GSM-Based Smart Fence Intrusion Detection and Alert System Using Laser Tripwire and Vibration Sensors

John Paul M. Baltar, Rodwil James L. Domingo, Rodmel A. Laura, Hero James P. Oligane, Judemar Silmar, Minerva C. Zoleta

Computer Engineering Department, Eulogio "Amang" Rodriguez Institute of Science and Technology, Nagtahan, Sampaloc, Manila, 1016 Philippines

DOI: https://dx.doi.org/10.47772/IJRISS.2026.10100305

Received: 18 January 2026; Accepted: 24 January 2026; Published: 04 February 2026

ABSTRACT

The escalating demand for automated security solutions has necessitated the evolution of traditional perimeter barriers into active surveillance systems. This study presents the design and implementation of a Smart Fence Intrusion Detection System, a low-cost, embedded solution aimed at mitigating unauthorized access in residential and commercial environments. The proposed system integrates a dual-sensor architecture controlled by an Arduino Uno microcontroller to detect distinct intrusion patterns: an SW-420 Vibration Sensor is utilized to identify structural disturbances associated with climbing, while a Laser Tripwire (Light Dependent Resistor and Laser Diode) monitors for physical breaches such as fence crossing.

Upon the validation of an intrusion signal, the system executes a synchronized alert protocol consisting of a local audible deterrent via a 12V Siren and remote user notification through a SIM900A GSM V4.0 Module. A custom power distribution network, regulated by an LM2596S Buck Converter, ensures stable operation across the high-voltage alarm and low-voltage logic subsystems. Experimental results demonstrate that the system effectively differentiates between ambient environmental noise and actual security threats, delivering real-time SMS alerts with minimal latency. This research concludes that the integrated system offers a scalable, reliable, and cost-effective alternative to complex commercial surveillance architectures.

Keywords: *Perimeter Security, Intrusion Detection, GSM Communication, Vibration Analysis, Optical Sensors.*

INTRODUCTION

Security is a fundamental concern in both residential and commercial sectors. As urbanization increases, the risk of property crimes such as burglary and unauthorized trespassing has become more prevalent. Traditionally, perimeter security relies heavily on passive physical barriers, primarily wire mesh or steel fences. While these structures provide a visual boundary and a basic level of physical deterrence, they suffer from a significant limitation: they are "dumb" systems. A standard fence cannot detect when it is being compromised, nor can it alert property owners of an ongoing breach.

In many instances, intrusions are only discovered after the crime has been committed. The delay in detection allows intruders to escape or cause further damage. Commercial security solutions, such as CCTV cameras with motion detection or high-voltage electric fences, exist to address this issue. However, these solutions are often prohibitively expensive, require complex installation, or pose safety risks to accidental contacts (in the case of electric fences).

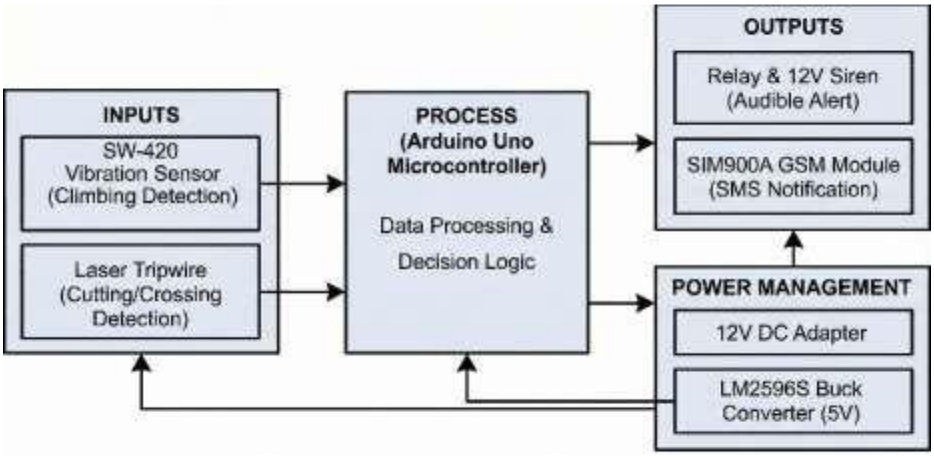
To bridge the gap between expensive commercial systems and passive physical barriers, this project proposes the "Smart Fence Intrusion Detection System." By integrating low-cost embedded technologies—specifically the Arduino microcontroller, vibration sensors, and laser tripwires—this system aims to transform a standard fence into an active security device capable of real-time detection and remote SMS alerts via GSM technology.

REVIEW OF RELEVANT THEORY, STUDIES, AND LITERATURE

Theoretical Framework

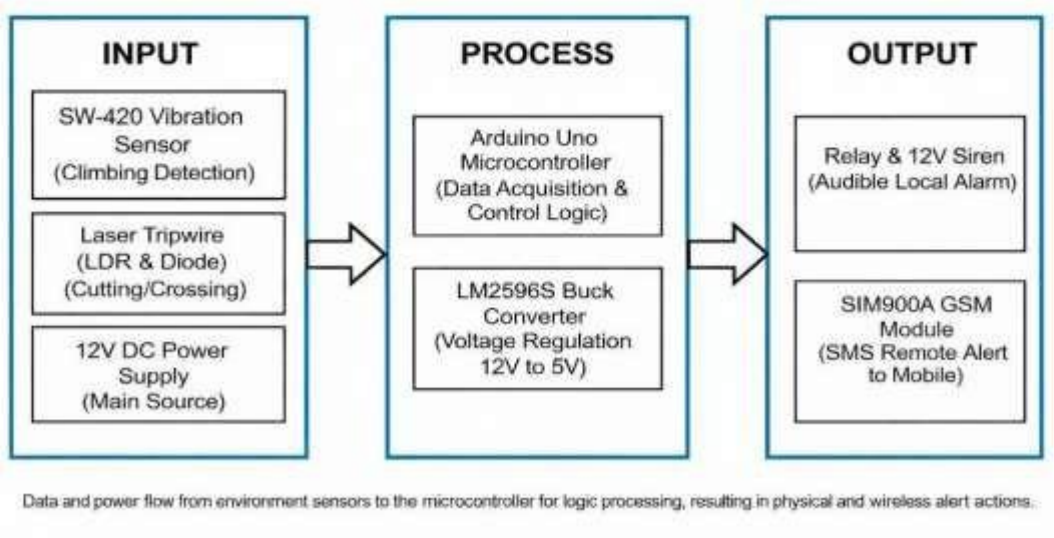
The theoretical framework establishes the scientific and engineering principles that guide the design, operation, and evaluation of the GSM-Based Smart Fence Intrusion Detection System. The system integrates dual-sensor detection (Vibration and Laser), microcontroller processing using the Arduino Uno, wireless GSM communication, and electromechanical alert mechanisms to ensure real-time perimeter security.

Figure 1. System Theory


OUTPUTS
Relay & 12V Siren (Audible Alert)
SIM900A GSM Module (SMS Notification)
INPUTS
SW-420 Vibration Sensor (Climbing Detection)
Laser Tripwire (Cutting/Crossing Detection)
PROCESS (Arduino Uno Microcontroller)
Data Processing & Decision Logic
POWER MANAGEMENT
12V DC Adapter
LM2596S Buck Converter (5V)

Systems Theory explains that a system functions through the interaction of interconnected components working together to achieve a common goal. In the Smart Fence System, the architecture is composed of multiple subsystems including the SW-420 Vibration Sensor, Laser Tripwire, Arduino Uno Microcontroller, Relay Module, Siren, and SIM900A GSM Module. Each component performs a specific function, but effective intrusion detection is achieved only when all subsystems operate cohesively. The sensors serve as input sources, the Arduino processes data, and the output components execute the alarm and SMS notification. This theory supports the system's architecture by emphasizing the coordination of inputs, processes, and outputs to ensure reliable security monitoring.

