Int. j. adv. multidisc. res. stud. 2026; 6(4):476-483

Received: 21-05-2026
Accepted: 02-07-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Energy-Efficient and Security-Conscious Design of a PIR-Based Motion-Responsive Lighting System: Bridging Occupancy Sensing and IoT Threat Mitigation

[1] Joseph Oladele Aremu, [2] Ibrahim Yakubu Aliyu, [3] Anah Hassan Bijik, [4] Olusegun Ishaya Adelaiye, [5] Theophilus Toro Danjuma

[1, 2, 3, 4, 5] Department of Computer Science, Bingham University, Karu, Nigeria

Corresponding Author: **Joseph Oladele Aremu**

Abstract

Conventional static lighting systems in residential and institutional environments remain a principal driver of unnecessary electrical energy consumption, particularly in contexts characterized by irregular and unpredictable occupancy patterns. Beyond inefficiency, the growing integration of embedded sensing and actuation hardware into building infrastructure introduces a parallel and frequently overlooked concern: such low-cost, often security-naive devices constitute an expanding attack surface within increasingly networked smart-building ecosystems. This study presents the design, hardware implementation, firmware development, and empirical evaluation of a low-cost, occupancy-driven motion-responsive illumination system founded on Passive Infrared (PIR) sensor technology interfaced with an Arduino Uno microcontroller, accompanied by a structured security-aware analysis of the system's architecture and deployment implications. In parallel, the system architecture was subjected to a threat-modeling analysis to identify cybersecurity-relevant weaknesses inherent to its embedded design. The system continuously monitors a designated indoor space and autonomously activates connected lighting loads upon detecting infrared radiation differentials attributable to human motion, subsequently deactivating the load after a configurable inactivity timeout of 12 seconds. Hardware components comprising an HC-SR501 PIR sensor, ATmega328P-based microcontroller, single-channel relay module, and LED illumination element were assembled and tested across multiple indoor scenarios including variable occupancy conditions, ambient illumination levels, and spatial configurations. Empirical evaluation yielded an aggregate detection accuracy of approximately 85%, a mean response time of 0.8 seconds, and an estimated energy reduction of up to 94% relative to manually operated conventional lighting over equivalent operational periods. The system demonstrated consistent and reliable functional performance across all evaluated scenarios, with residual limitations attributable to line-of-sight constraints and the inherent insensitivity of PIR technology to stationary occupants. The findings establish both the technical viability of PIR-microcontroller integration as an affordable, scalable strategy for demand-side lighting energy management in resource-constrained environments, and the necessity of incorporating baseline security safeguards prior to any networked extension of such systems, with particular relevance to Sub-Saharan African contexts characterized by persistent electricity supply deficits and accelerating smart-infrastructure adoption.

Keywords: Passive Infrared Sensor, Motion-Responsive Lighting, Arduino Microcontroller, Occupancy Detection, Demand-Side Energy Management, Embedded Systems, Smart Building, Energy Conservation, IoT Security, Embedded Systems Security, Threat Modeling

1. Introduction

Global electricity consumption attributable to artificial lighting constitutes approximately 15–19% of total electrical energy generated worldwide, with building-integrated lighting systems contributing an estimated 30–40% of a typical commercial structure's total energy demand (Fernandez & Mideros, 2018; Obioma *et al*., 2025) [6, 13]. A disproportionate fraction of this consumption is incurred during unoccupied periods, arising from the persistent reliance on manual switching mechanisms that afford no adaptive response to real-time occupancy conditions. In developing economies, particularly those in Sub-Saharan

Africa where electricity supply deficits impose severe economic and developmental constraints, the inefficient utilization of available power constitutes a compounding burden on households, institutions, and national energy infrastructure (Jin *et al*., 2020) [8].

Automated lighting control systems represent one of the most accessible and cost-effective interventions available for reducing building-level energy waste. Among the sensor modalities suitable for occupancy detection, Passive Infrared (PIR) technology has emerged as the preferred approach for low-cost embedded implementations, owing to its passive operational principle, low quiescent power draw, minimal processing overhead, and broad compatibility with microcontroller-based control architectures (Amuta *et al*., 2024; Sulaiman *et al*., 2024) [1, 17]. PIR sensors function by detecting spatial differentials in infrared radiation across a dual-element pyroelectric detector, enabling reliable discrimination between the thermal signature of a moving human body and the relatively uniform infrared background of an unoccupied space (Jia, 2024) [7].

