption may be crucial, especially for battery-operated devices.

1. **Cost:** Balancing the cost of the sensor against its performance and application requirements is essential.
2. **Interface Compatibility:** Ensure that the sensor's output is compatible with the input requirements of the system or device it interfaces with.

Understanding the specific requirements of the application and the characteristics of different sensor types is vital for selecting the most suitable sensor for a given task.

**2.4 Alarm Systems**

**2.4.1 Introduction to alarm system**

An alarm system is a security mechanism designed to alert individuals or authorities about potential threats or security breaches. These systems are used in various settings, including homes, businesses, and public spaces, to enhance security and provide peace of mind. Alarm systems typically consist of sensors, a control panel, and notification devices.

Sensors are designed to detect alterations in the environment, such as motion, heat, or sound. Strategically placed on objects or structures like doors, windows, and walls, they aim to identify potential intruders or instances of unauthorized access.

The central processing unit of the alarm system is the control panel. Gathering information from the sensors, it evaluates the data to determine if an alarm should be triggered. Typically located in a secure area, such as a closet or basement, the control panel is connected to sensors either through cables or wireless signals.

Alarm or notification systems are intended to alert individuals about potential risks or unauthorized access. This can involve loud alarms, flashing lights, or notifications dispatched to mobile devices or central monitoring stations. Alarm systems can be customized to meet specific security needs for a property or structure. Additionally, they can be integrated with other security measures like surveillance cameras, access control systems, and fire alarms to offer comprehensive protection against potential threats.

**2.4.2 Components of an alarm system**

**1.** **Sensors:**

- Door and Window Sensors: Detects unauthorized entry through doors or windows.

- Motion Sensors: Identify movement within a designated area.

- Glass Break Sensors: Trigger an alarm when they detect the sound of breaking glass.

- Smoke and Fire Detectors: Alert occupants to the presence of smoke or fire.

- Carbon Monoxide Detectors: Warn against the presence of this odorless and potentially lethal gas.

- Security Cameras: Provide visual surveillance and recording capabilities.

**2.** **Control Panel:**

- Acts as the central hub that processes signals from sensors and triggers appropriate responses.

- Typically installed in a secure location and may have a keypad for user input.

**3.** **Notification Devices:**

- Sirens and Alarms: Emit audible alerts to deter intruders and notify occupants.

- Strobe Lights: Visual indicators that enhance alert visibility.

- Communication Devices: Transmit alerts to monitoring centers, emergency services, or property owners.

- Mobile App Integration: Allows users to receive notifications on their smart-phones or tablets.

**2.4.3 Key Features and Functionality of an Alarm System**

**1. Arming and Disarming:**

- Users can arm and disarm the system using codes, key fobs, or mobile apps.

**2. Monitoring Services:**

- Professional monitoring services can be subscribed to, where a central monitoring station is alerted in case of an alarm. They, in turn, notify the appropriate authorities.

**3. Home Automation Integration:**

- Many modern alarm systems integrate with smart home devices, allowing users to control security aspects remotely.

1. **Video Surveillance:**

- Some alarm systems include video surveillance capabilities, enabling real-time monitoring and recording.

**5. Remote Access and Control:**

- Users can control and monitor their alarm systems remotely through mobile apps or web interfaces.

**6. Emergency Response:**

- In the event of an alarm, the system can initiate predefined emergency responses, such as contacting emergency services.

**2.4.4 Types of Alarm Systems**

**1. Burglar Alarms:**

- Designed to detect unauthorized entry or intrusion.

**2. Fire Alarms:**

- Detect smoke, fire, or a sudden increase in temperature.

**3. Medical Alarms:**

- Triggered by a medical emergency, often allowing individuals to call for assistance.

**4. Environmental Alarms:**

- Monitor environmental factors such as carbon monoxide levels or flooding.

**5. Panic Alarms:**

- Instantly alert authorities in emergency situations, such as a panic button for personal safety.

**2.4.5 Considerations Choosing Alarm System**

**1. Wired vs. Wireless Systems:**

- Wired systems involve physical connections, while wireless systems use radio frequency communication.

**2. Integration with Other Security Measures:**

- Alarm systems are often part of a broader security strategy that may include access control, surveillance, and monitoring.

**3. Maintenance:**

- Regular maintenance ensures the system's reliability and functionality.

**4. False Alarm Prevention:**

- Proper installation and user education help prevent false alarms, reducing unnecessary emergency responses.

Overall, alarm systems provide a critical layer of security, offering both proactive deterrence and rapid response capabilities to protect people and property.

