Solar-Powered Smart Guard: Autonomous Lighting, Intrusion Detection, and Surveillance Network

Mark Edisol M. Asistio , Nayeff L. Dingding , Mark Dennis L. Larioza , Janine P. Natalia , Janette Grace N. Siervo, Engr. Minerva C. Zoleta

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

DOI: https://doi.org/10.47772/IJRISS.2026.10100217

Received: 17 January 2026; Accepted: 23 January 2026; Published: 31 January 2026

ABSTRACT

To address the increasing needs of sustainable and active security options, this research paper proposes the creation of the Solar-Powered Smart Guard which is an autonomous surveillance system that is capable of working without the electrical system. The conventional security systems tend to be affected by dependency on constant power and passive recording functions, which make them useless during downtimes or need to be monitored manually. The proposed project will overcome these shortcomings by incorporating PIR motion sensors, IoT connectivity, and a solar powered energy harvesting system into the Arduino Uno and ESP32-CAM. The system uses sensor fusion algorithms to remove noise in the environment which is a huge filter and the false alarms are minimized and the correct intrusion detection is made. After checking the movement, the device will automatically activate local deterrence by using high-intensity floodlights and audible alarms and also send real-time email alerts and photographic alerts to the user over a GSM network.

The results of the tests ensured the capability of the system to support 24/7 autonomous functioning because of its Maximum Power Point Tracking (MPPT) charging circuit and ensured a high percentage of passing the tests in the differentiation between human movement and the environmental stimuli. The Solar-Powered Smart Guard is an effective product that offers a low cost, power saving and self sustaining alternative to traditional perimeter security.

Keywords: Motion Detection, Solar/Off-Grid, IoT Alerts, WSN/Tracking

INTRODUCTION

In an era of booming technology and urbanization, security is a necessary component of human existence. However, the current industry standard for facility protection, traditional Closed Circuit Television (CCTV) systems have critical limitations in function. While great for documenting, most traditional security arrangements are reactive in nature; the security is intended to capture the documentation of a crime either after it has happened, rather than actually preventing the breach from occurring in real time. This 'passive surveillance' model results in high-latency responses, where the damage or theft is often completed long before authorities or property owners can intervene.

Furthermore, existing security infrastructures have a major single point of failure: the fact that they are heavily reliant upon the commercial power grid. In developing regions where power fluctuations, brownouts and load shedding are common occurrences, standard security systems become a liability instead of an asset. In remote agricultural, construction site and off grid locations where there is no steady electricity supply, this weakness is further compounded. Criminals have used this dependency because they are known to turn off power lines to cripple monitoring systems before committing any criminal acts. The overdependence on perpetual power of the electricity and the system of constant hand monitoring exposes an unsafe vulnerability lapse, in other words, power goes off, security is gone.

To overcome these systemic flaws, this research aims at developing the "Solar Powered Smart Guard: Autonomous Lighting, Intrusion Detection, and Surveillance Network." This project is an integrated embedded system that combines the sustainability of renewable energy and the intelligence of Internet of Things (IoT).

The Smart Guard is designed to be energy independent and defended unlike the traditional system which is passive. By using a separate sensor fusion algorithm that cross checks data to ensure the human presence, the system reduces false alarms and instantly activates on-site local deterrence mechanisms (such as high intensity floodlights and audible alarms). This is an approach that psychologically startles intruders and halts unauthorized access, before material lost, while running completely off grid. The result is a self sustaining security node assuring continuous protection, regardless of the condition of the main electrical supply.

Importance and Relevance of the Study

The contemporary landscape of facility management, security is always a top concern; however, more traditional methods of surveillance are often not an effective means of addressing the dual challenges of energy reliability and proactive deterrence. Standard Closed-Circuit Television systems (CCTV) are largely reactive, intended to document incidents rather than prevent them, and have the major drawback of being critically dependent on the commercial power grid. This reliance issues a massive vulnerability gap especially in developing regions or in agricultural sites in remote areas of the hemisphere where the fluctuation of power is common making security infrastructure useless when power fails. Consequently, there is an urgent need from an engineering perspective for a paradigm shift from passive, grid dependent, monitoring through grid security into active autonomous security systems that can operate reliably in an off-grid environment.

To overcome these disadvantages, this study presents the "Solar-Powered Smart Guard" which is an embedded system that combines renewable energy harvesting technology with the Internet of Things (IoT) technology to form a self-sustaining security network. By using Maximum Power Point Tracking (MPPT) for effective solar charging, combined with the sensor fusion algorithms for the Passive Infrared (PIR) data analysis, the detection of an intrusion or non-intrusion from environmental noise discrimination is determined with high accuracy. This not only covers 24 by 7 autonomous operation but also provides the device with the ability to carry out immediate local deterrence (turning on high intensity lighting and audible alarms) and simultaneously send real time alert to user via GSM and represents the bridging of the gap between Energy efficient and Active facility protection situation.

The relevance of this study is not only confined to the immediate security application, but also has a large impact on the field of Green IoT and edge computing. By showing that high-level security operations can be performed on low-power microcontrollers, without access to cloud processing or wired electricity, the project has a scalable solution for remote communities, agricultural assets and even construction sites to be secured. Furthermore, it makes it worth mentioning the feasibility of substitution of traditional, energy-hungry security appliances with sustainable solutions, which will diminish carbon footprint of vital infrastructure without compromising any aspect of security through power instability.