Despite the theoretical maturity of PIR-based occupancy sensing, a persistent gap exists between conceptual demonstration and practically deployable, context-appropriate implementations. Many existing systems either lack rigorous empirical evaluation, depend on connectivity infrastructure unavailable in low-resource environments, or are cost-prohibitive for small-scale residential and institutional deployment (Argelwar *et al*., 2024; Li *et al*., 2023) [2, 9]. A further, less frequently examined gap concerns the security posture of such embedded systems: as occupancy-sensing and actuation hardware proliferates within smart-building ecosystems, even ostensibly standalone devices become candidates for future networked integration, and design decisions made at the prototype stage—such as the absence of authenticated programming interfaces or encrypted control channels—can propagate into deployed infrastructure with limited opportunity for retrofit (Sicari *et al*., 2015; Atzori *et al*., 2010) [16, 3]. This study addresses both gaps by presenting the design, implementation, and systematic evaluation of a standalone PIR-microcontroller-based motion-responsive illumination system engineered for cost-effective indoor deployment in the Nigerian context, together with a structured assessment of the cybersecurity implications of its architecture, where energy conservation and infrastructure security at the point of use are jointly of strategic importance.

1.1 Problem Statement

Conventional lighting systems operating under manual control remain the dominant paradigm in Nigerian residential, educational, and commercial buildings. These systems are functionally incapable of responding to dynamic occupancy states, resulting in sustained illumination of unoccupied spaces and consequent energy waste. The integration of automated, occupancy-responsive control mechanisms has been identified as a viable strategy for mitigating this inefficiency; however, existing implementations frequently fail to achieve the combination of low cost, technical robustness, and ease of deployment required for broad adoption in resource-constrained settings (Bachanek *et al*., 2021; Obioma *et al*., 2025) [4, 13]. Compounding this challenge, the embedded hardware underpinning such systems is typically engineered with cost and functional reliability as the dominant design criteria, with cybersecurity considerations—such as firmware integrity protection, sensor-spoofing resistance, and actuator access control—rarely addressed at the prototype or pilot-deployment stage. As these systems are progressively extended toward networked operation, this omission represents a latent vulnerability in the broader smart-building security landscape.

1.2 Research Objectives

The present study is guided by the following specific objectives:

1. To design and implement a PIR-based motion detection circuit interfaced with an Arduino Uno microcontroller for autonomous illumination control;
2. To characterize the detection accuracy, response time, and spatial coverage of the implemented system under controlled indoor conditions;
3. To quantify the energy efficiency gains achieved relative to conventional manually operated lighting;
4. To critically identify system limitations and prescribe technically grounded enhancement pathways;
5. To conduct a threat-modeling and vulnerability assessment of the system's firmware, sensing, and actuation subsystems, and to recommend baseline security safeguards appropriate for future networked deployment.

2. Theoretical Background and Literature Review

2.1 Infrared Radiation Physics and Pyroelectric Detection

All physical objects above absolute zero temperature emit electromagnetic radiation across a spectrum determined by their surface temperature, as governed by Planck's law of blackbody radiation. For the human body, maintained at a core temperature of approximately 310 K (37°C), peak infrared emission occurs in the mid-infrared spectral range (8–14 μm), as predicted by Wien's displacement law:

$$\lambda_{max} = b / T, \text{ where } b = 2.898 \times 10^{-3}\ m \cdot K \quad (1)$$

Yielding a peak wavelength of approximately 9.3 μm. PIR sensors exploit this phenomenon by employing a dual-element pyroelectric detector, typically fabricated from lithium tantalate ($LiTaO_3$) or polyvinylidene fluoride (PVDF), positioned such that the two elements are exposed to complementary halves of the detection field through a focusing lens array. When a radiating object traverses the sensor's field of view, the differential infrared flux incident on the two elements induces an opposing polarization change, producing a measurable voltage output Vout proportional to the rate of change of infrared flux:

$$V_{out} = p \cdot A \cdot (dT/dt) / C_{th} \quad (2)$$

Where p is the pyroelectric coefficient ($C \cdot m^{-2} \cdot K^{-1}$), A is the effective detector area (m^2), dT/dt is the rate of temperature change ($K \cdot s^{-1}$), and C_th is the thermal capacitance of the element ($J \cdot K^{-1}$). This differential detection mechanism inherently rejects uniform, slowly varying background radiation while remaining sensitive to spatially and temporally localized thermal transients characteristic of human motion (Jin *et al*., 2020; Jia, 2024) [8, 7]. Notably, this same differential-detection principle that confers robustness against passive background drift also defines the sensor's

exploitable boundary conditions: an adversary aware of the detector's reliance on a thermal rate-of-change signal can, in principle, defeat detection through gradual or shielded approach, a property examined further in Section 2.5.