**2.5 Micro-controller**

A micro-controller is a compact, integrated circuit (IC) that contains a processor core, memory, and programmable input/output peripherals. It serves as the brain of embedded systems, providing a single-chip solution for controlling and managing various functions within electronic devices.

A micro-controller is employed in the creation of embedded systems, typically integrated within other devices to govern the features or operations of the product. It is occasionally referred to as an embedded controller. Embedded systems are characterized as compact computers integrated into other devices to carry out specific functions. One-Time Programmable (OTP) memory is commonly utilized in embedded systems.

**2.5.1 Components of a Micro-controller**

**1. Processor/Core:**

- The central processing unit (CPU) or core executes instructions and performs computations. Micro-controllers often have a reduced instruction set computing (RISC) architecture for efficiency.

**2. Memory:**

- Micro-controllers have both volatile (RAM) and non-volatile (Flash or EEPROM) memory. RAM is used for temporary data storage, while Flash or EEPROM stores the program code.

**3. Peripherals:**

- Micro-controllers feature built-in peripherals such as timers, counters, communication interfaces (UART, SPI, I2C), analog-to-digital converters (ADC), and digital-to-analog converters (DAC).

**4. Input/Output Ports:**

- These are pins or connectors through which the micro-controller interacts with external devices. They can be configured as digital input/output or as analog pins for various applications.

**5. Clock Source:**

- Micro-controllers require a clock signal to synchronize their operations. The clock source can be internal or external, depending on the design.

**6. Power Supply:**

- Micro-controllers operate within a specific voltage range. They may include power management features to optimize energy consumption.

**2.5.2 Key Characteristics of a Micro-controller**

**1. Embedded Systems:**

- Micro-controllers are embedded in various electronic devices such as washing machines, microwave ovens, cars, medical devices, and consumer electronics.

**2. Real-Time Operation:**

- Many micro-controllers are designed for real-time applications, where they must respond to external events within specific time constraints.

**3. Low Power Consumption:**

- Micro-controllers are often optimized for low power consumption, crucial for battery-operated devices and energy-efficient applications.

**4. Programmability:**

- Micro-controllers can be programmed using high-level programming languages like C or assembly language. Program code is typically loaded onto the micro-controller's memory.

**5. Development Tools:**

- Micro-controller development involves using Integrated Development Environments (IDEs), compilers, and debugging tools. Common vendors include Microchip, Atmel, STMicroelectronics, and Texas Instruments.

**6. Variety of Architectures:**

- Micro-controllers are available with different architectures, including 8-bit, 16-bit, and 32-bit. The choice depends on the complexity of the application.

**2.5.3 Applications of a Micro-controller**

**1. Automotive Systems:**

- Engine control units, airbag systems, and dashboard controllers.

**2. Consumer Electronics:**

- Remote controls, home automation systems, and wearable devices.

**3. Industrial Control:**

- PLCs (Programmable Logic Controllers), motor control systems, and monitoring devices.

**4. Medical Devices:**

- Patient monitoring systems, infusion pumps, and diagnostic equipment.

**5. IoT (Internet of Things):**

- Micro-controllers play a vital role in IoT devices, providing connectivity and control.

**6. Robotics:**

- Micro-controllers are used in robot control systems for motor control, sensors, and decision-making.

Micro-controllers are fundamental components in modern electronics, enabling the functionality of a wide range of embedded systems across diverse industries.

**2.5.4 Types of Micro-controller**

Various kinds of micro-controllers exist, categorized into groups:

**2.5.4.1 Micro-controller classifications according to the number of bits**

The bits of a micro-controller are 8-bit, 16-bit, and 32-bit micro-controllers.

1. **8-bit Category:** In instances where the internal bus of an 8-bit micro-controller is 8 bits, the Arithmetic Logic Unit (ALU) performs arithmetic and logic operations. Examples of 8-bit micro-controllers include the Intel 8031/8051, PIC1x, and Motorola MC68HC11 families.
2. **16-bit Category:** The 16-bit micro-controller offers improved precision and functionality compared to its 8-bit counterpart. Unlike 8-bit micro-controllers constrained to an 8-bit range (0×00 - 0xFF or 0-255) for each cycle, 16-bit micro-controllers can process data within a broader range, spanning from 0×0000 - 0xFFFF (0-65535) per cycle. This expanded range, including the ability to handle larger timer values, proves advantageous in specific applications and circuits. Furthermore, certain micro-controllers like the 8051XA, PIC2x, Intel 8096, and Motorola MC68HC12, all belonging to the extended 16-bit family, can automatically operate on two 16-bit numbers.
3. **32-bit Category**: Micro-controllers of the 32-bit variety employ 32-bit instructions to carry out arithmetic and logic operations. These micro-controllers find application in diverse automated devices, including implantable medical devices, motor control systems, home appliances, office machines, and various embedded systems. Examples of 32-bit micro-controllers include the Intel/Atmel 251 family and the PIC3x.