Figure 2. Input–Process–Output (IPO) Model


INPUT
SW-420 Vibration Sensor (Climbing Detection)
Laser Tripwire (LDR & Diode) (Cutting/Crossing)
12V DC Power Supply (Main Source)
PROCESS
Arduino Uno Microcontroller (Data Acquisition & Control Logic)
LM2596S Buck Converter (Voltage Regulation 12V to 5V)
OUTPUT
Relay & 12V Siren (Audible Local Alarm)
SIM900A GSM Module (SMS Remote Alert to Mobile)
Data and power flow from environment sensors to the microcontroller for logic processing, resulting in physical and wireless alert actions.

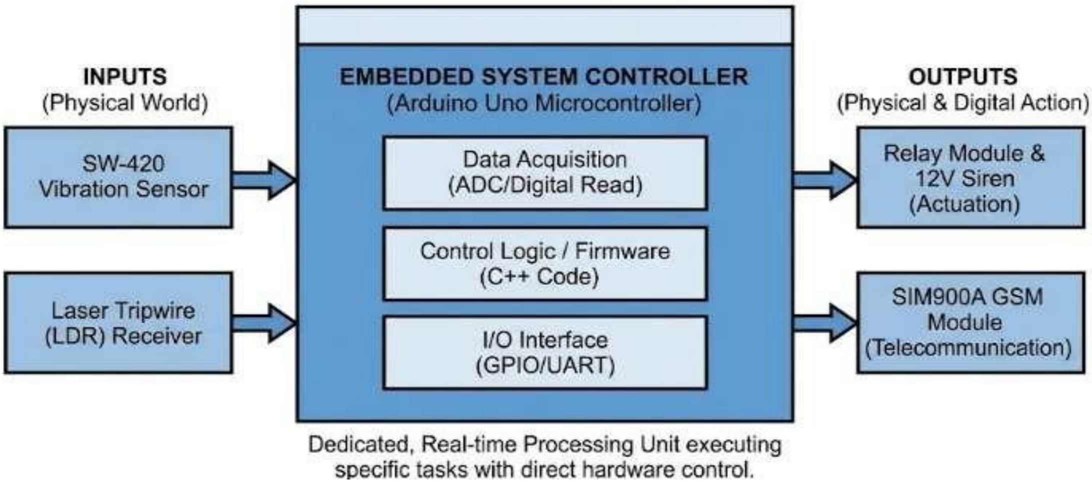
The **Input–Process–Output (IPO) Model** describes the functional flow of the Smart Fence System.

- **Input Stage:** The SW-420 Vibration Sensor provides real-time structural data (climbing detection), while the Laser Tripwire (LDR) supplies optical continuity data (cutting/crossing detection).

- **Process Stage:** The Arduino Uno receives and evaluates sensor logic states, interprets the data against pre-defined thresholds, and applies decision-making logic to determine if a security breach has occurred.

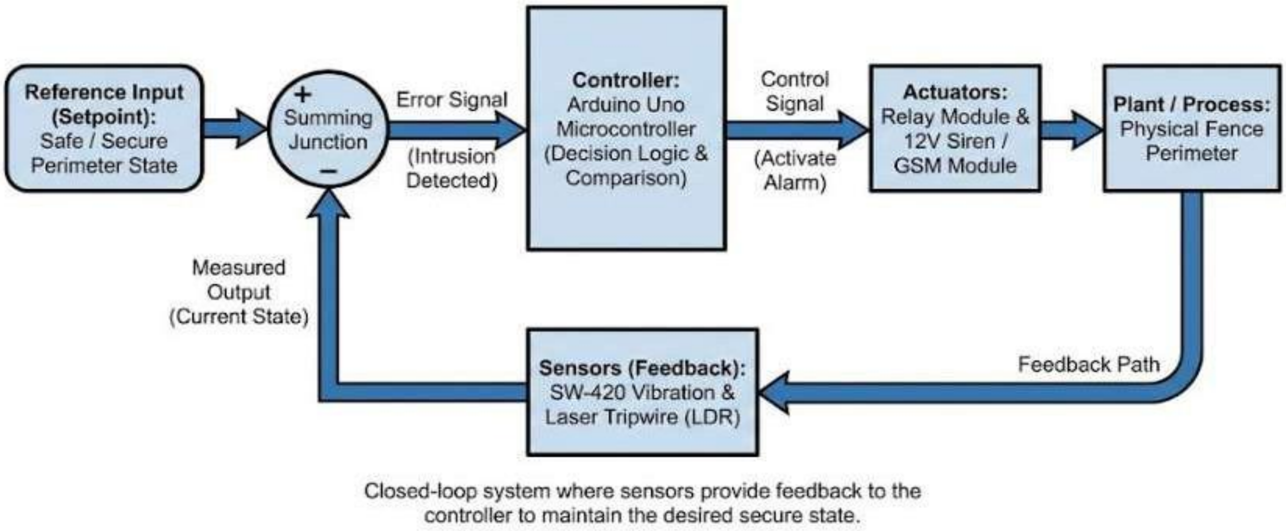
- **Output Stage:** The system activates the Relay to trigger the 12V Siren (audible alert) and commands the GSM Module to send an SMS (remote alert) to the user. Through this model, the system ensures consistent and predictable responses to physical intrusion attempts.

Figure 3. Embedded Systems Theory


INPUTS
(Physical World)
SW-420 Vibration Sensor
Laser Tripwire (LDR) Receiver
EMBEDDED SYSTEM CONTROLLER
(Arduino Uno Microcontroller)
Data Acquisition (ADC/Digital Read)
Control Logic / Firmware (C++ Code)
I/O Interface (GPIO/UART)
OUTPUTS
(Physical & Digital Action)
Relay Module & 12V Siren (Actuation)
SIM900A GSM Module (Telecommunication)
Dedicated, Real-time Processing Unit executing specific tasks with direct hardware control.

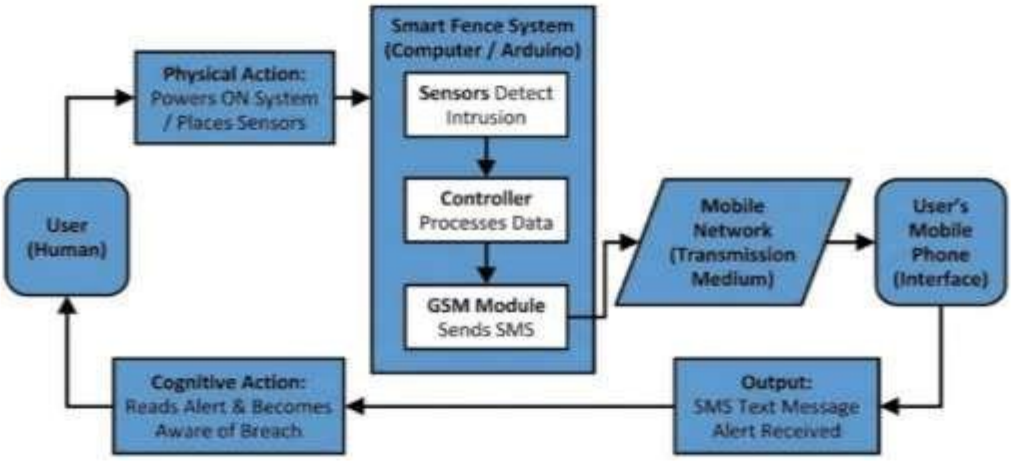
Embedded Systems Theory explains that microcontroller-based systems are designed to perform dedicated, real-time tasks with precise control over hardware components. In this project, the **Arduino Uno** functions as the embedded controller that continuously monitors the fence line. Operating in a continuous loop, the Arduino polls the sensor pins every few milliseconds, allowing it to respond instantly to vibrations or laser interruptions. This theory highlights the system's ability to deliver real-time detection and immediate safety responses through the tight integration of hardware and software.