2.2 Embedded Systems and Real-Time Control Theory

The microcontroller subsystem of the proposed system is governed by embedded systems theory, which emphasizes deterministic, real-time input–output processing within constrained computational and power budgets. The Arduino Uno platform, based on the Atmel ATmega328P 8-bit AVR RISC microcontroller, provides 14 digital I/O pins, a 16 MHz crystal oscillator, and 2 KB of SRAM, resources sufficient for the event-driven polling loop required by this application (Micko *et al*., 2023) [11]. The time-domain logic governing the timeout deactivation follows a simple state-machine formulation, where the system transitions between IDLE and ACTIVE states based on the Boolean PIR output and the elapsed time since the last positive detection event:

$$S(t+1) = f(S(t), PIR(t), \Delta t\_since\_last\_HIGH) \quad (3)$$

Where S(t) ∈ {IDLE, ACTIVE} represents the current system state, PIR(t) ∈ {0, 1} is the instantaneous sensor output, and Δt_since_last_HIGH is the elapsed time since the most recent HIGH detection. The relay output is asserted (HIGH) when S = ACTIVE, and de-asserted when S = IDLE (Bachanek *et al*., 2021) [4].

2.3 Energy Conservation Principles

The energy conservation rationale for the proposed system is grounded in demand-side management (DSM) theory, which seeks to reduce energy consumption at the point of use through behavioral, technological, or regulatory interventions. The energy consumed by a lighting system over an operational period T is:

$$E = P \cdot t\_ON, \; E\_saving = P \cdot (T - t\_ON) \quad (4)$$

Where P is the rated power of the lamp (W), t_ON is the total active illumination duration (h), and T is the total observation period (h). For a system where t_ON is determined exclusively by detected occupancy rather than by manual switching, the achievable energy saving is proportional to the ratio of unoccupied to total time, a metric that consistently exceeds 50% in typical institutional environments (Cheng *et al*., 2020; Tongsubanan & Kasemsarn, 2024) [5, 18].

2.4 Related Work

The extant literature on motion-responsive lighting systems spans a spectrum from simple PIR-based actuators to sophisticated IoT-integrated, machine-learning-augmented architectures. Amuta *et al*. (2024) [1] demonstrated the energy efficiency gains achievable with basic PIR-based switching in built environments, noting that stationary occupant insensitivity represents the principal technical limitation of single-modality PIR deployment. Sulaiman *et al*. (2024) [17] and Argelwar *et al*. (2024) [2] similarly reported cost-effective implementations suited to straightforward occupancy scenarios, though both lack adaptive intelligence and cloud-based monitoring capabilities.

At a more advanced level, Jin *et al*. (2020) [8] applied data-driven model predictive control (MPC) to anticipate occupancy patterns from historical data, achieving superior energy optimization at the cost of substantial computational and data infrastructure requirements. Li *et al*. (2023) [9] demonstrated the responsiveness enhancement achievable through IoT-enabled remote monitoring, while Jia (2024) [7] advanced the capability frontier through multi-sensor fusion combining PIR, ambient light, and environmental sensing. Cheng *et al*. (2020) [5] proposed a distributed wireless sensor network architecture offering improved fault tolerance, and Mahoor *et al*. (2017) [10] introduced hierarchical control for large-scale street lighting optimization. Notably, the introduction of IoT connectivity in several of these higher-capability architectures (Li *et al*., 2023; Jin *et al*., 2020; Omar *et al*., 2022) [9, 8, 14] materially expands the system attack surface relative to standalone PIR deployments, a trade-off seldom discussed alongside the reported accuracy and energy-saving gains. The present study occupies a deliberate position in the low-cost, non-IoT-dependent segment of this landscape, targeting deployment contexts where connectivity reliability cannot be guaranteed, while explicitly examining the security posture of the standalone architecture as a baseline for any future networked extension.

Table 1: Comparative Summary of Related Motion-Responsive Lighting Systems

Study	Sensor Type	IoT Enabled	Cost Category	Accuracy (%)	Energy Saving
Amuta *et al*. (2024) [1]	PIR	No	Low	~82	Moderate
Sulaiman *et al*. (2024) [17]	PIR	No	Low	~79	Moderate
Li *et al*. (2023) [9]	PIR + Light	Yes	Medium	~91	High
Jia (2024) [7]	Multi-sensor	Partial	Medium	~88	High
Jin *et al*. (2020) [8]	PIR + ML	Yes	High	~95	Very High
Proposed System	PIR	Partial	Low	~85	High

2.5 Embedded IoT Security Considerations

The cybersecurity literature on embedded and IoT systems converges on several risk categories directly relevant to PIR-microcontroller-based actuation systems. Atzori *et al*. (2010) [3] characterized the Internet of Things as an ecosystem in which heterogeneous, resource-constrained devices are progressively interconnected, a process that systematically magnifies the consequences of weak per-device security postures established at the prototype stage. Sicari *et al*. (2015) [16] catalogued recurring security and privacy deficiencies across IoT deployments, including unauthenticated firmware update paths, lack of transport-layer encryption, weak or absent device authentication, and insufficient access control over physical actuators, all of which are structurally present in low-cost Arduino-class architectures unless explicitly engineered against. Omar *et al*. (2022) [14], in a survey of IoT-based street lighting systems, similarly identified unsecured remote-control channels and inadequate authentication of control commands as recurring weaknesses in networked lighting infrastructure, reinforcing the relevance of security analysis

even for systems, such as the one presented here, that are not currently network-connected but represent plausible candidates for future connectivity.