**2.5.4.2 Micro-controller classifications according to memory**

There are two classifications of storage devices employed in embedded systems.

**1. Micro-controllers with Built-in Memory:**

- An embedded micro-controller denotes a unit that integrates all functional components directly onto the chip. For instance, the 8051 exemplifies this category, featuring onboard program and data memory, I/O ports, serial communications, counters and timers, as well as interrupts.

1. **Microcomputers Utilizing External Memory:**

- Conversely, an external memory micro-controller is a type of embedded system utilizing a micro-controller unit lacking some built-in functional components available on the chip. An illustration is the 8031, which lacks on-chip program memory and necessitates external memory for its operation.

**2.5.4.3 Micro-controller classifications according to instruction sets**

**1. CISC (Complex Instruction Set Computer):**

- CISC stands for Complex Instruction Set Computer, enabling a programmer to substitute a single instruction with multiple, simpler instructions.

**2. RISC (Reduced Instruction Set Computer):**

- Conversely, RISC (Reduced Instruction Set Computer) simplifies microprocessor architecture to align with industry standards. RISC facilitates simultaneous access to program and data, allowing each instruction to operate on any register or address in a flexible manner.

**2.5.5 FEATURES OF A MICROCONTROLLER**

**1. CPU (Central Processing Unit):**

The central processor unit (CPU) consists of components such as the arithmetic logic unit (ALU), register, stack pointer, program counter, accumulator register, and register file. As the computer's core, it reads, decodes, and executes instructions for arithmetic logic and data transfer activities. Responsible for data processing in the micro-controller, the CPU can run programs, manage system interrupts, access memory for read and write operations, and interact with input and output ports.

**2. INTERRUPTS:**

Interrupts represent a crucial feature and handling method in micro-controllers. They denote occurrences or operations demanding immediate attention. When an interrupt occurs, the micro-controller suspends its current task to address the interrupt, launching the interrupt service function (ISR). The ISR executes necessary processing based on the interrupt source before the micro-controller returns to its paused task, resuming normal operations. Interrupts can be external (initiated through an interrupt pin) or internal (activated via a programming interrupt command).

**3. ADC (Analog-to-Digital Converter):**

Given that most sensors produce analog signals, an analog-to-digital converter (ADC) plays a vital role in converting these analog signals to digital ones. The ADC interfaces between external analog input devices and the micro-controller's processor. Since processors exclusively handle digital data (1s and 0s), they rely on the ADC to interpret analog signals.

**4. DAC (Digital-to-Analog Converter):**

Contrary to the ADC, the DAC functions in reverse, converting digital signals into analog ones. Serving as an interface between the micro-controller's processor and external analog devices like DC motors, the DAC facilitates compatibility with various drives.

**5. INPUT/OUTPUT PINS:**

Input/output ports serve as the connection points between the micro-controller and external components. Input ports receive signals from devices like switches and keypads, conveying the data to the processor. After processing the signals, the processor responds through the output port to devices such as printers and LEDs.

**6. TIMER/COUNTER:**

Timers measure time intervals, while counters tally occurrences of specific events based on a clock signal. Essential for providing time and duration information, timers and counters contribute to measuring time intervals and counting external events. The Programmable Interval Timer (PIT) is a commonly used timer, signaling the end of counting processes by sending an interrupt signal to the processor. This functionality is valuable in applications like thermostats, where periodic temperature monitoring determines device activation. In summary, timers and counters are crucial features for measuring time intervals and counting external events, with the PIT being particularly useful across various applications, including thermostats.

**2.6 Review of related works**

Erick Kithinji et al (2017), introduced a monitoring system for transformer vandalism using Arduino, radar sensors, and GSM technology. The system incorporates strategically positioned radar sensors, Arduino for control, GSM for communication, a buzzer for alarms, and a reset switch to enable continuous 24/7 security monitoring. This cost-effective approach utilizes Arduino and PIR sensor technologies, providing an efficient solution to transformer vandalism while ensuring uninterrupted power supply. Despite its promising aspects, the paper lacks specific testing details and effectiveness, creating uncertainties regarding real-world application. A more thorough exploration of potential challenges and future improvements could enhance the paper's comprehensiveness. Nevertheless, the proposed system offers valuable insights into combating transformer vandalism, presenting a technologically advanced solution for future consideration.