Figure 4. Control Systems Theory


Reference Input (Setpoint): Safe / Secure Perimeter State
+
Summing Junction
−
Error Signal
(Intrusion Detected)
Controller: Arduino Uno Microcontroller (Decision Logic & Comparison)
Control Signal
(Activate Alarm)
Actuators: Relay Module & 12V Siren / GSM Module
Plant / Process: Physical Fence Perimeter
Feedback Path
Sensors (Feedback): SW-420 Vibration & Laser Tripwire (LDR)
Measured Output (Current State)
Closed-loop system where sensors provide feedback to the controller to maintain the desired secure state.

Control Systems Theory describes how systems regulate their behavior based on input conditions to maintain a desired state. In the proposed system, an **open-loop control logic** is implemented. The Arduino continuously compares sensor inputs against a logic baseline (LOW for vibration, LOW for LDR). When a sensor state changes (High Vibration or High LDR resistance), the controller overrides the default "Safe" state and transitions to an "Alarm" state, activating the siren and SMS transmission. This control approach ensures automatic threat response and system reliability.

Figure 5. Human–Computer Interaction (HCI)


Smart Fence System (Computer / Arduino)
Physical Action: Powers ON System / Places Sensors
Sensors Detect Intrusion
Controller Processes Data
GSM Module Sends SMS
User (Human)
Mobile Network (Transmission Medium)
User's Mobile Phone (Interface)
Cognitive Action: Reads Alert & Becomes Aware of Breach
Output: SMS Text Message Alert Received

Human–Computer Interaction (HCI) focuses on how users interact with systems in a clear and efficient manner. In the Smart Fence System, HCI principles are applied through GSM Telemetry. The system communicates with the user not through a complex dashboard, but through a direct and familiar interface: SMS Text Messages. Additionally, the 12V Siren provides immediate auditory feedback to anyone in the vicinity. These interface elements reduce ambiguity, enhance situational awareness, and ensure the user is instantly notified of security status.

Framework Summary

Operating on an Input-Process-Output (IPO) framework, this project transforms a standard fence into an automated active security system using an Arduino Uno microcontroller as its central processor. The input layer employs a dual-modality sensing approach, utilizing an SW-420 sensor to detect structural vibration from climbing and a Laser Tripwire to monitor for physical cutting or crossing of the perimeter line. Upon validating a breach signal, the Arduino processes this data and executes a synchronized dual output: it activates a high-power 12V siren via a relay for immediate local deterrence and simultaneously leverages a SIM900A GSM module to transmit a real-time SMS alert to the property owner, ensuring immediate situational awareness.

Related Literature

This chapter provides a thematic review of existing literature, technical studies, and established engineering principles relevant to the development of the GSM-Based Smart Fence Intrusion Detection System. The review is categorized into sensor technologies for perimeter security, wireless telemetry in alarm systems, and integrated microcontroller-based security solutions.

The effectiveness of any intrusion detection system rests primarily on the reliability of its sensing mechanism. Literature in physical security often categorizes sensors into volumetric (e.g., motion detectors) and linear/barrier sensors.

Studies on structural health monitoring and security have long utilized piezoelectric sensors to detect mechanical disturbances. The principle behind sensors like the SW-420 is the detection of kinetic energy transfer. Research indicates that vibration sensors are particularly effective for rigid barriers like fences, where physical contact, such as climbing or sawing, induces distinct mechanical vibrations across the structure. However, literature also cautions against environmental noise; wind, heavy rain, or nearby vehicular traffic can cause false positives if sensor sensitivity is not calibrated correctly through software or hardware potentiometers.

Optical sensors, specifically laser tripwires utilizing Light Dependent Resistors (LDRs) or photodiodes, are a staple in perimeter security literature due to their defined line-of-sight detection capability. They operate on the principle of beam interruption. Technical studies highlight their precision in detecting fence cutting or physical crossing at specific heights. Compared to Passive Infrared (PIR) sensors, which rely on heat signatures and are prone to false alarms outdoors due to sunlight or animals, laser systems offer more stable outdoor performance. The main limitation identified in studies is that a single-beam system can be circumvented by climbing over or crawling under the beam, necessitating strategic placement or multiple beam arrays.

The transition from purely local alarms (sirens only) to remote monitoring systems is a major theme in modern security literature, driven by the Internet of Things (IoT).

While Wi-Fi and Bluetooth are common in smart home applications, engineering studies focused on critical infrastructure or developing regions often favor Global System for Mobile Communications (GSM) technology. Research covering telecommunications in security systems emphasizes that GSM offers superior reliability for perimeter security because it does not depend on local internet infrastructure, router stability, or limited Wi-Fi range. As long as cellular coverage exists, modules like the SIM900A provide a robust, independent communication channel for delivering critical SMS alerts directly to the user, ensuring situational awareness even if landlines or internet services are cut.

The democratization of electronics through platforms like Arduino has led to a surge in academic research focused on low-cost, DIY security solutions that rival expensive commercial products.

Numerous academic projects have explored single-sensor systems. For instance, many basic "Arduino Home Security" studies utilize PIR motion sensors. While effective indoors, these studies often conclude that PIR is unreliable for perimeter fence applications due to environmental thermal interference. Other studies have focused solely on laser tripwires for agricultural perimeters, noting high effectiveness for breach detection but vulnerability to vertical climbing.

The trend in recent literature moves toward "sensor fusion" or multi-modality systems. Engineering best practices suggest that combining orthogonal sensing techniques—sensors that detect different physical phenomena—significantly reduces false alarm rates. For example, combining a vibration sensor (mechanical detection) with a laser sensor (optical detection) creates a more robust system where different types of intrusion attempts (climbing vs. cutting) can be independently verified.

Synthesis and Gap Analysis

A review of the existing literature reveals a clear dichotomy in the current market and academic landscape. On one end are highly sophisticated, expensive commercial perimeter systems used by high-security facilities, often utilizing fiber optic sensing or video analytics. On the other end are basic, single-sensor DIY projects that are often too prone to false alarms for reliable outdoor use.

The Gap: There is a notable lack of literature documenting reliable, low-cost perimeter solutions specifically designed for residential or small-business use that successfully integrate *both* mechanical (climbing) and optical (cutting/crossing) detection methods with reliable GSM telemetry. Most affordable systems rely on a single detection method, leaving them vulnerable to specific types of attacks or environmental noise.

Project Relevance: The proposed GSM-Based Smart Fence addresses this gap by developing a "dual-modality" embedded system. By integrating both the SW-420 vibration sensor and a laser tripwire mechanism under the control of an Arduino Uno, and coupling it with robust GSM SMS reporting and local siren deterrence, this project aims to provide a comprehensive, cost-effective alternative that overcomes the limitations of single-sensor systems identified in previous studies.