REVIEW OF RELATED LITERATURE

In the present chapter an overall and holistic literature review is covered, targeting the critical joins of Motion Detection technologies, Solar/Off-Grid energy infrastructures, Internet of Things (IoT) based alert systems and Wireless Sensor Networking (WSN). The main goal of this review is to lay the groundwork of a good theoretical and technical background for the current investigation. By analysing existing pieces of work in the field critically, the researchers hope to deconstruct the underlying mechanism through Passive Infrared (PIR) sensing, analyse the effectiveness of sustainable power management strategies and assess the reliability of IoT protocols in real-time remote communication.

Beyond the theoretical aspects, this chapter examines such practical studies along with empirical data which validate the effectiveness of these technologies in real-life scenarios. Special attention is devoted to the operational reliability of PIR sensors with regards to activate immediate security actions and technical feasibility of using solar energy harvesting to provide autonomous operation in environments where there is no connectivity to the grid. These studies are the evidence that is needed to support the shift from traditional, grid systems of dependent surveillance to self-sustaining, active deterrence systems.

Therefore, the following parts summarize these findings and use them in the architectural layout of the "Solar-Powered Smart Guard" (Asistio et al., Proposed). This review has not only drawn attention on benchmarks set by previous innovations but also speculated individual technological gaps such as the necessity for integrated visual verification and active deterrence that the current study attempts to address. By describing these relevant strategies, this chapter provides the overall blueprint for the achievement of the peculiar objectives of the proposed system.

Motion Detection

The usage of Passive Infrared (PIR) sensors is still a staple in automated security research because of its effectiveness in detecting human presence. Sushmasri et al. (2025) have shown the usefulness of PIR sensors in particular, in detecting human presence and activating local outputs such as lights and alarms to provide a direct relationship between detection and deterrence. Building on this, Abirami et al. (2018) and Abiodun et al. (2025) used PIR triggers to activate camera modules with a particular focus, in this case, on covert camera triggers to capture intruder evidence discreetly. To solve the reliability issue, Verma et al. (2025) targeted the accuracy of PIR detection and the coverage areas and Surantha et al. (2018) combined PIR triggers with recognition systems to increase the security intelligence. These studies support the approach of Asistio et al. (Proposed) which uses PIR detection not only for mere motion detection, but as a two-trigger for both presence verification and intrusion response.

Solar/Off-Grid

Sustainable operation is essential for security systems that are being used in remote regions or in areas without access to a grid. Abiodun et al. (2025) achieved the successful implementation of a security system coupled with both solar energy and rechargeable batteries to demonstrate the feasibility of off-grid surveillance, which does not require mains electricity. This literature directly relates to the methodology of the current study by Asistio et al. aimed at the development of a fully solar powered system with battery backup, so that security functions (such as lighting and alert) can be maintained in the event of power failure or at locations without infrastructure.

IoT Alerts

The transition from local alarm systems employing powerful videos to remote monitoring systems, all active, is a major trend in recent studies. Abirami et al. (2018) and Verma et al. (2025) identified the effectiveness of using GSM and IoT modules to send immediate SMS and email notifications on detection and the user is aware of the detection irrespective of his/her physical location. Furthermore, Sahoo et al. (2018) and Surantha et al. (2018) extended this concept and utilized cloud-based updates and apps to provide real-time alerts. These findings form the technical background for the current project by Asistio et al. that implements real-time alerts with evidence of images or videos, which increases the user's ability to verify and react to threats remotely.

WSN/Tracking

Wireless Sensor Networks (WSN) do not limit monitoring to just a point detection. Jisha et al. (2015) discussed on using PIR sensors which are distributed on a number of sensor nodes, to not only detect presence but also to track path of movement of an intruder. Similarly, Sun et al. (2020) used WSN frameworks for distinguishing and tracking the approaching persons or vehicles. These methodologies are relevant to the proposed system by Asistio et al., designed to assist in the distributed wireless nodes, and allow creating a broader and smarter surveillance network for tracking the patterns of intrusion throughout a facility.

Table 1.

Study	Sensors Used	Controller	Main Outputs	Scope	Key Features	Gap Addressed by This Study
Sushmasri et al. (2025)	PIR Sensor	Arduino	Lights, Audible Alarms	Local Security	Automates lighting and security alarms	Lacks remote IoT notification and visual