In a different study, Thomas Nyajowi et al (2022), introduced an innovative approach to combat transformer vandalism by employing state-of-the-art computer vision techniques. The proposed system integrates two distinct neural network architectures to effectively identify individuals in proximity to restricted transformer zones, aiming to prevent potential malicious activities. The researchers meticulously fine-tuned the system's parameters, achieving an impressive 99% accuracy in detecting and mitigating possible threats. The system's robustness arises from its ability to extract insights from three-dimensional images, autonomously discern crucial details, and even predict potential future incidents. However, to enhance the paper, further exploration of diverse settings and an evaluation of the system's performance across various scenarios could be beneficial in ensuring its adaptability and effectiveness.

Shreyansh Likhar, in this paper, proposes an autonomous monitoring system for power transformers to overcome the limitations of existing SCADA-based solutions, particularly in small-scale industries with limited automation. The suggested system employs embedded systems and focuses on detecting phase failure, unbalanced voltage, earth fault, as well as monitoring oil level and temperature. Components such as potential transformers, a micro-controller (AVR), a temperature sensor (TMP36), and a conservator oil level indicator with a magnetic oil gauge are integrated into the design. The system's objective is to offer real-time monitoring and comparison of transformer outputs with reference values, providing potential benefits in enhancing transformer health monitoring for smaller industries and minimizing downtime. However, the paper falls short in providing details on the experimental validation of the proposed system, and it lacks a comprehensive discussion on potential challenges in real-world implementation and scalability. Moreover, the economic viability and feasibility in diverse operational environments should be considered for practical application.

In their 2020 paper, Mary Ahuna et al introduce an anti-vandalism system for power pylons utilizing a machine learning approach, specifically the Google Inception deep convolutional object detection model. The system aims to monitor the pylon's environment for potential vandalism by detecting human images with confidence levels ranging from 68% to 97%. Noteworthy aspects of the system include its use of machine learning for real-time surveillance, enabling early detection and alerting. The methodology involves a Raspberry Pi as the central processing unit and training the Inception model with an ImageNet dataset, showcasing promising capabilities in detecting human presence with satisfactory confidence levels. However, the paper acknowledges ongoing testing, limited outdoor deployment results, potential weather-related challenges, and the need for further real-world validation as areas requiring attention.

The paper by Sajidur Rahman et al (2017) introduces a Real-Time Transformer Health Monitoring System (THMS) employing GSM technology for monitoring distribution transformers. The system addresses crucial parameters such as load currents, overvoltage, transformer oil level, and oil temperature. Through the integration of a GSM modem, microcontroller, and sensors, the system enables automatic data acquisition and real-time monitoring, with alerts sent via SMS in case of abnormalities. The wireless communication aspect eliminates the need for costly large cables, and potential advantages include optimizing transformer utilization, early issue identification, and reducing human dependence. However, the paper lacks detailed technical insights into the system's implementation, and its practical effectiveness is not evaluated with real-world data or field trials. Additionally, a more thorough exploration of potential challenges and limitations would enhance the paper's completeness.

In their 2020 paper on "Condition Monitoring of Distribution Transformer using IoT," the authors propose a system for the condition monitoring of distribution transformers using IoT technology. The system employs sensors to monitor key parameters such as load current, voltage, oil level, and oil temperature. The data collected by the sensors is sent to an ESP32 micro-controller, which communicates with an IoT web server (Blynk software) through Wi-Fi. The system allows for real-time monitoring of transformer parameters, and in case of abnormality, the operator receives an SMS through a GSM module. The system's strength lies in its potential to provide continuous and remote monitoring, enabling early detection of issues and preventive action. Additionally, the use of the ESP32 micro-controller with integrated Wi-Fi and Bluetooth reduces the size of the project. However, the paper lacks specific details about the implementation, testing, and validation of the proposed system, and it could benefit from more in-depth discussions on the practical challenges and limitations of the proposed approach.

In 2018, Patrick Kabanda and Samson Ssemakalu Ttondo devised a technical remedy to address transformer oil theft within Uganda's power distribution network. Their solution incorporates a monitoring system utilizing a float switch to gauge oil levels, trigger alarms, and communicate via GSM. This innovative sensor technology demonstrates a proactive strategy for identifying abnormal leakage. Despite its merits, challenges such as potential delays in SMS relay and compatibility issues with local networks highlight areas for optimization in practical scenarios.

**CHAPTER THREE: METHODOLOGY**

* 1. **Introduction**

In this chapter, we delve into the testing methods employed to create and build our transformer vandalism detection alarm system. We'll provide a clear explanation of how it functions, highlighting its organized and controllable components seamlessly integrated to safeguard transformers. Additionally, we'll explore the advancements made in our distribution transformer vandalism detection and control system.

