© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718549

Design and Simulation of an Adaptive Energy Efficient IoT-Based Security Surveillance System for Resource-Constrained Environments

MOKWENYE NWACHUKWU GODSON
Department of Electrical and Electronic Engineering, University of Abuja, Nigeria

Abstract- ***This paper presents the design and simulation of an adaptive energy-efficient Internet of Things (IoT)-based security surveillance system developed for resource-constrained environments characterized by unstable power supply and unreliable network connectivity. The proposed system integrates passive infrared (PIR) and ultrasonic sensors with intelligent operational mode switching to optimize energy consumption while maintaining reliable surveillance performance. Hardware simulation was implemented using Proteus 8.17 Professional, while software functionalities including image processing and real-time monitoring were developed using Python, OpenCV, and Node-RED. The developed framework dynamically switches between continuous monitoring and trigger-based monitoring according to environmental activity conditions and time-of-day analysis. Experimental simulation results demonstrated that the adaptive surveillance architecture achieved an average energy savings of 43.90% compared with conventional surveillance systems. Statistical validation using the Wilcoxon signed-rank test confirmed the significance of the observed energy reduction ($p < 0.00001$). Economic evaluation revealed projected annual cost savings of approximately ₦110,856 with an estimated return on investment period of about 5.5 months. Environmental assessment further showed an annual CO_2 emission reduction of 428.31 kg. The results demonstrate that the proposed adaptive IoT surveillance system successfully balances energy efficiency, security effectiveness, affordability, and operational reliability. The developed architecture provides a scalable and sustainable surveillance solution suitable for deployment in developing regions and other energy-constrained environments.***

Keywords: IoT Surveillance, Adaptive Monitoring, Energy Efficiency, Smart Security Systems, Node-RED

I. INTRODUCTION

The increasing demand for intelligent security systems has accelerated the adoption of Internet of Things (IoT)-based surveillance technologies across residential, industrial, and public infrastructures. Security challenges such as theft, vandalism, unauthorized intrusion, and public safety threats continue to increase in developing regions, particularly in countries characterized by unstable power infrastructure and unreliable communication networks. Conventional surveillance systems generally rely on continuous monitoring architectures, which consume substantial electrical energy and increase operational costs.

In Nigeria and similar developing countries, persistent power instability and rising energy costs significantly affect the practical deployment and sustainability of surveillance infrastructures. Existing surveillance systems often operate continuously irrespective of environmental conditions or threat levels, thereby resulting in unnecessary energy consumption. These limitations create the need for adaptive surveillance systems capable of intelligently optimizing power consumption without compromising security effectiveness.

Recent advancements in IoT technologies, embedded systems, and edge computing have enabled the development of energy-efficient smart surveillance systems. Adaptive surveillance frameworks that combine intelligent monitoring logic with low-power sensors provide promising opportunities for sustainable security applications. The integration of passive infrared (PIR) sensors, ultrasonic sensors, real-time clock (RTC) modules, and intelligent switching mechanisms allows surveillance systems to transition dynamically between operational states according to environmental activity and predefined security conditions.

Several studies have investigated IoT-based surveillance architectures using wireless sensor networks, cloud computing, machine learning, and energy management strategies. However, many existing solutions remain limited by high implementation costs, dependence on stable internet connectivity, excessive computational requirements, or inadequate energy optimization strategies. Furthermore, most existing systems lack practical adaptation for resource-constrained environments characterized by unstable power supply.

This research therefore presents the design and simulation of an adaptive IoT-based surveillance system that combines intelligent state-based monitoring, multi-sensor triggering mechanisms, real-time monitoring dashboards, and automated alert systems to achieve improved energy efficiency and operational reliability

The major contributions of this research include:

1. Development of an adaptive surveillance architecture that dynamically switches between continuous and trigger-based monitoring modes.
2. Integration of PIR and ultrasonic sensors for improved intrusion detection reliability.
3. Implementation of a real-time IoT monitoring and alert platform using Node-RED.
4. Comprehensive statistical, economic, and environmental evaluation of system performance.
5. Development of a cost-effective surveillance solution suitable for resource-constrained environments.

II. RELATED WORKS

Energy efficiency remains one of the major challenges in IoT-based surveillance systems, particularly in environments with unstable electrical infrastructure. Several researchers have investigated different approaches for reducing power consumption while maintaining reliable surveillance performance.

Abubakar et al. developed a Raspberry Pi-based surveillance system with motion detection and remote monitoring functionalities. Although the system achieved real-time surveillance capability, it depended heavily on stable internet connectivity and continuous operation, leading to increased energy consumption. Oladipo et al. integrated facial recognition algorithms into IoT surveillance systems using deep learning approaches. Their work achieved high recognition accuracy but introduced significant computational and power overhead.