					upon detecting motion.	evidence capture.
Abirami et al. (2018)	PIR Sensor	Microcontroller	Camera, SMS, Email	IoT Security	Integrates motion detection with camera capture and GSM/IoT alerts.	Does not integrate solar sustainability or visual verification.
Jisha et al. (2015)	PIR Sensor	WSN Nodes	Intruder Tracking Data	Wireless Sensor Network (WSN)	Uses multiple wireless nodes to track the *movement path* of an intruder.	Focuses on tracking algorithms rather than active deterrence or power autonomy.
Surantha et al. (2018)	PIR Sensor, Camera	Raspberry Pi / IoT	Camera Stream, Cloud Alerts	Smart Home	Uses algorithms to *recognize* objects/faces and update cloud dashboards.	High cost and power consumption (Raspberry Pi); relies on stable internet/cloud.
Saranu, Abirami et al. (2018)	PIR Sensor	Microcontroller	Theft Alert	Theft Detection	Focuses on detecting theft events and triggering basic alerts.	Does not integrate solar sustainability or visual verification..
Abiodun et al. (2025)	PIR Sensor	Microcontroller	Covert Camera	Solar/Off-G rid	Solar-driven system focused on *spy* (covert) detection.	Focuses on *hiding* the security (spy) rather than *active deterrence* (floodlights/loud alarms).
Verma et al. (2025)	PIR Sensor	(Sensor Focus)	SMS, Email	Sensor Optimizati o n	Focuses purely on enhancing the sensitivity and range of the PIR component.	Improves the sensor itself but lacks a complete, integrated system (Alerts + Solar + Logic).
Sun et al. (2020)	PIR Sensor	WSN Nodes	Tracking Data	Advanced WSN	Distinguishes between approaching persons and vehicles; tracks direction.	Highly complex WSN setup that may betoo costly/complex for simple facility protection.
Sahoo et al.	PIR Sensor	IoT	App	Remote	Detects intrusion	Lacks the

(2018)		Controller	Notificatio ns	Monitoring	and transmits status to the user via IoT.	physical deterrence mechanisms (Floodlight/Sire n) found in our system.
Nayak et al. (2018)	PIR Sensor, Camera	Raspberry Pi	Surveillanc e Monitor	Smart Surveillanc e	Uses Raspberry Pi for robust monitoring and surveillance.	High power requirement makes it difficult to run purely on small-scale solar setups.

METHODOLOGY

In the solar-powered smart guard, renewable energy source extraction, integrated sensing mechanism, and wireless communication element architecture are integrated. The system is modeled as an event-driven control system in which inputs from the environment are processed to make the autonomous security outputs. The device has a modular hardware platform focusing on the Arduino Uno and integrates it with an ESP32-CAM to perform visual processing.

Enclosure and Deployment: The mechanical design is based on a rugged and weather popular architecture installed in the junction box of IP66. Unlike normal indoor security units, the system is totally self-contained. The mechanical setup has a pole mounted bracket system, the solar panel is at an angle between 15deg to 30deg to allow maximum sun exposure, and the sensor dome and camera lens sit at the vertical face allowing for an optimal field of view.

Energy Harvesting and Regulation: To interface the solar input to that of storage system the CN3791 MPPT (Maximum Power Point Tracking) module is used. This module draws variable power from the photovoltaic panel to efficiently charge the 3x 18650 Lithium-Ion battery bank to ensure the system can operate independently from the grid. The Arduino is used in the control to monitor voltage level so that deep discharge can be avoided and to regulate the active and sleep states of the system.

Sensor Array: Perception is achieved through specific environmental sensing modules:

- Detection: An HC-SR501 Passive Infrared (PIR) sensor is mounted on the front chassis. It detects differential thermal signatures (human body heat) against the background temperature to identify potential intruders.
- Surveillance: An ESP32-CAM module serves as the visual verification unit. Upon receiving a logic signal from the main controller, it wakes from deep sleep to capture photographic evidence of the event.

Human-Machine Interface (HMI): The system utilizes a dual-interface approach. Locally, a Piezo Electric Buzzer and High-Intensity Floodlight provide immediate physical feedback to deter intruders. Remotely, the SIM800L GSM Module acts as the user dashboard, delivering real-time logic states and alerts directly to the user's mobile device via SMS.

Software Implementation: The control logic is developed in C++ within the Arduino IDE. The software architecture utilizes a non-blocking loop structure, employing internal timers rather than delay() functions to manage the GSM transmission and sensor polling simultaneously without halting the intruder detection logic.

The detection algorithm implements a "Smart Filtering" strategy combined with Day/Night logic. The decision hierarchy is prioritized as follows:

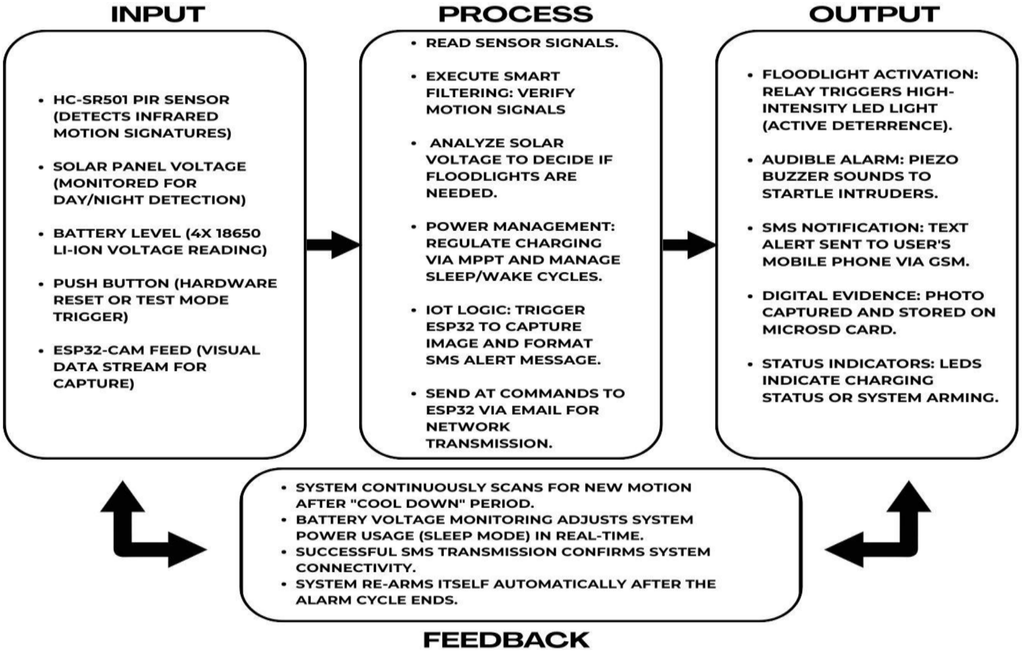
- Initial Motion Analysis: The system first monitors the PIR sensor pin. If a signal is triggered (HIGH):