* 1. **System Design**
     1. **Micro-controller used**

The esp32 and ATMEGA328 are both being used in this project. The esp32 is used because it is a powerful, low-cost System on a Chip (SoC) micro-controller with built-in Wi-Fi and Bluetooth connectivity. It is a popular choice for Internet of Things (IoT) projects and other applications requiring wireless communication and moderate processing power. The ATMEGA328 is used because it is a popular 8-bit micro-controller developed by Atmel, now a part of Microchip Technology. It belongs to the AVR family of micro-controllers and is widely used in various embedded systems and DIY electronics projects.

**3.2.1.1 Key features of the esp32**

1. Processor: Dual-core Tensilica Xtensa LX6 microprocessor, clocked at up to 240 MHz.
2. Memory: 320 KiB RAM, 4 MB Flash storage (expandable with SD card).

**3.** Wireless connectivity: Built-in Wi-Fi (802.11 b/g/n) and Bluetooth 4.2 (classic and Low Energy).

**4.** Peripherals: 34 programmable GPIO pins, 12-bit ADC, 2 DACs, touch sensors, SPI, I2S, etc.

**5.** Power consumption: Ranges from deep sleep mode (μA) to active mode (mA).

**6.** Development environment: Supports Arduino IDE, PlatformIO, IDF (Espressif Development Framework), etc.

**3.2.1.2 Applications**

1. IoT projects (smart home devices, wearables, sensors)
2. Robotics and automation
3. Industrial control and monitoring
4. Data logging and acquisition
5. Wearable electronics

**3.2.1.3 Key features of the ATMEGA328**

1. Processor: 8-bit AVR RISC processor, clocked at 16 MHz (overclockable to 20 MHz).
2. Memory: 32 KB Flash storage, 2 KB RAM, 1 KB EEPROM.
3. Peripherals: 14 Digital I/O pins (with PWM), 6 Analog-to-Digital converters (ADCs), timers, USART, etc.
4. Power consumption: Low power consumption, suitable for battery-powered projects.
5. Development environment: Supports Arduino IDE, PlatformIO, AVR Studio, etc.

**3.2.1.4 Applications**

1. Embedded Systems: Used in industrial control systems, automation equipment, and control panels.
2. Consumer Electronics: Found in remote controls, electronic toys, and gaming peripherals.
3. IoT Devices: Powers environmental sensors, smart meters, and home automation systems.
4. Robotics: Utilized for motor control, sensor interfacing, and overall system control in hobbyist and educational robotics projects.
5. DIY Projects: Popular for creating LED displays, weather stations, motion detectors, and more among hobbyists and makers.

**3.2.1.5 ESP32 PIN CONFIGURATION**

The ESP32 micro-controller, developed by Espressif Systems, features a variety of pins for different functionality. Here's an overview of the pin configuration:

**1. GPIO (General Purpose Input/Output) Pins:** These pins can be configured as either inputs or outputs and are used for general digital communication or controlling external devices. There are a total of 34 GPIO pins labeled GPIO0 to GPIO33.

**2. Analog Input Pins:** The ESP32 has a built-in Analog-to-Digital Converter (ADC) with a total of 18 channels. These pins allow analog signals to be read by the microcontroller. They are labeled ADC1\_CH0 to ADC1\_CH7 and ADC2\_CH0 to ADC2\_CH7.

**3. Serial Communication Pins:**

**- UART (Universal Asynchronous Receiver/Transmitter)**: The ESP32 supports multiple UART interfaces for serial communication. The primary UART interface pins are usually labeled UART0\_TX, UART0\_RX, UART1\_TX, and UART1\_RX.

**- SPI (Serial Peripheral Interface):** The ESP32 has multiple SPI interfaces for high-speed serial communication with peripherals such as sensors and displays. The pins for SPI communication include MOSI, MISO, SCK, and CS.

**- I2C (Inter-Integrated Circuit):** The ESP32 supports I2C communication for connecting to devices like sensors and EEPROMs. The I2C pins are typically labeled SDA and SCL.