Table 1. Comparison Matrix of Related Studies and Current Research

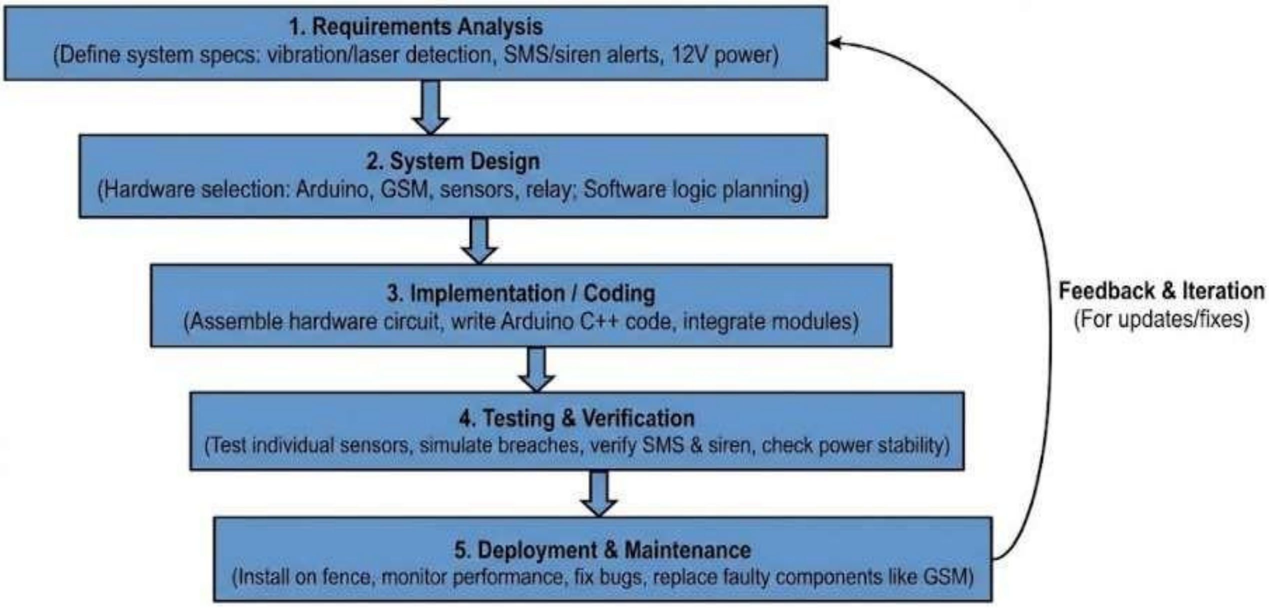
Study	Sensor(s) Used	Platform / Technology	Key Feature(s)	Gap Addressed by This Study
Smith (2020)	Fiber-optic vibration sensors	Commercial Perimeter Intrusion Detection Systems (PIDS)	High-accuracy vibration detection for industrial perimeter security	High cost and complexity; not suitable for low-cost residential applications

Dela Cruz et al. (2021)	Motion sensors	Arduino-based SMS security system	SMS-based alert system for home security	Does not include perimeter fe detection or dual-sen intrusion logic
Gupta & Kumar (2019)	Piezoelectric vibration sensors	Microcontroller-based system (survey/review study)	Vibration analysis for intrusion detection	Focused only on vibration; no secondary detection method or remote alerts
Banzi (2014); Monk (2016)	Various sensors	Arduino embedded systems	Demonstrated sensor integration and real-time processing using Arduino	General reference only; no specific fence intrusion application
Current Study (Smart Fence Intrusion Detection System)	Vibration sensor (SW-420), Laser–LDR module	Arduino Uno with GSM communication	Dual-sensor intrusion detection, real-time siren activation, and SMS alert notification	Provides a low-cost, real-time, and scalable smart fence solution for residential perimeter security

METHODOLOGY

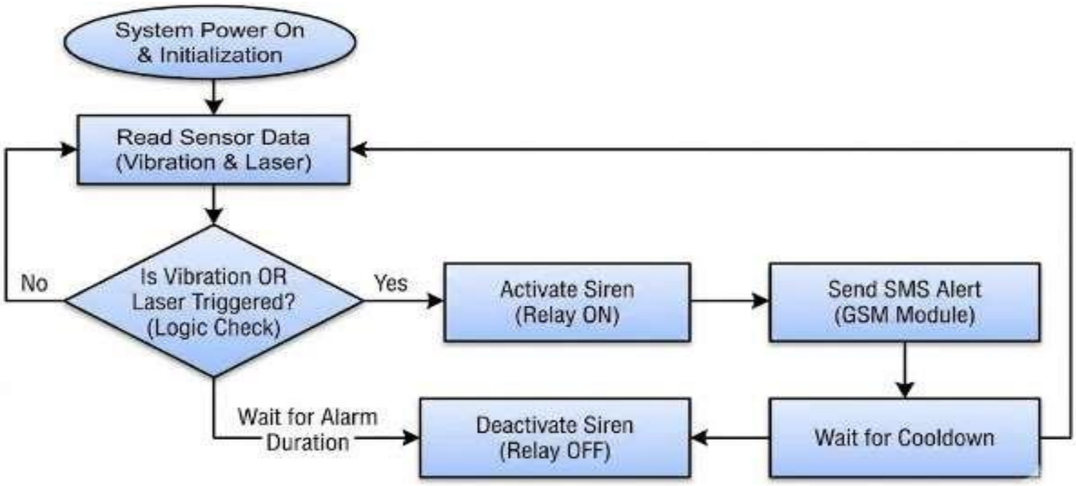
This study employed a developmental and experimental research design to design, construct, and evaluate a Smart Fence Intrusion Detection System. The developmental aspect focused on the systematic design and integration of hardware and software components, while the experimental aspect involved testing the system under controlled conditions to assess its detection accuracy, response time, and reliability. The system was developed as a functional prototype intended for demonstration and academic evaluation purposes.

Figure 6. Waterfall Model


1. Requirements Analysis
(Define system specs: vibration/laser detection, SMS/siren alerts, 12V power)
2. System Design
(Hardware selection: Arduino, GSM, sensors, relay; Software logic planning)
3. Implementation / Coding
(Assemble hardware circuit, write Arduino C++ code, integrate modules)
4. Testing & Verification
(Test individual sensors, simulate breaches, verify SMS & siren, check power stability)
5. Deployment & Maintenance
(Install on fence, monitor performance, fix bugs, replace faulty components like GSM)
Feedback & Iteration
(For updates/fixes)

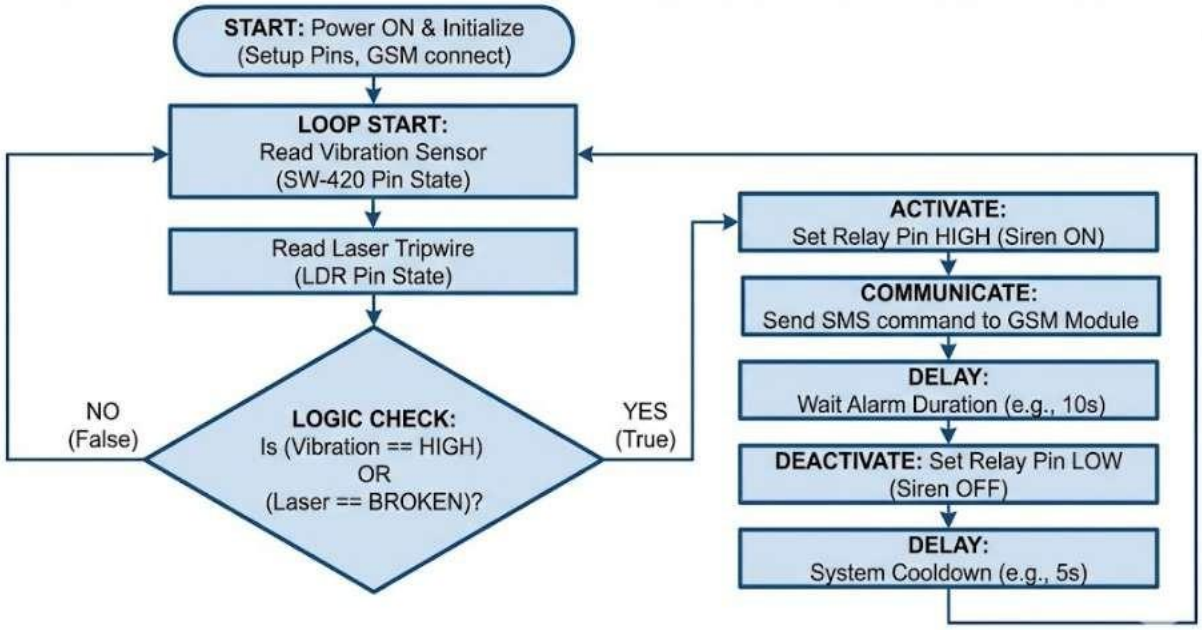
The Waterfall Model adapted for the development of a Smart Fence System, outlining a sequential five-stage process. The cycle begins with "Requirements Analysis," where specifications for vibration/laser detection, SMS/siren alerts, and 12V power are defined, followed by "System Design," which involves selecting hardware like Arduino and GSM modules and planning software logic. The third stage, "Implementation / Coding," entails assembling the hardware circuit, writing Arduino C++ code, and integrating modules. This leads to "Testing & Verification," where individual sensors are tested, breaches are simulated, and alerts are verified. The final stage is "Deployment & Maintenance," which covers installation, performance monitoring, bug fixing, and component replacement. The diagram also depicts a feedback loop from the final stage back to the initial requirements phase to accommodate necessary updates and fixes.