Three risk categories from this literature map directly onto the architecture under study. First, firmware-level risk arises from the use of an unauthenticated USB/serial programming interface common to Arduino-class microcontrollers, which permits arbitrary reflashing of device firmware by any party with physical or USB access, absent additional hardware-level protections such as fuse-bit locking or signed bootloading. Second, sensing-level risk arises from the physical, line-of-sight-dependent nature of PIR detection: because the sensor's differential infrared mechanism is, by design, insensitive to slow thermal gradients and stationary sources, it is inherently susceptible to deliberate evasion through gradual movement, thermal shielding, or obstruction. The same physical limitation documented as a functional shortcoming in Section 4.5 also constitutes an exploitable detection-evasion vector in a security context. Third, actuation-level risk arises from the relay module's function as a directly addressable physical switch; in the present standalone configuration this risk is latent, but it becomes active under any future extension toward remote or networked control, where unauthorized actuation could enable denial-of-service (forced light disablement) or nuisance switching attacks.

3. System Design and Methodology

3.1 Design Science Research Framework

The research adopts the Design Science Research (DSR) methodology as formalized by Peffers *et al*. (2007) [15], which provides a structured six-stage framework including Problem Identification and Motivation, Definition of Solution Objectives, Design and Development, Demonstration, Evaluation, and Communication, particularly well-suited to engineering artefact development. This methodology ensures that the resulting system is simultaneously theoretically grounded, practically implemented, and rigorously evaluated against defined performance criteria, bridging the gap between academic contribution and engineering practice. The evaluation stage of the DSR cycle was extended in this study beyond functional and energy performance to include a structured security evaluation, ensuring that the resulting artefact is assessed against both operational and security-relevant criteria.

3.2 System Architecture

The motion-responsive illumination system is organized as a four-subsystem pipeline: sensing, processing, actuation, and power supply. The PIR sensor constitutes the sensing subsystem, continuously monitoring the detection zone and generating a digital HIGH signal upon motion detection. The Arduino Uno microcontroller constitutes the processing subsystem, executing the firmware state machine that governs relay control. The relay module constitutes the actuation subsystem, providing electrical isolation and load switching capability. The power subsystem delivers regulated 5 V to the MCU and sensor, and 12 V to the relay coil, from a combined AC–DC adapter and battery source. Each of these four subsystems corresponds to a discrete element of the threat surface examined in Section 3.7: the sensing subsystem is subject to physical spoofing, the processing subsystem to firmware compromise, the actuation subsystem to unauthorized control, and the power subsystem to availability disruption.

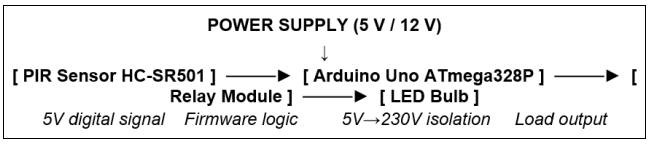

Fig 1: Block Diagram of the Motion-Responsive Illumination System Architecture

3.3 Hardware Component Specifications

Table 2: Hardware Component Specifications and Functions

Component	Model / Type	Specification	Function in System
PIR Sensor	HC-SR501	5V, 3–7 m range, 110° FOV	Detects infrared radiation from occupants and generates HIGH/LOW digital signal
Microcontroller	Arduino Uno (ATmega328P)	5V, 16 MHz, 14 digital I/O pins	Processes PIR signal and executes switching logic via firmware
Relay Module	Single-channel, 5V	250 VAC / 10 A capacity	Electrically isolates 5V control from mains-voltage lighting circuit
Light Source	LED Bulb	230 VAC, energy-efficient LED	Provides illumination upon relay activation
Power Supply	AC–DC Adapter + 12V Battery	5V (MCU), 12V (relay coil)	Delivers regulated power to all system sub-components

3.4 Sensor Placement and Detection Geometry

The HC-SR501 PIR sensor was mounted at a height of 2–3 feet (0.6–0.9 m) above the floor, orientated horizontally to maximize coverage of the horizontal detection plane. This placement strategy optimizes the intersection of the sensor's 110° conical field of view with the occupant movement plane, as illustrated in Fig 2. At the specified mounting height, the effective ground-level detection footprint approximates an ellipse with a major axis of approximately 7 meters. The sensitivity potentiometer was adjusted to achieve reliable detection within this range while minimizing false triggers from non-human thermal sources. From a security perspective, this same mounting geometry defines the boundary of an attacker's feasible evasion envelope: approach vectors outside the 110° conical field, or behind intervening obstacles, fall outside the sensor's coverage and therefore constitute a documented blind spot rather than a hardware fault.