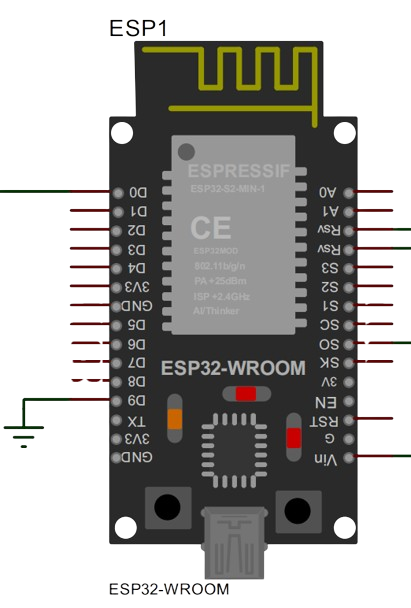
**4. PWM (Pulse Width Modulation) Pins**: These pins allow the generation of analog-like signals with varying duty cycles. They are often used for controlling LED brightness, motor speed, and generating audio tones. PWM pins are usually labeled with GPIO numbers.

**5. Touch Sensor Pins**: The ESP32 includes built-in capacitive touch sensors that can detect touch inputs. These pins are often labeled T0, T1, T2, etc.

**6. Power Supply Pins:** These pins provide power to the microcontroller and connected peripherals. Common power pins include VCC, GND, and sometimes VIN for input voltage.

**7. Boot Mode Configuration Pins:** These pins are used to configure the boot mode of the ESP32 during startup. Common boot mode pins include GPIO0, GPIO2, and GPIO15.

**8. Special Function Pins:** Some pins have special functions like controlling the built-in LED or connecting to external crystals for clock generation.



**Figure 3-1: ESP32-PIN OUT**

* + 1. **GSM MODULE**

A GSM module is a self-contained wireless module that allows a device to connect to a cellular network. It functions similarly to a mobile phone but is designed for machine-to-machine (M2M) communication rather than human use. It supports voice, SMS, and data communication over cellular networks. This allows devices to communicate with each other and with the internet, even in remote locations where Wi-Fi is unavailable. They are small and lightweight, making them ideal for integrating into devices with limited space. The GSM modules are designed to be energy efficient, which is important for battery-powered devices. It typically uses AT commands, a simple set of instructions that allow devices to control the module's functionality. The motion sensor continuously monitors its surroundings. When it detects movement, it sends a signal to the micro-controller (if used) or directly to the GSM module. The micro-controller receives the signal, analyzes it to avoid false alarms (optional), and then triggers the GSM module. The GSM module connects to the cellular network using the SIM card. Then, depending on the specific configuration:

**SMS alert:** The module sends a pre-programmed SMS message containing an alert notification and potentially location information to one or more designated phone numbers.

**Voice call:** The module dials a pre-programmed phone number and plays a recorded message or allows live audio through the sensor's location.

**Data transmission:** The module sends data over the internet to a server, which can trigger further actions like activating sirens, notifying security personnel, or recording video footage. Upon receiving the alert, the optional alarm system, like a siren or flashing lights, can be activated to deter further vandalism and attract attention.



**FIG 3-2: GSM MODULE**

* + 1. **MICROWAVE SENSOR**

The microwave sensor is being used for this project, majorly for motion detection. Microwave radiation, unlike visible light, has the ability to penetrate some materials, albeit with reduced range and clarity. This characteristic allows microwave sensors to detect motion behind thin walls, partitions, or even closed doors.

However, it's important to understand the limitations:

**Penetration depth:** The ability to "see" through walls depends on the material, thickness, and frequency of the microwave radiation used. Typically, microwave sensors can only detect motion behind thin materials like drywall (up to a few inches) or wood (even less). They won't work through concrete, brick, or metal walls.

**Reduced sensitivity:** The signal weakens as it passes through walls, making the sensor less sensitive to motion behind them. So, while it might pick up major movements, subtle gestures or slow walking might go undetected.

**False positives:** The sensor might misinterpret environmental changes, like vibrations or shifting objects behind the wall, as motion. This can lead to false alarms.