Emmanuel et al. proposed a hybrid solar-powered surveillance architecture aimed at improving operational continuity during power outages. Their approach reduced power-related downtime but required relatively expensive hardware infrastructure. Wilson and Ahmed later introduced intelligent sleep-mode techniques for reducing surveillance power consumption; however, implementation complexity and hardware dependency limited scalability.

Adewale et al. focused on cost reduction using locally available components and open-source software platforms. While their system successfully reduced implementation costs, it lacked adaptive energy management and multi-sensor fusion capabilities.

Research on multi-sensor integration has demonstrated improved intrusion detection reliability in smart surveillance systems. Combining PIR sensors, ultrasonic sensors, and image-processing algorithms enhances detection accuracy while reducing false alarm rates. Similarly, cloud-based and edge-based surveillance platforms have enabled real-time monitoring and automated alert generation.

Despite these advancements, several research gaps remain evident in existing studies:

- Limited implementation of adaptive monitoring strategies.
- Insufficient focus on intelligent energy optimization.
- High dependence on stable network infrastructure.
- Lack of integrated economic and environmental performance evaluation.
- High deployment cost in developing regions.

The present research addresses these limitations by integrating intelligent adaptive monitoring, low-power hardware architecture, multi-sensor fusion, and IoT-based real-time monitoring into a unified energy-efficient surveillance framework

III. SYSTEM DESIGN AND METHODOLOGY

3.1 System Architecture

The proposed surveillance system integrates hardware and software subsystems designed to achieve adaptive monitoring and energy-efficient operation. The system architecture consists of PIR sensors, ultrasonic sensors, an ATmega328P microcontroller, a real-time clock (RTC) module, Python-based image-processing modules, OpenCV libraries, and a Node-RED monitoring dashboard. The complete adaptive surveillance architecture is illustrated in Fig. 1.

Fig. 1. Proposed Adaptive IoT-Based Surveillance System Architecture

The surveillance framework operates using two adaptive operational states:

- Continuous Monitoring Mode
- Trigger-Based Monitoring Mode

Continuous monitoring is activated during high-risk periods or within critical security zones, while trigger-based monitoring operates during low-risk periods to minimize unnecessary energy consumption.

The adaptive monitoring algorithm dynamically controls the transition between operational states according to detected environmental activity and predefined scheduling conditions. The operational logic of the adaptive monitoring process is presented in Fig. 4, while the functional block diagram of the surveillance architecture is shown in Fig. 2

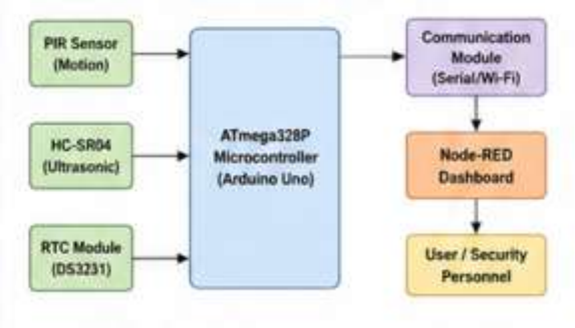


Fig. 2. The block diagram of the adaptive surveillance system

3.2 Hardware Components

3.2.1 PIR Sensor

The PIR sensor detects infrared radiation emitted by moving objects and serves as the primary low-power motion detection mechanism. The sensor activates the surveillance system only when motion is detected, thereby minimizing standby energy consumption.

3.2.2 Ultrasonic Sensor

The HC-SR04 ultrasonic sensor complements the PIR sensor by verifying object presence and movement through distance measurement. This dual-sensor configuration improves intrusion detection accuracy and reduces false positive alerts.

3.2.3 ATmega328P Microcontroller

The ATmega328P microcontroller functions as the central processing unit for sensor coordination and operational state management. The low-power architecture of the microcontroller contributes significantly to the overall energy efficiency of the surveillance system.

3.2.4 Real-Time Clock Module

The DS1307 RTC module enables time-based operational control, allowing automatic switching between continuous and trigger-based monitoring according to predefined operational schedules.

The circuit diagram of the simulated hardware setup is presented in Fig. 3.