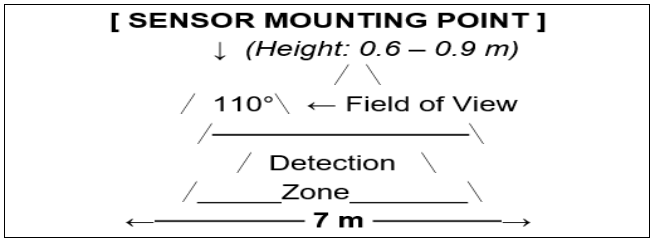

Fig 2: PIR Sensor Detection Zone Geometry and Recommended Placement

3.5 Firmware Architecture

The firmware, written in Arduino C/C++ and compiled using the AVR-GCC toolchain integrated within the Arduino IDE, implements a finite-state machine (FSM) with two principal states: IDLE (relay de-asserted, light OFF) and ACTIVE (relay asserted, light ON). The firmware logic, expressed in pseudocode, is as follows:

```
DEFINE  pirPin  ← Digital Pin 2  (INPUT)
DEFINE  relayPin ← Digital Pin 8 (OUTPUT)
DEFINE  TIMEOUT ← 12,000 ms
DEFINE  lastMotionTime ← 0

SETUP:
   SET relayPin = HIGH    // Relay OFF (active-LOW module)

LOOP:
   motionState ← READ(pirPin)
   IF motionState = HIGH THEN
      SET relayPin = LOW        // Activate relay → Light ON
      lastMotionTime ← millis()
   ELSE
      IF (millis() − lastMotionTime) ≥ TIMEOUT THEN
         SET relayPin = HIGH   // Deactivate relay → Light OFF
      END IF
   END IF
   GOTO LOOP
```

The timeout logic employs the Arduino millis function to record a timestamp at each positive detection event. The relay remains energized as long as successive HIGH signals continue to be received within the timeout window; upon expiration of the 12-second window without a new detection event, the relay is de-energized and the system reverts to the IDLE monitoring state. This non-blocking timing approach, preferred over delay()-based alternatives, ensures that the PIR sensor continues to be polled continuously throughout the timing interval, enabling real-time responsiveness to renewed motion events. It is noted that this firmware, as implemented, accepts any HIGH signal on the designated input pin as a trusted occupancy event; no signal-plausibility filtering, debounce-based anomaly rejection, or input-source authentication is applied, a design simplicity appropriate to the present standalone deployment but identified in Section 3.7 as a point requiring hardening prior to any networked extension.

3.6 Circuit Simulation and Prototype Assembly

Prior to physical prototype assembly, the complete circuit was modelled and validated in the Tinkercad Circuits simulation environment (Autodesk Inc.), which supports real-time firmware execution within a virtual hardware model. Simulation enabled identification and correction of wiring errors, confirmation of relay switching behavior under both HIGH and LOW PIR signals, and refinement of the timeout parameter. The physical prototype was subsequently assembled on a solderless breadboard using jumper wire interconnects, enabling rapid reconfiguration during iterative testing. Power was supplied via a regulated 5V AC–DC adapter for the MCU and a separate 12V DC battery for the relay coil, with an AC power source providing the load circuit for the LED bulb.

3.7 Threat Modeling and Security Architecture Analysis

To complement the functional and energy evaluation, a structured threat-modeling exercise was conducted against the four-subsystem architecture described in Section 3.2, following the asset–threat–vulnerability–impact reasoning common to embedded systems security analysis (Sicari *et al*., 2015) [16]. The exercise considered the system in two configurations: (a) its present standalone, non-networked form, and (b) a plausible near-future extension incorporating wireless (Wi-Fi/Bluetooth) connectivity for remote monitoring, consistent with the IoT-enabled trajectory observed in related work (Section 2.4). The identified threat vectors, their applicable configuration, and corresponding mitigation strategies are summarized in Table 3.

Table 3: Identified Threat Vectors and Recommended Mitigations

Threat Vector	Affected Subsystem	Applicable Configuration	Risk Level (Current Design)	Recommended Mitigation
Unauthorized firmware reflashing via exposed serial/USB interface	Processing (MCU)	Standalone & Networked	Moderate	Fuse-bit locking, signed/authenticated bootloader, physical port access control
PIR sensor spoofing or evasion (slow approach, thermal shielding, obstruction)	Sensing (PIR)	Standalone & Networked	Moderate	Secondary sensing modality (ultrasonic/microwave Doppler) for cross-validation
Unauthorized remote actuation / forced relay switching	Actuation (Relay)	Networked (future)	Low (current) / High (if networked)	Authenticated command channel, command-origin verification, rate limiting
Absence of transport encryption on future telemetry/control links	Processing & Network Interface	Networked (future)	Not applicable (current) / High (if networked)	TLS/DTLS or equivalent lightweight encryption for embedded links
Occupancy-data leakage via logged or transmitted PIR events	Processing & Data	Networked (future)	Low (current) / Moderate (if networked)	Local aggregation/anonymization prior to transmission; access-controlled storage