- ○ Signal Verification: The software executes a "Double-Check" routine, waiting 200 milliseconds to confirm the signal remains HIGH. This filters out momentary noise caused by wind or

  fast-moving debris.

- Environmental Context: Once motion is verified, the system checks the ambient light levels (Day vs. Night).
  - ○ Day Mode: If sunlight is detected, the system executes a "Silent Alert" routine—triggering the ESP32 to capture an image and the GSM module to send an SMS notification, without activating the floodlight.
  - ○ Night Mode: If darkness is detected, the system executes the full "Active Deterrence" routine—simultaneously activating the relay-controlled Floodlight and the Audible Alarm while transmitting the remote alerts.
- Reset and Recovery: After the deterrence cycle is complete, the system enters a "Cool Down" state for 10 seconds to allow the intruder to leave before resetting the sensors for the next trigger event.

Figure 1. Input–Process–Output (IPO) Model


INPUT
• HC-SR501 PIR SENSOR (DETECTS INFRARED MOTION SIGNATURES)
• SOLAR PANEL VOLTAGE (MONITORED FOR DAY/NIGHT DETECTION)
• BATTERY LEVEL (4X 18650 LI-ION VOLTAGE READING)
• PUSH BUTTON (HARDWARE RESET OR TEST MODE TRIGGER)
• ESP32-CAM FEED (VISUAL DATA STREAM FOR CAPTURE)
PROCESS
• READ SENSOR SIGNALS.
• EXECUTE SMART FILTERING: VERIFY MOTION SIGNALS
• ANALYZE SOLAR VOLTAGE TO DECIDE IF FLOODLIGHTS ARE NEEDED.
• POWER MANAGEMENT: REGULATE CHARGING VIA MPPT AND MANAGE SLEEP/WAKE CYCLES.
• IOT LOGIC: TRIGGER ESP32 TO CAPTURE IMAGE AND FORMAT SMS ALERT MESSAGE.
• SEND AT COMMANDS TO ESP32 VIA EMAIL FOR NETWORK TRANSMISSION.
OUTPUT
• FLOODLIGHT ACTIVATION: RELAY TRIGGERS HIGH-INTENSITY LED LIGHT (ACTIVE DETERRENCE).
• AUDIBLE ALARM: PIEZO BUZZER SOUNDS TO STARTLE INTRUDERS.
• SMS NOTIFICATION: TEXT ALERT SENT TO USER'S MOBILE PHONE VIA GSM.
• DIGITAL EVIDENCE: PHOTO CAPTURED AND STORED ON MICROSD CARD.
• STATUS INDICATORS: LEDS INDICATE CHARGING STATUS OR SYSTEM ARMING.
• SYSTEM CONTINUOUSLY SCANS FOR NEW MOTION AFTER "COOL DOWN" PERIOD.
• BATTERY VOLTAGE MONITORING ADJUSTS SYSTEM POWER USAGE (SLEEP MODE) IN REAL-TIME.
• SUCCESSFUL SMS TRANSMISSION CONFIRMS SYSTEM CONNECTIVITY.
• SYSTEM RE-ARMS ITSELF AUTOMATICALLY AFTER THE ALARM CYCLE ENDS.
FEEDBACK