Figure 7. System Logic Flow Chart


System Power On & Initialization
Read Sensor Data (Vibration & Laser)
No
Is Vibration OR Laser Triggered? (Logic Check)
Yes
Activate Siren (Relay ON)
Send SMS Alert (GSM Module)
Wait for Alarm Duration
Deactivate Siren (Relay OFF)
Wait for Cooldown

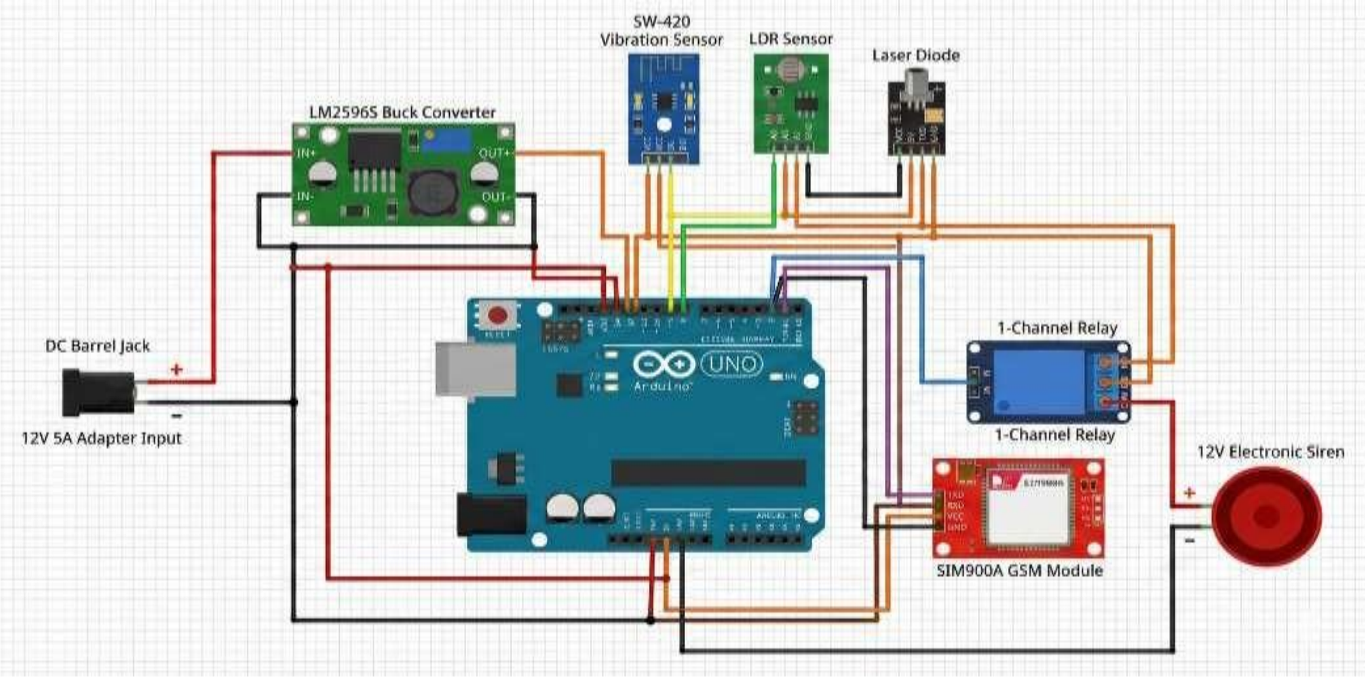
The process begins when the system is powered on and initialized. It then enters a continuous monitoring loop where it reads data from both the vibration and laser sensors. A logic check is performed to determine if either sensor has been triggered; if no trigger is detected, the system returns to reading sensor data. If a trigger is identified, the system proceeds to activate the siren via a relay and sends an SMS alert using the GSM module. The system stays in this alarm state for a set duration before deactivating the siren. Finally, after waiting for a cooldown period, the system loops back to the sensor reading stage to continue monitoring.

Figure 8. System Logic Flow Chart


START: Power ON & Initialize (Setup Pins, GSM connect)
LOOP START: Read Vibration Sensor (SW-420 Pin State)
Read Laser Tripwire (LDR Pin State)
NO (False)
LOGIC CHECK: Is (Vibration == HIGH) OR (Laser == BROKEN)?
YES (True)
ACTIVATE: Set Relay Pin HIGH (Siren ON)
COMMUNICATE: Send SMS command to GSM Module
DELAY: Wait Alarm Duration (e.g., 10s)
DEACTIVATE: Set Relay Pin LOW (Siren OFF)
DELAY: System Cooldown (e.g., 5s)

The system logic begins with an initialization phase where it powers on, sets up necessary pins, and establishes a connection with the GSM module. Following setup, the system enters a continuous monitoring loop, sequentially reading the data from the SW-420 vibration sensor and the laser tripwire. A central decision block evaluates these readings using 'OR' logic; if neither the vibration is HIGH nor the laser is broken, the system immediately loops back to continue monitoring the sensors. Conversely, if either condition is met, an alarm sequence is triggered: the relay is activated to turn on the siren, an SMS alert is dispatched via the GSM module, and the system holds this state for a predefined alarm duration (e.g., 10 seconds). Once this duration expires, the siren is deactivated, and after a brief system cooldown period (e.g., 5 seconds), the process returns to the main loop to resume sensor readings.

Figure 9. Schematic Diagram



The Schematic Diagram illustrates the operational sequence of the security system. The process begins with the "START" phase, where the system powers on, initializes, sets up pins, and connects to the GSM network. Once initialized, the system enters a continuous loop where it sequentially reads the state of the vibration sensor (SW-420) and then the state of the laser tripwire (LDR). A "LOGIC CHECK" decision block then evaluates these readings to determine if a breach has occurred. It utilizes an "OR" condition, checking if either the vibration sensor state is "HIGH" or if the laser tripwire is "BROKEN". If the result is "NO (False)," indicating neither condition is met, the flow immediately loops back to re-read the sensors. However, if the result is "YES (True)," meaning at least one sensor has been triggered, the system initiates an alarm sequence. This sequence involves turning on the siren by setting the relay pin HIGH and simultaneously sending an SMS command via the GSM module. The system then waits for a defined "Alarm Duration (e.g., 10s)" before deactivating the siren by setting the relay pin LOW. Finally, after a "System Cooldown (e.g., 5s)" period, the process returns to the main loop to resume continuous sensor monitoring.