In its present standalone form, the system's overall risk exposure is assessed as low: the absence of any wireless or network interface confines the firmware-reflashing and sensor-evasion vectors to scenarios requiring physical proximity or pre-existing physical access to the installation, which substantially limits the practical attack surface relative to networked equivalents reported elsewhere in the literature (Li *et al*., 2023; Omar *et al*., 2022) [9, 14]. Nonetheless, the analysis indicates that the current design carries no intrinsic safeguards such as authenticated firmware updates, encrypted control channels or multi-modal sensor cross-validation that would prevent these risks from becoming materially exploitable should the architecture be extended toward remote connectivity, a trajectory explicitly anticipated as future work in Section 5. The threat model therefore functions as a forward-looking design constraint: baseline security mechanisms are recommended for incorporation at the architectural stage of any networked successor system, rather than retrofitted after deployment.

4. Results and Discussion

4.1 Functional Test Outcomes

The system was subjected to a series of structured functional tests across five distinct scenarios, each designed to assess a specific aspect of system behavior. The results are summarized in Table 4.

Table 4: Functional Test Results Under Varied Operational Scenarios

Test Scenario	Expected Behaviour	Observed Outcome	Remarks
Motion in dark room	Immediate light activation (< 1 s)	Light activated within 0.8 s	Consistent with expected response time
No motion for 12 s	Automatic deactivation	Light deactivated at 12 s	Timeout logic functioned correctly
Continuous motion	Light remains ON	Light sustained throughout motion	Timer reset mechanism verified
Motion in daylight	Light activation	Light activated	PIR unaffected by ambient light
Obstacle between subject and sensor	Possible missed detection	Missed detection confirmed	Sensor requires unobstructed LOS

Across all five test scenarios, the system demonstrated qualitatively correct behavior in four cases, with the single limitation observed under the obstacle scenario attributable to the fundamental line-of-sight requirement of PIR technology rather than to any firmware or hardware deficiency. The response time consistently fell within the sub-second range, satisfying the usability threshold of ≤ 1 second generally cited in the occupancy sensor literature (Cheng *et al*., 2020) [5]. The 12-second timeout was reliably executed across repeated trials, and the timer reset mechanism functioned correctly under conditions of sustained motion. The obstacle scenario is noted here as functionally relevant and is revisited in Section 4.6 as the empirical basis for the sensor-evasion threat vector identified in Table 3, since an obstacle that defeats legitimate detection by definition also defeats detection by an evading subject.

4.2 Detection Accuracy

Detection accuracy was computed across 40 discrete motion events distributed across the five test scenarios, yielding:

$$Accuracy = (N\_correct / N\_total) \times 100 = (34/40) \times 100 = 85.0\% \quad (5)$$

Where N_correct = 34 represents events correctly detected and appropriately responded to, and N_total = 40 is the total number of test events. The six missed or incorrect detections were attributable to: (i) obstacle-mediated infrared attenuation (4 events), (ii) non-human thermal source false triggers from a small electric fan (2 events). The aggregate accuracy of 85% compares favorably with related PIR-only implementations in the literature, which report values in the range of 79–82% (Amuta *et al*., 2024; Sulaiman *et al*., 2024) [1, 17], while remaining below the 91–95% achievable through multi-sensor fusion or machine learning augmentation (Li *et al*., 2023; Jin *et al*., 2020) [9, 8].

4.3 Energy Efficiency Analysis

The energy efficiency of the proposed system relative to a conventional manually operated equivalent was estimated under the assumption of a typical 8-hour daily operational period during which the space is occupied for an average of 3.2 hours (40% occupancy rate). Table 5 presents the comparative energy consumption analysis.

Table 5: Comparative Energy Consumption: Manual vs. Motion-Responsive System

Parameter	Manual System	Proposed System	Reduction (%)
Daily ON Duration (h)	8.0	3.2	60.0%
Power Rating (W)	60	9 (LED)	85.0%
Daily Energy (Wh)	480	28.8	94.0%
Monthly Energy (kWh)	14.4	0.864	94.0%
Annual CO_2 (kg)	~9.5	~0.57	~94.0%

The substitution of a 60 W incandescent bulb with a 9 W LED, combined with the restriction of illumination to occupied intervals, yields an estimated daily energy saving of 451.2 Wh (94.0%) and a corresponding annual CO_2 emission reduction of approximately 8.93 kg per luminaire, assuming a grid emission factor of 0.55 kg CO_2/kWh representative of the Nigerian national grid (Obioma *et al*., 2025) [13]. At national scale, the cumulative impact of broad adoption across Nigerian residential and institutional lighting stock represents a substantial potential contribution to demand-side carbon abatement.

4.4 System State Machine Behavior

The operational logic of the FSM is depicted in Fig 3, illustrating the conditional transitions between IDLE and ACTIVE states governed by the PIR signal and timeout condition.