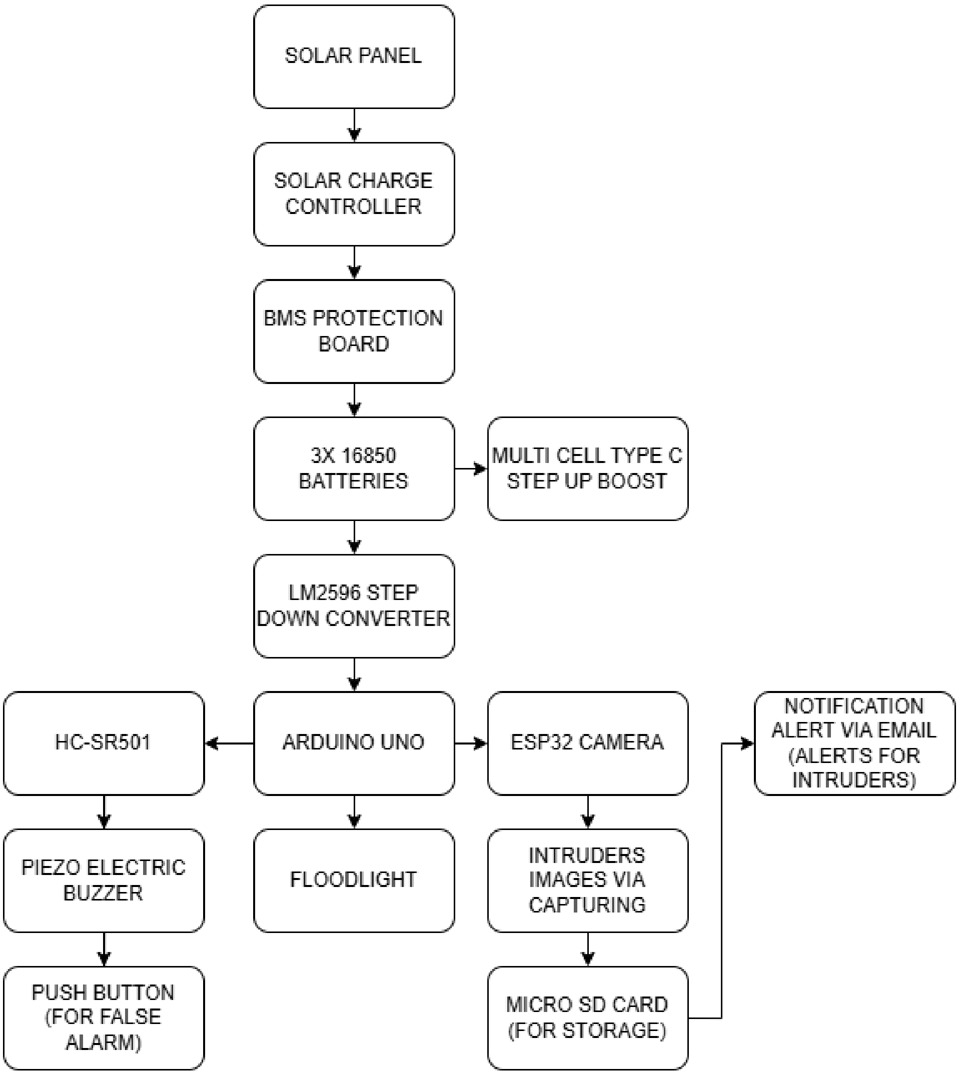
The working principle of this system starts from the Input phase where the system continuously collects information from its surroundings in the form of environmental data using its sensor array and power modules. The main input is from the HC-SR501 PIR sensor that scans for infrared movement signatures to identify any potential intruders and the ESP32-CAM is used as a feed for visual data to verify. Simultaneously the system measures the voltage levels of the solar panel and the 3x 18650 Li-Ion battery bank; the voltage information is important not only to check the available power, but also to serve as a day/night sensor to know when to light. A physical push button is also provided as a manual input and allows the user to reset the system or force a test mode manually.

In the Process phase the microcontroller performs the role of the brain, analysing these raw inputs through certain logic algorithms. The system implements a routine of "Smart Filtering" which checks the motion signals to eliminate false alarms produced by momentary glitches or wind. It then measures the voltage from the solar to measure the current lighting conditions (Day vs. Night) and controls the power consumption by using Maximum Power Point Tracking (MPPT) logic to ensure efficient charging.

If a valid threat is confirmed, then the processor calls the IoT logic and instructs ESP32 to capture an image and creates the required AT commands to send an email alert.

Lastly, the Physical Response is implemented through the Output and Feedback phases and the operational loop is closed. When a threat is processed, the system will enable high-intensity floodlights and a piezo buzzer to perform instant active deterrence, an email notification will be sent, and photographic evidence will be stored on a MicroSD card. After the alarm cycle has finished, the system goes into feedback loop; It constantly checks the state of the battery to regulate power consumption (Entering the sleep mode when needed) and self re-arms itself after a cool-down period. This makes the device be always ready and keep scanning on new movements and adjusting to the actual conditions of power.