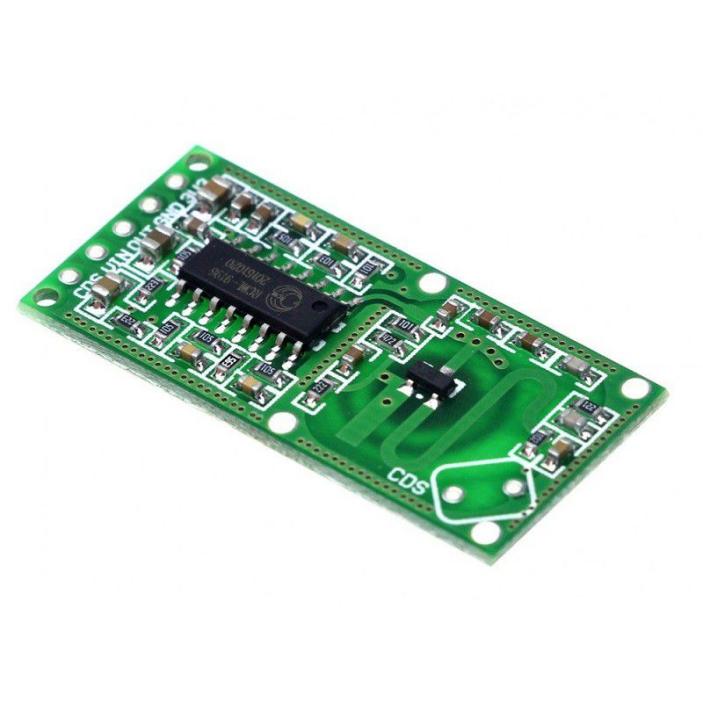
**Applications:**

This "wall-seeing" ability has some niche applications, such as:

**Security systems**: Microwave sensors can be used to monitor for intruders even if they haven't breached the physical barrier yet. This can provide an early warning and potentially deter break-in attempts.

**Building automation:** Sensors can detect occupancy in adjacent rooms, even through partitions, helping optimize lighting, heating, or ventilation based on real-time usage.

**Assisted living:** Microwave sensors can be used to monitor the movement of elderly or disabled individuals behind closed doors, providing peace of mind and enabling timely assistance if needed.



**Figure 3-3: MICROWAVE SENSOR**

* + 1. **ATMEGA328P**

The ATmega328P uses the Harvard architecture, which separates program memory and data memory. This means that the micro-controller can access both types of memory simultaneously, which can significantly improve performance compared to micro-controllers that use a von Neumann architecture (where program and data memory share the same space).

imagine you have two assistants, one for fetching instructions (program memory) and the other for getting data. With the von Neumann architecture, they both have to take turns using the same toolbox (memory). In the Harvard architecture, each assistant has their own dedicated toolbox, allowing them to work independently and much faster.

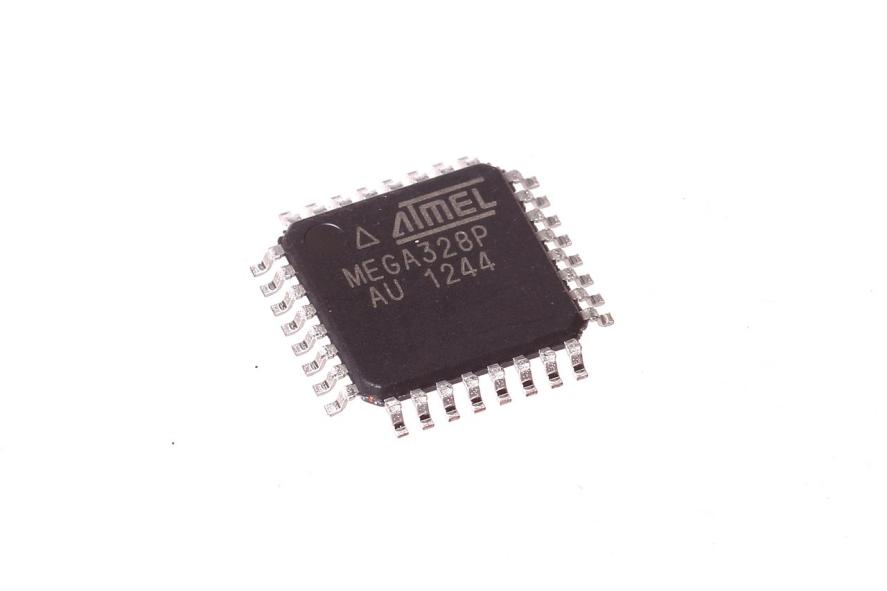
This separation of memory in the ATmega328P contributes to its efficiency and makes it a popular choice for embedded systems and hobbyist projects where performance is important.

This tiny chip packs a lot of power within its 28-pin DIP (Dual In-Line Package) format.

**It features:**

* A high-performance 8-bit AVR processor running at up to 20 MHz
* 32 KB of internal flash memory for storing your code
* 1 KB of internal SRAM for data manipulation
* 2 KB of EEPROM for non-volatile data storage
* 14 digital I/O pins, several of which can be used for analog-to-digital conversion (ADC)
* Serial communication interfaces like SPI, I2C, and UART

Despite its small size, the ATmega328P is a powerful and versatile micro-controller that can be used for a wide range of applications.