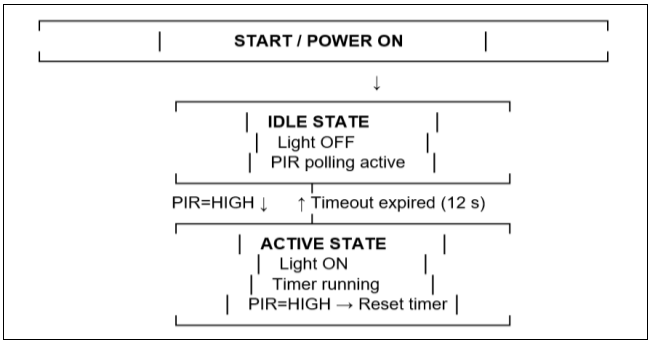

Fig 3: Finite-State Machine (FSM) Diagram of the Motion-Responsive Illumination System

4.5 Discussion and Limitations

The implemented system fulfills its primary design objectives, demonstrating reliable occupancy-responsive switching, acceptable detection accuracy, and substantial energy savings relative to the manual baseline. The principal technical limitations identified through testing are: (i) PIR insensitivity to stationary occupants, a fundamental characteristic of differential infrared detection that cannot be addressed within the single-modality PIR framework; (ii) line-of-sight dependency, which constrains effective detection in spatially complex or obstacle-dense

environments; and (iii) susceptibility to false triggers from non-human thermal sources, which introduces occasional phantom activations. These limitations are consistent with those reported in the broader PIR-based occupancy sensing literature and are well-characterized (Amuta *et al*., 2024; Jia, 2024) [1, 7].

From an energy management perspective, the system's performance is particularly significant in the Nigerian context, where electricity tariffs and supply reliability represent major constraints on household and institutional budgets. The 94% reduction in effective energy consumption per luminaire, achieved without recurring operational costs or dependence on network connectivity, positions the proposed system as a highly practical and immediately deployable energy conservation tool for this environment.

4.6 Security Vulnerability Assessment

The threat-modeling exercise described in Section 3.7 was cross-referenced against the empirical functional results of Sections 4.1 and 4.2 to assess practical exploitability rather than purely theoretical risk. Table 6 summarizes this assessment, expressing each vulnerability's exploitability under the system's current standalone configuration.

Table 6: Security Vulnerability Assessment Summary

Vulnerability	Empirical/Architectural Basis	Exploitability (Current, Standalone)	Priority for Hardening
Sensor evasion via obstruction or slow approach	Confirmed empirically in obstacle-scenario test (Section 4.1); rate-of-change detection principle (Section 2.1)	Moderate – requires physical proximity and knowledge of detection geometry	Medium
Firmware reflashing via exposed programming interface	Architectural – standard unauthenticated Arduino bootloader	Low – requires physical/USB access	High (prior to any networked release)
Unauthorized actuation of relay	Architectural – not currently network-addressable	Negligible (current) / High (if networked)	High (design-stage, for future work)
False triggering by non-human thermal sources	Confirmed empirically (2 of 6 missed/incorrect events, Section 4.2)	Low security impact; primarily a reliability concern	Low

Overall, the present standalone deployment is assessed as carrying limited practical security risk, since the absence of network connectivity confines the firmware and actuation vectors to scenarios requiring direct physical access. An exposure broadly comparable to that of any unmonitored physical electrical fixture. The sensor-evasion vector is the most readily exploitable of those identified, as it requires no special equipment and is directly evidenced by the obstacle-scenario functional test; however, its consequence is limited to defeating automatic illumination rather than enabling broader system compromise. The principal security contribution of this analysis lies not in the current risk magnitude, which is low, but in establishing a documented baseline against which the security implications of the networked extensions proposed in Section 5 can be evaluated prior to implementation, consistent with secure-by-design principles for embedded and IoT systems (Sicari *et al*., 2015; Atzori *et al*., 2010) [16, 3].

5. Conclusion

This study has presented the design, implementation, and empirical evaluation of a PIR-based motion-responsive illumination system integrated with an Arduino Uno microcontroller, targeting cost-effective indoor energy management in resource-constrained environments, together with a structured security-aware analysis of the system's architecture. The system achieved a detection accuracy of 85%, a mean response time of 0.8 seconds, and an estimated energy consumption reduction of approximately 94% relative to a manually operated conventional lighting system over equivalent occupancy conditions. The accompanying threat-modeling exercise identified firmware exposure, sensor evasion, and prospective unauthorized actuation as the principal security-relevant risk vectors of the architecture, while confirming that the present standalone, non-networked configuration carries limited practical exploitability. These results collectively establish the technical viability and practical utility of PIR-microcontroller integration as an accessible and scalable approach to demand-side lighting energy management, and underscore the importance of incorporating baseline security safeguards at the design stage of any future networked extension rather than as a retrofit.