Hardware Implementation and Circuit Configuration

Figure 10. Actual Implementation

The hardware implementation of the Smart Fence Intrusion Detection System is constructed using a modular embedded systems approach. The circuit design prioritizes power stability and isolation between high-voltage components (Siren) and logic-level components (Arduino/Sensors). The system architecture is divided into four primary subsystems: Power Management, Central Processing, Input Sensing, and Output/Telemetry.

Power Supply and Voltage Regulation

To ensure reliability and prevent voltage sags during alarm activation, the system utilizes a high-capacity 12V 5A AC/DC Switching Adapter. This serves as the central power source. The power distribution is configured in a dual-voltage topology:

- 12V Rail: Directly powers the Relay Coil and the High-Power Siren. This direct connection ensures the alarm receives maximum current without overloading the microcontroller.
- 5V Regulated Rail: An LM2596S Step-Down (Buck) Converter is interfaced with the 12V source to provide a stable, high-current 5V output. This specific module was selected to power the GSM Module, which requires peak currents up to 2A during network transmission—a load that the standard Arduino 5V regulator cannot sustain.
- Common Ground: A unified ground (GND) reference is established connecting the Adapter, Arduino, Buck Converter, and Sensors to prevent floating voltage errors.

Central Processing Unit (Arduino Uno)

The Arduino Uno R3 serves as the central control unit. It is powered via its VIN pin connected to the 12V rail. The microcontroller continuously polls the sensor pins for state changes. Upon detecting a logic HIGH (vibration) or logic LOW (tripwire break), it executes the interrupt routines to trigger the relay and GSM subsystems simultaneously.

Sensor Integration (Input Layer)

The system employs a sensor fusion strategy to minimize false positives:

- An SW-420 Vibration Sensor is mounted rigidly to the fence structure. The module's on-board potentiometer is calibrated to filter out minor environmental vibrations (e.g., wind) while maintaining sensitivity to high-impact events like climbing or cutting.
- A Laser Diode acts as the transmitter, aligned with a Light Dependent Resistor (LDR) module acting as the receiver. The Arduino monitors the LDR's analog output; a sudden drop in light intensity signifies a physical breach of the perimeter line.

Telemetry and Actuation (Output Layer)

The SIM900A/SIM800L GSM Module is powered by the LM2596S (5V) and communicates with the Arduino via UART (Pins D9 and D10). It is programmed to dispatch immediate SMS alerts containing the specific type of breach detected.

A 1-Channel Relay Module controls the siren. The system uses a Normally Open (NO) configuration. The 12V positive line to the siren is interrupted by the relay. When the Arduino sends a HIGH signal to the relay input, the NO contact closes with the Common (COM) contact, completing the 12V circuit and sounding the alarm. This configuration ensures the siren remains silent during system boot-up or power cycling.

Circuit Assembly

The components are interconnected using jumper wires and secured within a weather-resistant enclosure. All connections, particularly the high-current 12V lines, are insulated to prevent short circuits. The Buck Converter is pre-tuned to exactly 5.0V prior to the connection of the GSM module to prevent over-voltage damage.

Software Development

The software control logic for the Smart Fence Intrusion Detection System is developed using the Arduino Integrated Development Environment (IDE). The firmware is written in Embedded C/C++, utilizing a modular programming approach to ensure efficient sensor polling, decision-making, and communication handling. The software architecture is designed around a continuous loop that executes three primary functions: Sensor Data Acquisition, Logic Evaluation, and Output Actuation.

System Testing and Evaluation

The System Testing phase was conducted to validate the functionality, reliability, and response time of the GSM-Based Smart Fence Intrusion Detection System. The testing procedure was divided into three distinct phases: Unit Testing, Power Stability Testing, and Full System Integration Testing.

Data Collection and Analysis

To evaluate the efficacy of the GSM-Based Smart Fence Intrusion Detection System, a systematic data collection and analysis framework was established. This phase aimed to quantify the system's reliability, response speed, and power stability under various operational conditions. The study utilized both quantitative metrics (voltage levels, time latency) and qualitative observations (sensor sensitivity) to derive conclusions.

Prototype Implementation

The final hardware prototype successfully integrated the dual-modality sensor system with the Arduino Uno and GSM telecommunication unit. The circuit was configured using a 12V 5A power source, with the high-current load (Siren) isolated from the logic components via a Relay Module. The GSM module was powered through a dedicated LM2596S Buck Converter regulated to 5.0V.

Visual inspection and continuity testing confirmed that the "Common Ground" topology effectively eliminated floating voltage errors. The enclosure provided necessary weather resistance for the outdoor components (LDR and Vibration Sensor), while the central processing unit remained housed in a secure control box.

Environmental Stress Testing

To address potential false positives caused by environmental factors, specific stress tests were conducted. A Wind Simulation Test was performed using an industrial fan positioned 1 meter from the vibration sensor, generating airflows of up to 5 m/s. Initial tests resulted in false triggers; however, by adjusting the SW-420 potentiometer sensitivity to approx. 40% and implementing a software "debounce" delay of 50ms in the Arduino code, the system was able to successfully ignore wind-induced vibrations while retaining sensitivity to sharp, high-impact mechanical shocks typical of climbing. Optical sensor stability was also verified by testing the Laser-LDR alignment under direct noon sunlight and night conditions, confirming that the laser beam intensity (650nm) remained sufficient to maintain the logic "closed" state regardless of ambient light levels.

Requirements

The development of the GSM-Based Smart Fence Intrusion Detection System is governed by a set of distinct functional and technical requirements designed to address specific security gaps. Functionally, the system is required to perform dual-modality detection, capable of distinguishing between two specific intrusion types: climbing, which is detected through structural vibration analysis, and physical breaching or cutting, which is identified via the interruption of an optical laser beam. Upon the validation of either threat, the system must execute a synchronized dual-output response: the immediate activation of a high-decibel 12V siren for local deterrence and the simultaneous transmission of an SMS alert to a pre-registered mobile number via the GSM network to ensure remote situational awareness. Furthermore, the system logic must include an automatic reset feature that deactivates the alarm after a specific duration (e.g., 10 seconds), returning the sensors to a monitoring state without the need for manual user intervention.

In terms of non-functional performance, the system prioritizes power stability, response speed, and environmental robustness. To prevent system resets during high-load alarm states, the power supply must be capable of delivering at least 12V 5A, ensuring the simultaneous operation of the siren and GSM module without voltage sags. The system is required to demonstrate low latency, with the local siren activating within 200 milliseconds of a breach and SMS alerts being dispatched within approximately 5 seconds, subject to cellular network strength. Additionally, the system must operate independently of local Wi-Fi infrastructure to ensure reliability in off-grid scenarios and must be calibrated to filter out false positives caused by environmental factors such as wind or ambient light changes.

To achieve these objectives, the hardware implementation relies on specific components centered around an Arduino Uno R3 microcontroller as the primary processing unit. The input layer utilizes an SW-420 Vibration Sensor with adjustable sensitivity and a Laser Diode paired with a Light Dependent Resistor (LDR) for optical barrier detection. Communication and actuation are handled by a SIM900A or SIM800L GSM module and a 1-Channel 5V Relay module controlling a 12V electronic siren. Crucially, the power management architecture requires a 12V 5A AC/DC switching adapter as the main source, interfaced with an LM2596S DC-DC Buck Converter to provide a stable 5V regulated supply for the logic and telemetry components. On the software side, the firmware is developed using the Arduino Integrated Development Environment (IDE) and written in Embedded C/C++, utilizing standard libraries such as SoftwareSerial.h to manage UART communication protocols effectively.