Figure 2. Block Diagram

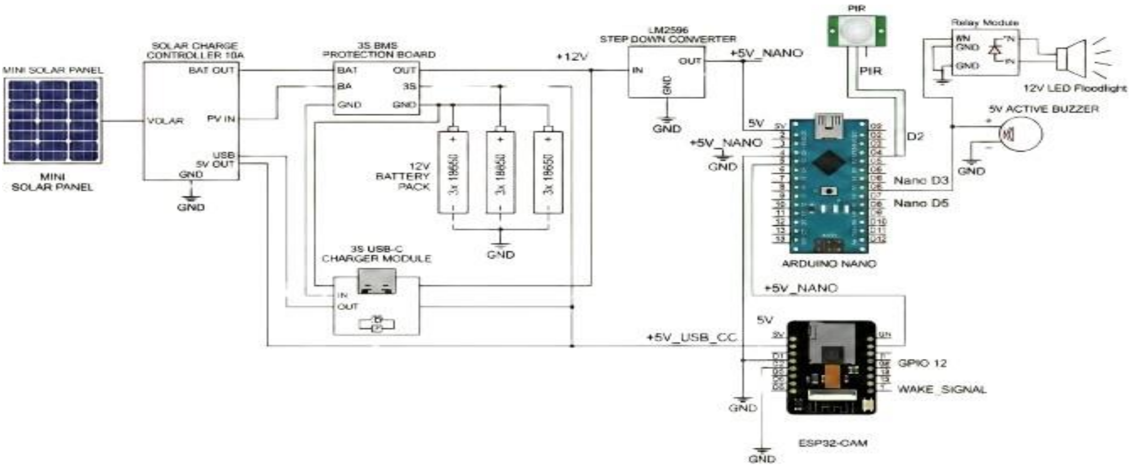

SOLAR PANEL
SOLAR CHARGE CONTROLLER
BMS PROTECTION BOARD
3X 16850 BATTERIES
MULTI CELL TYPE C STEP UP BOOST
LM2596 STEP DOWN CONVERTER
HC-SR501
ARDUINO UNO
ESP32 CAMERA
NOTIFICATION ALERT VIA EMAIL (ALERTS FOR INTRUDERS)
PIEZO ELECTRIC BUZZER
FLOODLIGHT
INTRUDERS IMAGES VIA CAPTURING
PUSH BUTTON (FOR FALSE ALARM)
MICRO SD CARD (FOR STORAGE)

The Power Supply and Energy Management Subsystem is designed to enable robust, indefinite off-grid operation without reliance on commercial electricity. The process begins with a Solar Panel that harvests solar energy, which is passed through a Solar Charge Controller to prevent overcharging and ensure battery longevity. This energy is stored in a high-capacity bank of three 18650 Lithium-Ion batteries, which are protected by a BMS (Battery Management System) Board to prevent short circuits and under-voltage issues. To power the electronics safely, the system utilizes a Multi-Cell Type-C Step-Up Boost module for external interfaces and an LM2596 Step-Down Converter, which stabilizes the battery output to a steady 5V/9V level for the Arduino Uno and sensors.

The Arduino Uno has been used as the core logic in the Processing and Local Defense phase. It is constantly monitoring the HC-SR501 PIR Sensor for the presence of any infrared signatures of a human motion. The Arduino then carries out local deterrence by turning on the Floodlight to shine light on the area and producing sound on the Piezo Electric Buzzer to frighten the intruder upon detection of a threat. To ensure control over operational errors a Push Button is incorporated into the circuit thus allowing the user to manually intervene to reset the alarm system in a case of a false trigger.

Finally, Visual Surveillance and Remote IoT Notification Parallel to the physical deterrence, the system uses the forensic and communication capabilities. When it detects the movement, the Arduino Uno transfers a logic signal to the ESP32 Camera module which awakens it from its low power state. The ESP32-CAM's first purpose is to take high-resolution images of the intruder, which is then written to an onboard Micro SD Card immediately. This local storage helps to ensure evidence is conserved even if there is instability in the internet connection. Second, the ESP32 uses its inbuilt wifi capabilities to join the network and use an SMTP protocol to send the Notification Alert using Email to the user's smartphone directly. This email consists of the timestamp of the intrusion and, depending on the configuration of the code, the image of the capture so the user receives in real time intelligence on the security breach regardless of their geographical location.

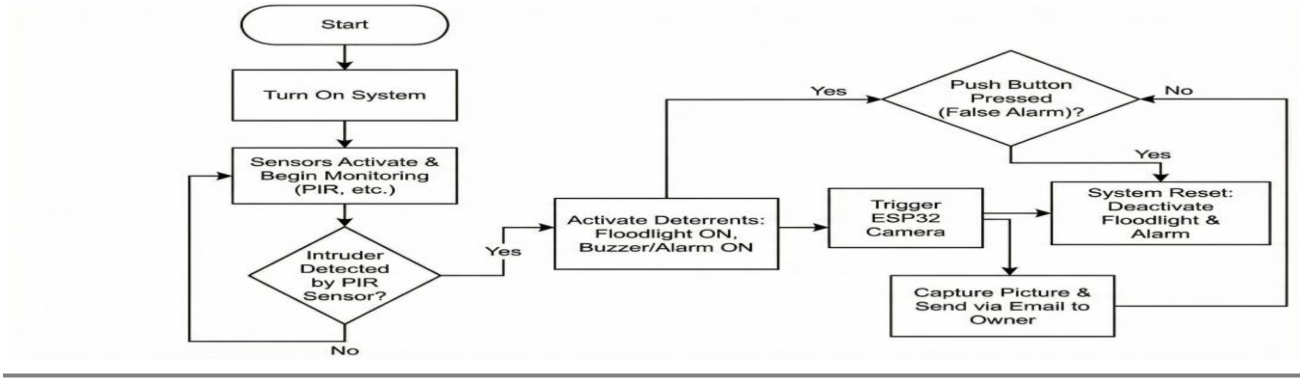
Figure 3. Schematic Diagram



The schematic design of the system is based on a robust off-grid power management circuit that is responsible to maintain a steady autonomy. A photovoltaic panel is coupled to a Solar Charge Controller which is used to regulate the energy harvesting to charge a battery bank consisting of three 18650 Lithium-Ion cells protected by a BMS (Battery Management System) board. To get the voltage difference between the battery bank (high capacity) to the sensitive logic components, an LM2596 Step-Down Buck Converter is used to stepped down the voltage to a stable voltage for Arduino Uno and a Multi-Cell Type-C Boost module as auxiliary power interfaces. The central control unit is the Arduino Uno which is electrically connected to a HC-SR501 PIR sensor to pick up the movement input, and pumps up a high-current floodlight using a relay board, and a piezoelectric buzzer using a direct digital output to have active deterrence.