**Figure 3-4: Diagram of the ATMEGA328P**

* + 1. **ARDUINO IDE SOFTWARE**

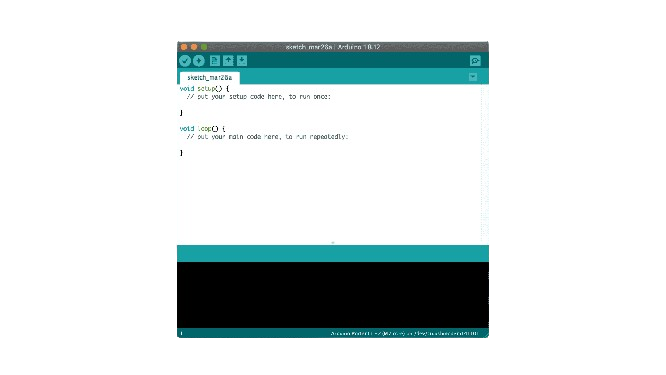
The Arduino IDE is an open-source software platform specifically designed for writing code and uploading it to Arduino boards. It's popular among beginners and experienced developers alike due to its user-friendly interface, wide range of capabilities, and strong community support. Here's a breakdown of its key features:

**Functionality:**

1. **Code editor:** Provides syntax highlighting, code completion, and debugging tools for C/C++ based programming.
2. **Board manager:** Simplifies installation and management of various Arduino boards and additional libraries.
3. **Serial monitor:** Allows communication with an Arduino board through the serial port, displaying text and sensor data.
4. **Plotter**: Visualizes data received from the serial port in real-time, aiding in data analysis.
5. **Burn boot-loader:** Enables uploading the boot-loader firmware required for using an Arduino board.
6. **Libraries:** Extensive library support expands functionality beyond built-in features.

**Benefits:**

1. **Beginner-friendly:** Simple interface and clear error messages make it easy to learn for newcomers.
2. **Cross-platform compatibility:** Runs on Windows, macOS, and Linux operating systems.
3. **Open-source community:** Access to a vast library of code examples, tutorials, and forums for support.
4. **Hardware flexibility:** Supports countless Arduino boards and third-party boards with compatible micro-controllers.
5. **Affordable hardware:** Arduino boards are generally inexpensive compared to other development platforms.



**Figure 3-5: ARDUINO SOFTWARE**

* 1. **Block diagram of the system**

DC SOURCE

MICRO CONTROLLER

(ESP32)

GSM MODULE

RF MODULE

MICROWAVE SENSOR

SURVEILLANCE CAMERA

IOT WEBSERVER

MICRO CONTROLLER

(ATMEGA328)

**Figure 3-6: SYSTEM BLOCK DIAGRAM**

* 1. **Flow chart of the system**

The flowchart can be expanded to include specific actions based on the severity of the detected vandalism or unauthorized access. Error handling and recovery mechanisms should be implemented for power failures, communication disruptions, or sensor malfunctions.

System parameters and sensitivity levels of the microwave sensor may need to be adjusted based on the specific deployment environment. The system can be integrated with additional security measures like physical barriers, lighting enhancements, and perimeter alarms for increased protection.

**SYSTEM POWER INITIALIZATION (RF, GSM).**

**POWER UP**

**IS THE POWER CONNECTED? (GRID/BATTERY)**

**SYSTEM MONITORING**

**VANDALISM ALERT**

**ALERT CONFRIMATION AND RESPONSE**

**NORMAL OPERATION:**

**CONTINUOUSLY MONITOR SENSOR AND SYSTEM STATUS**

**HANDLE FAILURE**

**END**

**START**

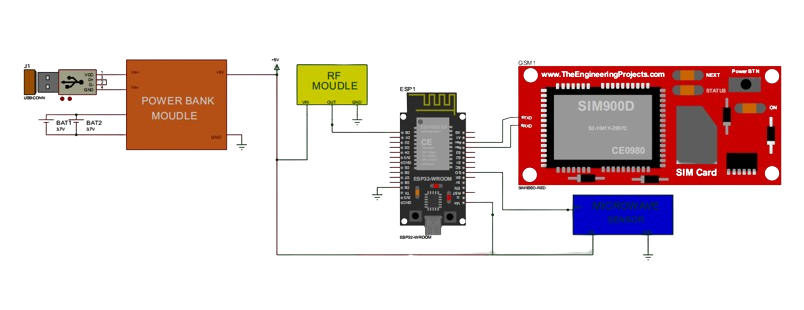
**LIVE STREAM THROUGH SURVEILLANCE CAMERA**

**NO**

**YES**

**FIG 3.7: SYSTEM FLOW CHART DIAGRAM**

**3.5 System circuit diagram**

****

**Figure 3-8: SYSTEM CIRCUIT DIAGRAM**