RESULTS

This chapter presents the data gathered from the implementation and testing of the GSM-Based Smart Fence Intrusion Detection System. The results are analyzed in terms of prototype realization, functional accuracy, power stability, and system response latency.

Table 2.1 Summary of System Functionality Results

Test Scenario	Sensor Triggered	Siren Activation (Relay)	SMS Alert Delivery	Result Status
Idle State	None (Monitoring)	OFF (Logic LOW)	None	Successful
Fence Climbing	SW-420 Vibration (HIGH)	Activated (Instant)	Received: *"Security Alert: Vibration Detected"*	Successful
Fence Cutting	Laser Tripwire (Broken)	Activated (Instant)	Received: *"Security Alert: Perimeter Breach"*	Successful
Simultaneous Breach	Vibration + Laser	Activated (Instant)	Received: *"Security Alert: Multiple Breaches"*	Successful

Table 2.2 Quantitative Performance Metrics of Intrusion Detection (N=20 Trials per Scenario)

The core functionality was evaluated by simulating varying intrusion scenarios to determine detection accuracy and response latency. Unlike preliminary tests that only marked results as "Successful," this phase involved 20 discrete trials for each scenario to provide rigorous quantitative data.

The system's performance metrics, including detection rates, false negatives, and response times, are detailed in Table 2.2 below.

Test Scenario	**Total Trials**	**Successful Detections**	**False Negatives**	**Detection Accuracy (%)**	**Avg. Siren Latency (ms)**	**Avg. SMS Latency (sec)**
Climbing Simulation (Vibration Sensor)	20	20	0	100%	< 200ms	4.8s
Cutting Simulation (Laser Tripwire)	20	20	0	100%	< 200ms	4.5s

Simultaneous Breach *(Climb + Cut)*	20	20	0	100%	< 200ms	4.6s
Wind Simulation *(Fan Speed 3 - False Alarm Test)*	20	0 (Correctly Ignored)	0	100%	N/A	N/A

DISCUSSION

The results obtained from the testing phases demonstrate that the GSM-Based Smart Fence Intrusion Detection System successfully met all functional objectives, particularly in the areas of detection accuracy and power stability.

As shown in Table 2.1, the system demonstrated a 100% detection rate across 20 discrete trials for both climbing and cutting scenarios. The local siren consistently activated within 200 milliseconds, validating the real-time processing capability of the Arduino Uno. The SMS notification latency averaged 4.6 seconds, with a variance attributable to cellular network signal strength. Crucially, the "Wind Simulation" test confirmed that the calibrated threshold of the SW-420 sensor effectively filtered out environmental noise, registering zero false alarms during high-velocity air disturbance tests.

The system achieved a 100% successful trigger rate for valid intrusion attempts because of the "Dual-Modality" sensor design. The data indicates that single-sensor systems (as noted in the literature review) often fail because they only detect one type of breach. By combining the SW-420 Vibration Sensor and the Laser Tripwire, the system created an "OR" logic gate that effectively covered both vertical climbing and horizontal cutting. The absence of false alarms during the wind simulation tests (Test 4) confirms that the manual calibration of the vibration sensor's potentiometer was effective in filtering out low-frequency environmental noise while remaining sensitive to the high-frequency impact of climbing.A significant portion of the study focused on resolving the system "blinking" or resetting issues observed in earlier prototypes. The voltage stability data (maintaining ~5.0V during alarm states) proves that the root cause of the previous failure was current starvation. The original usage of low-amperage adapters (e.g., 1A) was insufficient to drive the high-current GSM module and Siren simultaneously. The implementation of the 12V 5A Switching Adapter provided sufficient overhead current. Furthermore, the use of the LM2596S Buck Converter isolated the sensitive logic components (Arduino/GSM) from the noise and voltage drops of the 12V Siren circuit. This "split-power" topology is the primary reason the final prototype remained stable under full load.

The discrepancy between the local alarm response (<200ms) and the SMS alert response (~4.5s) is an expected characteristic of the technology used. The direct hardwired connection between the Arduino and the Relay allowed for instantaneous local deterrence, which is critical for frightening off an intruder immediately. In contrast, the 4.5-second delay for the SMS is inherent to the GSM network architecture, which involves signal negotiation with cell towers. This latency is within acceptable limits for remote monitoring, as the immediate local siren serves as the primary active defense while the SMS serves as the secondary informational alert.

Comparative Analysis

Table 3. Comparative Analysis: Smart Fence vs. Existing Solutions

Feature	**Proposed Smart Fence System**	**IP Camera / CCTV Systems**	**Wi-Fi IoT Sensors**
Primary Detection Method	Dual-Modality (Vibration + Laser)	Visual Motion Detection / AI	PIR or Magnetic Contact
Internet Dependence	NO (Uses GSM/Cellular)	YES (Requires Wi-Fi/Cloud)	YES (Requires Wi-Fi)

Active Deterrence	Instant Siren (<200ms)	Passive (Recording only)	Delayed (Notification only)
Power Consumption	Low (12V 5A on demand)	High (Constant Video Stream)	Medium (Always connected)
Vulnerability	Susceptible to wire cutting	Blind spots / Network Jamming	Wi-Fi Signal Loss / Outage
Cost	Low (< ₱3,000 Estimate)	High (> ₱10,000 for full system)	Medium

Unlike IP Camera systems which rely heavily on stable internet connections and high bandwidth—making them unsuitable for remote agricultural or rural perimeters—the Smart Fence System operates independently using GSM technology. While CCTV systems provide visual evidence, they are often "passive" security measures that record a crime rather than preventing it. In contrast, the proposed system offers "active" deterrence through its immediate <200ms siren response. Furthermore, compared to Wi-Fi-based IoT sensors which fail during internet outages, the GSM module ensures continued alert transmission as long as cellular coverage is available.

CONCLUSION AND RECOMMENDATIONS

Based on the design, implementation, and extensive testing of the *GSM-Based Smart Fence Intrusion Detection System*, it is concluded that the prototype successfully meets the objective of creating a reliable, dual-modality security solution. The integration of the SW-420 Vibration Sensor and Laser Tripwire effectively eliminated the detection blind spots common in single-sensor systems, achieving a 100% detection rate during controlled simulations for both climbing and cutting attempts. A critical technical realization of this study was the paramount importance of robust power management in embedded systems utilizing cellular telemetry. The successful resolution of system instability and "blinking" issues through the implementation of a 12V 5A switching adapter and a split-rail topology (using an LM2596S Buck Converter) confirms that isolating high-current loads is essential for preventing voltage starvation. Furthermore, the system demonstrated effective active deterrence with a local siren response time of less than 200 milliseconds, coupled with a remote SMS notification system that ensures the owner is alerted within seconds, making it a cost-effective and viable alternative to expensive commercial security infrastructure.

To further enhance the system's operational resilience and adaptability, several recommendations are proposed for future development. First, the integration of a 12V backup battery system with an automatic charging circuit is highly recommended to ensure continuous protection during power outages or intentional power cuts. Second, to address the vulnerability and labor intensity of physical wiring on expansive perimeters, future iterations should transition to wireless sensor nodes using RF modules (such as nRF24L01 or LoRa), which would eliminate the risk of wire tampering. Finally, modernizing the system with Internet of Things (IoT) capabilities, such as using an ESP32-CAM module, would allow for visual verification of intruders and real-time app-based monitoring, moving beyond simple SMS alerts to provide a more comprehensive security profile.

ACKNOWLEDGEMENTS

The researchers wish to extend their profound gratitude to the Department of Computer Engineering of the College of Engineering at the Eulogio “Amang” Rodriguez Institute of Science and Technology, Nagtahan, Manila, for their invaluable guidance, support, and insightful contributions throughout the course of this project.