The communication and forensic functions of the system are implemented by a communication circuit of a serial interface (UART, Universal Asynchronous Receiver-Transmitter) between the main Arduino microcontroller and ESP32-CAM module. When a high-logic signal is validated by the PIR sensor, the Arduino sends a serial trigger to the ESP32 which interrupts its low-power state and reads an image and stores it on a MicroSD card using the SPI bus. At the same time, ESP32 implements a programmed SMTP protocol to send the evidence taken through email. A manual override circuit, which is a tactile push-button with an internal pull-up resistor, is incorporated into the circuit so that the user can interrupt the alarm loop and reset the system hardware in case of false triggers or maintenance.

Figure 4. Flow Chart


Start
Turn On System
Sensors Activate & Begin Monitoring (PIR, etc.)
Intruder Detected by PIR Sensor?
Yes
No
Activate Deterrents: Floodlight ON, Buzzer/Alarm ON
Yes
Push Button Pressed (False Alarm)?
No
Yes
Trigger ESP32 Camera
System Reset: Deactivate Floodlight & Alarm
Capture Picture & Send via Email to Owner

The operation of the system starts as soon as the device is powered, thus the solar energy harvesting circuit and the sensor array are initialized. Once active, the HC-SR501 Passive Infrared (PIR) sensor enters a continuous scan mode where they track the area they are meant to protect for thermal-motion signatures which are characteristics of human presence. During this standby mode, the system is working in an efficient manner to save battery life, it is waiting for a valid trigger from the environmental system while the power management module takes care of the power remains stable.

Upon detection of a verified intruder, the microcontroller puts in place a simultaneous dual-response protocol for securing the area. The system triggers the "Active Deterrence" mechanisms instantaneously through a combination of high-intensity floodlight on and piezoelectric buzzer sounding to startle the intruder.

Concurrently, the logic signal is used to activate ESP32-CAM module that captures real-time image of the scene and sends direct image evidence to the owner through email so that the owner gets an immediate awareness of the breach done.

To deal with errors that may occur during the operation and for manual control, a reset mechanism is included in the system at the hardware level. In the event of a false alarm, which is made by environmental factors or by authorized personnel, there is a special push button where the user can manually interrupt the alarm process and reset the system instantly. Once the system has been reset or an alarm cycle has been completed the program goes back to the initial standby state, the sensors are re-armed to again monitor for new threats.

RESULTS AND DISCUSSION

The Solar-Powered Smart Guard was tested and assessed by a series of empirical test runs that were aimed at the reliability of the detection, responsiveness of the system, and energy independence. The development of the system was done as an event-based control system where the environmental inputs are computed in an

effort to arrive at autonomous security outputs. The core of this assessment was combination of Arduino Uno and ESP32-CAM Architecture that provides ability to get complex logic without using the cloud processing.

Motion Detection Performance

Four distinct distances of 1 feet, 2 feet, 5 feet and 7 feet were taken to investigate the effectiveness of the HC-SR501 PIR sensor and the algorithm of Smart Filtering.

Trial	Distance	Detection Outcome	System Response	Aletert Latency
1st trial	1 feet	High reliability	Immediate local deterrence (Lights/Alram)	5 - 7 seconds
2nd trial	2 feet	Stable	Verified signal; SMS and image capture	5 - 7 seconds
3rd trial	5 feet	Optimal Sensitivity	Remote notification and visual evidence	5 - 7 seconds
4th trial	7 feet	Threshold detection	Verified signal; SMS and image capture	5 - 7 seconds

The results of the experimental process supported the capability of the system to ensure 24/7 autonomous functioning along with correctly recognizing the presence of a human being as opposed to the noise of the environment. A 1 feet, 2 feet, 5 feet and 7 feet trials showed that the "Smart Filtering" strategy was necessary: a 200 milliseconds-long Double-Check routine allowed the software to detect instantaneous noise due to a wind or a moving object. This will guarantee that the high-intensity floodlights and audible alarm will only be activated in response to confirmed intrusion and save battery power which is stored in the 3x 18650 Lithium-Ion bank.

Moreover, it was noted that the Solar Charge Controller also was highly effective in maintaining the stability of the battery voltage in different weather conditions so as to enable the device to operate in full swing without having to rely on the commercial power grid. Whilst the local response (Floodlight and Buzzer) was almost real-time , the remote alert latency through the ESP32-CAM took on average 5 to 7 seconds. To a great extent, this difference in speed was conditional upon the internet connectivity and Wi-Fi signal strength, however, not the delays in internal processing. The results validate the prototype as a scalable energy efficient alternative to conventional, reactive CCTV systems that has the potential to serve as a proactive deterrent in remote settings where power stability is an issue in locations that are off-grid.

CONCLUSION

The Smart Guard, which is solar-powered, was used to conduct autonomous energy harvesting experiments and motion-based intrusion detection and an active deterrence using IoT integration. During most of the trials, the system was able to continue during the tests and robustly detect the presence of human with the help of the PIR sensors and "Smart Filtering" logic. Specifically, the Solar Charge Controller helped to keep the voltage levels of the 3x 18650 battery bank stable during day and night cycles; while the sensor fusion algorithm made corrections for environmental noise to control false alarms. Additionally, the system provided its ability for email notification and capture visual proof in case of an unauthorized entry using ESP32 Camera for remote communication. All parts of feedback like floodlight, piezo buzzer, and email alerts was responsible to give instant indication of the security actions carried out during the experiment.