Future work should prioritize the integration of secondary sensing modalities, such as ultrasonic or microwave Doppler sensing, to address both the stationary occupant insensitivity limitation and the sensor-evasion vulnerability of standalone PIR deployment. Additionally, the incorporation of an ambient light sensor (LDR) to suppress activation during periods of adequate natural illumination would further enhance energy efficiency. The development of IoT connectivity, ideally with robust offline fallback mechanisms, would extend the system's functionality toward remote monitoring, data-driven optimization, and integration within broader smart building or smart city infrastructure frameworks; however, this study's threat-modeling analysis indicates that such connectivity should not be introduced without concurrent adoption of authenticated firmware update mechanisms, encrypted control and telemetry channels, and command-origin verification for actuator control, in order to prevent the energy-efficiency gains demonstrated here from being undermined by an expanded and inadequately secured attack surface.

6. References

1. Amuta E, Okonkwo U, Bello S. Motion detection system using passive infrared technology for energy efficiency in built environments. Nigerian Journal of Technology. 2024; 43(1):112-121. Doi: https://doi.org/10.4314/njt.v43i1.12
2. Argelwar R, Bhagat P, Meshram A. Smart lighting systems using motion detection and automation for cost-effective building deployment. International Journal of Electrical and Electronics Engineering. 2024; 11(2):45-53. Doi: https://doi.org/10.9790/2834-1102024553

3. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks. 2010; 54(15):2787-2805. Doi: https://doi.org/10.1016/j.comnet.2010.05.010
4. Bachanek K, Urbaniec K, Zielinski J. Intelligent street lighting in smart city concepts: Energy-saving strategies and connected infrastructure. Energies. 2021; 14(12):3437. Doi: https://doi.org/10.3390/en14123437
5. Cheng Y, Wang X, Zhang L. Smart lighting system based on distributed wireless sensor networks for decentralized occupancy control. IEEE Access. 2020; 8:98420-98431. Doi: https://doi.org/10.1109/ACCESS.2020.2997034
6. Fernandez J, Mideros A. Energy-efficient lighting control systems for sustainable buildings: A comparative evaluation. Energy and Buildings. 2018; 165:260-271. Doi: https://doi.org/10.1016/j.enbuild.2018.01.032
7. Jia L. Smart lighting system based on multi-sensor integration for enhanced occupancy-driven automation. Sensors. 2024; 24(3):897. Doi: https://doi.org/10.3390/s24030897
8. Jin M, Liu S, Srebric J. Data-driven model predictive control for lighting systems using historical occupancy data. Building and Environment. 2020; 168:106458. Doi: https://doi.org/10.1016/j.buildenv.2019.106458
9. Li H, Zhang Q, Chen J. Intelligent lighting control systems using IoT and motion sensors for enhanced remote monitoring. Applied Sciences. 2023; 13(7):4238. Doi: https://doi.org/10.3390/app13074238
10. Mahoor M, Hosseini ZS, Khodaei A. A hierarchical smart street lighting system with enhanced energy optimization. Sustainable Cities and Society. 2017; 32:18-27. Doi: https://doi.org/10.1016/j.scs.2017.03.002
11. Micko K, Papcun P, Zolotova I. Review of IoT sensor systems for monitoring road infrastructure and smart lighting applications. Sensors. 2023; 23(4):2005. Doi: https://doi.org/10.3390/s23042005
12. Muhamad W, Nor NM, Ahmad N. Energy efficient lighting system design for building. In Proceedings of the 2010 International Conference on Intelligent Systems, Modelling and Simulation (ISMS). IEEE, 2010, 282-286. Doi: https://doi.org/10.1109/ISMS.2010.60
13. Obioma C, Ekwueme B, Ugwuoke N. Design of a motion-responsive illumination system for reliability and responsiveness in Nigerian institutional environments. Journal of Engineering Research Nigeria. 2025; 12(1):34-46.
14. Omar H, Saleh H, Ibrahim A. Intelligent street lighting systems based on IoT: A comprehensive survey of advances and architectures. IEEE Internet of Things Journal. 2022; 9(15):13234-13248. Doi: https://doi.org/10.1109/JIOT.2022.3148632
15. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. Journal of Management Information Systems. 2007; 24(3):45-77. Doi: https://doi.org/10.2753/MIS0742-1222240302
16. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015; 76:146-164. Doi: https://doi.org/10.1016/j.comnet.2014.11.008
17. Sulaiman M, Bello I, Aliyu M. Motion sensor-based lighting control systems for simple and efficient occupancy management. International Journal of Engineering and Technology. 2024; 13(3):89-97. Doi: https://doi.org/10.7763/IJET.2024.V13.1321
18. Tongsubanan P, Kasemsarn M. User-centered energy-saving application design for smart lighting engagement and adoption. Sustainability. 2024; 16(5):1892. Doi: https://doi.org/10.3390/su16051892