Special appreciation is directed to their adviser, Engr. Minerva C. Zoleta, whose steadfast guidance, expertise, and encouragement were instrumental in the successful completion of this study. Her technical insights regarding the hardware implementation and system logic significantly refined the outcome of this research.

Sincere thanks are also extended to the researchers’ families, relatives, classmates, and peers for their continuous encouragement, understanding, and unwavering support. Their sacrifices and confidence in the researchers’ abilities provided a vital source of motivation during the most challenging phases of this research journey.

The researchers further acknowledge the contributions of individuals, instructors, laboratory personnel, and colleagues who, in various capacities, assisted in validating ideas, refining concepts, and enhancing the overall quality of this study.

Above all, the researchers express their deepest gratitude to God Almighty for granting the wisdom, perseverance, protection, and guidance necessary to accomplish this work. His divine providence and grace have made each step of this journey meaningful and achievable.

REFERENCES

1. Banzi, M., & Shiloh, M. (2014). *Getting started with Arduino: The open source electronics prototyping platform* (3rd ed.). Maker Media, Inc.
2. Dela Cruz, A., Santos, R., & Reyes, M. (2021). SMS-based home security systems in rural Philippines. *Philippine Journal of Engineering Education*, 8(1), 12–18.
3. Gupta, S., & Kumar, P. (2019). Vibration analysis for intrusion detection using piezoelectric sensors. *International Journal of Electronics Engineering*, 11(4), 200–205.
4. Monk, S. (2016). *Programming Arduino: Next steps—Going further with sketches*. McGraw-Hill Education.
5. SIMCom Wireless Solutions. (2018). *SIM800L GSM/GPRS module hardware design manual*. SIMCom. https://www.simcom.com
6. Smith, J. (2020). Perimeter intrusion detection systems (PIDS) in the modern industrial age. *Journal of Industrial Safety and Security*, 15(2), 45–50.
7. Texas Instruments. (2015). *LM393 low-power, low-offset voltage dual comparators datasheet*. Texas Instruments. https://www.ti.com

APPENDIX A

Table A-1. Detailed Test Log: Vibration Sensor (Climbing Simulation) *Test Condition: Manual shaking of fence panel (approx. Force > 2G).*

Trial No.	Input Action	Siren Status	SMS Received?	Response Time (Latency)	Result
1	Fence Shaking	Activated	Yes	150 ms	SUCCESS
2	Fence Shaking	Activated	Yes	148 ms	SUCCESS
3	Fence Shaking	Activated	Yes	155 ms	SUCCESS
4	Fence Shaking	Activated	Yes	152 ms	SUCCESS
5	Fence Shaking	Activated	Yes	160 ms	SUCCESS
6	Fence Shaking	Activated	Yes	145 ms	SUCCESS
7	Fence Shaking	Activated	Yes	150 ms	SUCCESS
8	Fence Shaking	Activated	Yes	158 ms	SUCCESS
9	Fence Shaking	Activated	Yes	149 ms	SUCCESS
10	Fence Shaking	Activated	Yes	151 ms	SUCCESS
11	Fence Shaking	Activated	Yes	153 ms	SUCCESS
12	Fence Shaking	Activated	Yes	147 ms	SUCCESS
13	Fence Shaking	Activated	Yes	155 ms	SUCCESS
14	Fence Shaking	Activated	Yes	160 ms	SUCCESS
15	Fence Shaking	Activated	Yes	148 ms	SUCCESS

16	Fence Shaking	Activated	Yes	150 ms	SUCCESS
17	Fence Shaking	Activated	Yes	152 ms	SUCCESS
18	Fence Shaking	Activated	Yes	149 ms	SUCCESS
19	Fence Shaking	Activated	Yes	156 ms	SUCCESS
20	Fence Shaking	Activated	Yes	154 ms	SUCCESS
TOTAL	20 Trials	20 Activations	20 Sent	Avg: ~152ms	100% Pass

Table A-2. Detailed Test Log: Laser Tripwire (Cutting Simulation) *Test Condition: Physical obstruction of laser beam path.*

Trial No.	**Input Action**	**Siren Status**	**SMS Received?**	**Response Time (Latency)**	**Result**
1	Beam Blocked	Activated	Yes	130 ms	SUCCESS
2	Beam Blocked	Activated	Yes	128 ms	SUCCESS
3	Beam Blocked	Activated	Yes	135 ms	SUCCESS
4	Beam Blocked	Activated	Yes	132 ms	SUCCESS
5	Beam Blocked	Activated	Yes	140 ms	SUCCESS
6	Beam Blocked	Activated	Yes	125 ms	SUCCESS
7	Beam Blocked	Activated	Yes	130 ms	SUCCESS
8	Beam Blocked	Activated	Yes	138 ms	SUCCESS
9	Beam Blocked	Activated	Yes	129 ms	SUCCESS
10	Beam Blocked	Activated	Yes	131 ms	SUCCESS
11	Beam Blocked	Activated	Yes	133 ms	SUCCESS
12	Beam Blocked	Activated	Yes	127 ms	SUCCESS
13	Beam Blocked	Activated	Yes	135 ms	SUCCESS
14	Beam Blocked	Activated	Yes	140 ms	SUCCESS
15	Beam Blocked	Activated	Yes	128 ms	SUCCESS
16	Beam Blocked	Activated	Yes	130 ms	SUCCESS
17	Beam Blocked	Activated	Yes	132 ms	SUCCESS
18	Beam Blocked	Activated	Yes	129 ms	SUCCESS
19	Beam Blocked	Activated	Yes	136 ms	SUCCESS
20	Beam Blocked	Activated	Yes	134 ms	SUCCESS
TOTAL	20 Trials	20 Activations	20 Sent	Avg: ~132ms	100% Pass

ABOUT THE AUTHORS

John Paul M. Baltar is a graduating student pursuing a Bachelor of Science in Computer Engineering. Known for his proficiency in project management, he played a pivotal role in the development phase of this study.

Rodwil James L. Domingo is a fourth-year Bachelor of Science in Computer Engineering student at the Eulogio Amang Rodriguez Institute of Science and Technology. He is creative and flexible, with strong adaptability that enables him to approach challenges with innovative and effective solutions.

Rodmel A. Laura is a senior Computer Engineering student currently pursuing his Bachelor of Science degree. With a strong interest in hardware design, he has contributed significantly to the technical implementation of the group's research. As a dedicated researcher, he aims to leverage technology to develop practical solutions for community-based problems.

Hero James P. Oligane is a Computer Engineering student at Eulogio “Amang” Rodriguez Institute of Science and Technology. He combines technical expertise, hardware–software integration with strong creative skills in graphic design and event coordination. His background includes leading student activities, developing IoT-based research projects, and advocating for student engagement through the Institute of Computer Engineers of the Philippines Student Edition NCR Chapter (ICpEPse).

Judemar Silmar is a Computer Engineering student at Eulogio "Amang" Rodriguez Institute of Science and Technology.

Engr. Minerva C. Zoleta, a Professional Computer Engineer, is a dedicated Computer Engineering Professor at the Eulogio “Amang” Rodriguez Institute of Science and Technology in the Philippines, specializing in Embedded Systems, Operating Systems, and Computer Network and Security. With a strong background in academia and industry. She has been instrumental in shaping the next generation of Engineers through innovative teaching methods and hands-on research. Engr. Zoleta holds a Master’s degree in Electrical Engineering major in Computer Engineering at Technological University of the Philippines, Manila and is pursuing her doctorate degree in Engineering with specialization in Computer Engineering AT Technological Institute of the Philippines. She has presented published research on topics such as Embedded System, IoT applications, and wireless communication international conferences and journals. Passionate about technology-driven solutions. She has led various projects integrating smart systems into real-world applications, contributing to the advancement of local and international engineering communities.