The latency time of each successful remote alert was dependent on internet connectivity and signal strength not cellular networks. Many first tests proved the need for accurate calibration of the PIR sensor in order to obtain the required detection reliability. Therefore, the proposed solution provides an integrated linking of multiple

tasks such as off-grid power management, real-time active physical deterrence and visual monitoring. Consequently, the proposed solution through the use of Arduino Uno and ESP32 architecture is able to conduct autonomous, sustainable security monitoring across predetermined facility.

The time (latency) of each successful remote alert was between 5 and 7 seconds depending on the cellular signal strength. Many initial tests have shown that there is a need for accurate sensitivity calibration of the PIR sensor to achieve the required reliability to detect it. Therefore, the proposed solution offers a seamless connection of many different tasks including off-grid power management, real-time, active physical deterrence, and real-time visual monitoring, which has not been achieved in other solutions that have only research limited to solving passive recording or simple lighting functions. Therefore, the proposed solution with the Arduino Uno and ESP32 architecture is able to perform the autonomous sustainable security monitoring throughout a residual pre-determined facility.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to our research advisor for their continuous guidance, enthusiastic encouragement, and useful critiques of this research work. We also wish to thank the Department of Computer Engineering at the Eulogio “Amang” Rodriguez Institute of Science and Technology for providing the necessary laboratory facilities and resources required to complete this project. Finally, we extend our appreciation to our families and peers for their support and motivation throughout the development of this prototype.

REFERENCES

1. M. Sushmasri; Mohameed Jameel. “Automatic Security Light and Alarm Using Arduino and PIR Sensor.” Volume. 9 Issue.12, December-2024 International Journal of Innovative Science and Research Technology (IJISRT), 881-886, https://doi.org/10.5281/zenodo.14550740
2. P. N. Saranu, G. Abirami, S. Sivakumar, K. M. Ramesh, U. Arul and J. Seetha, "Theft Detection System using PIR Sensor," 2018 4th International Conference on Electrical Energy Systems (ICEES),

Chennai, India, 2018, pp. 656-660, https://doi.org/10.1109/ICEES.2018.8443215

3. R. C. Jisha, M. V. Ramesh and G. S. Lekshmi, "Intruder tracking using wireless sensor network," 2010 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, 2010, pp. 1-5, https://doi.org/10.1109/ICCIC.2010.5705799
4. Surantha, N., & Wicaksono, W. R. (2018). Design of smart home security system using object recognition and PIR sensor. Procedia Computer Science, 135, 465–472. https://doi.org/10.1016/j.procs.2018.08.198
5. Mouri, S. P., Sakib, S. N., Ferdous, Z., & Taher, M. A. (2015). Automatic lighting and security system design using PIR motion sensor. Journal of Institute of Information Technology, Jahangirnagar University,14(8).https://www.researchgate.net/publication/303314563_AUTOMATIC_LIGHTING_AND_SECURITY_ SYSTEM_DESIGN_USING_PIR_MOTION_SENSOR
6. Abiodun, S. S., Lasisi, O. H., Olasunkanmi, O. J., Mujeeb, B., & Tewogbade, A. (2025). Design and implementation of a solar-driven spy security motion detector. Journal of Engineering and Scientific Research, 7(2). https://jesr.eng.unila.ac.id/index.php/ojs/article/view/216
7. Verma, M., Kaler, R. S., & Singh, M. (2021). Sensitivity enhancement of Passive Infrared (PIR) sensor for motion detection. Optik, 244, 167503. https://doi.org/10.1016/j.ijleo.2021.167503
8. Nayak, M., & Dash, P. (2018). Smart surveillance monitoring system using Raspberry Pi and PIR sensor. Paripex-Indian Journal of Research,7(6). https://www.worldwidejournals.com/paripex/fileview/June_2018_1529064229 28.pdf
9. Sahoo, K. C., & Pati, U. C. (2017). IoT based intrusion detection system using PIR sensor. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology(RTEICT),1641–1645. https://doi.org/10.1109/RTEICT.2017.8256877.

About the Authors

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. Minerva C. Zoleta holds a Master’s degree in Electrical Engineering with a major in Computer Engineering from the Technological University of the Philippines, Manila. Currently, she is pursuing her Doctorate in Engineering with a specialization in Computer Engineering at the Technological Institute of the Philippines.

The authors, [1]Mark Edisol M. Asistio, [2]Nayeff L. Dingding, [3]Mark Dennis L. Larioza, [4]Janine P. Natalia, and [5]Janette Grace N. Siervo, are currently pursuing their Bachelor of Science degrees in Computer Engineering at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST), Manila, Philippines.

As a collaborative research group, their academic focus lies at the intersection of embedded systems, renewable energy integration, and the Internet of Things (IoT). They are dedicated to developing sustainable, technology-driven solutions that address real-world security and energy challenges. This project, the *Solar-Powered Smart Guard: Autonomous Lighting, Intrusion Detection, and Surveillance Network*, stands as a testament to their commitment to engineering excellence and serves as a partial fulfillment of the requirements for their collegiate degree.