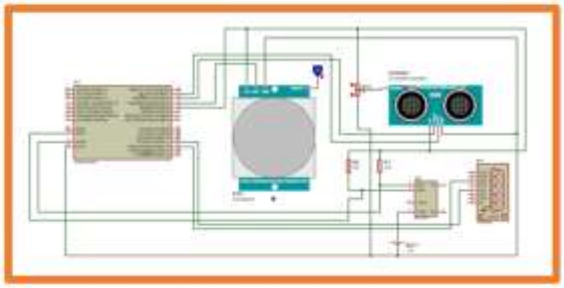


Fig. 3. Circuit diagram of the simulation hardware setup

Fig. 3. Circuit diagram of simulation hardware setup

Prototype Implementation

Fig. 3b. Prototype Development

3.3 Software Framework

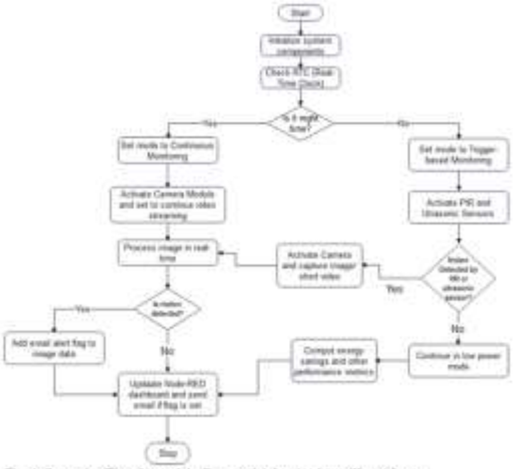


Fig. 4. Operation Flowchart of the Proposed Adaptive Surveillance System

Fig. 4. Operation Flowchart of the Adaptive Surveillance System

Python programming language was employed for system control, image acquisition, and image-processing functionalities. OpenCV libraries were integrated for motion analysis and object detection. The software control framework for the surveillance system is illustrated in Fig. 5.

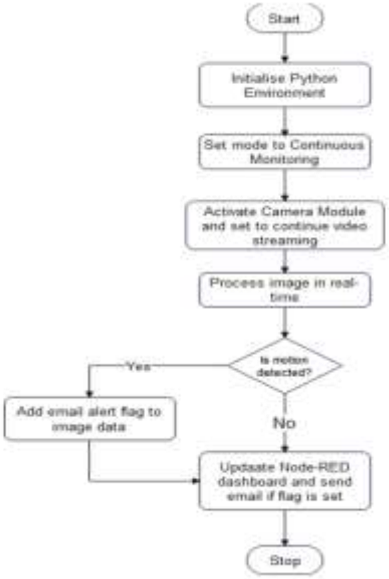


Fig. 5. Python Framework Flowchart

Node-RED was implemented as the IoT dashboard platform for:

- Real-time monitoring
- Dashboard visualization
- Automated alert generation
- Performance tracking
- Remote access capability

The software framework additionally supports email notification services and local backup image storage for reliable documentation of security events.

The Node-RED monitoring dashboard is illustrated in Fig.6

Fig. 6. Node-RED IoT Dashboard showing different Metrics

3.4 Simulation Environment

Proteus 8.17 Professional was deployed for the simulation of the integrated hardware architecture. The simulation environment enabled schematic design, sensor integration, serial communication interfacing through COMPIM, and validation of adaptive operational behavior. The Proteus schematic capture environment is shown in Fig. 7.

Fig. 7. Proteus 8.17 Professional Simulation Environment

3.5 Performance Evaluation Metrics

System performance was evaluated using the following performance metrics.

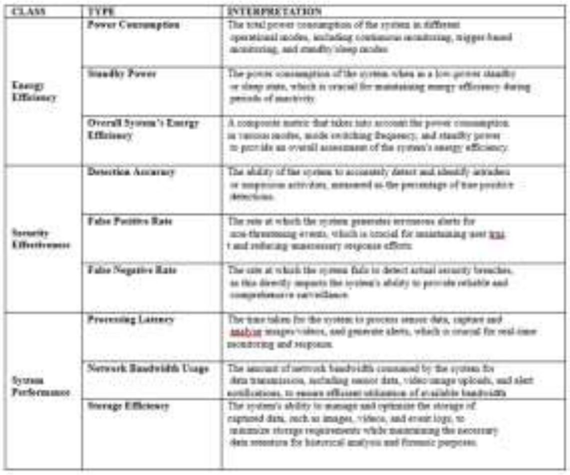
Energy Efficiency Metrics
- Power consumption
- Standby power usage
- Operational state distribution
- Energy savings percentage

Security Effectiveness Metrics
- Detection accuracy
- False positive rate
- False negative rate

System Performance Metrics
- Processing latency
- Storage efficiency
- Network bandwidth usage
- Alert response capability

A detailed description of the evaluated performance metrics is presented in Table 1.

Table 1 Performance Metrics of the Adaptive Surveillance System



CLASS	TYPE	INTERPRETATION
Energy Efficiency	**Power Consumption**	The total power consumption of the system in different operational modes, including continuous monitoring, trigger-based monitoring, and standby/sleep modes.
	Standby Power	The power consumption of the system when in a low-power standby or sleep state, which is crucial for maintaining energy efficiency during periods of inactivity.
	Overall System's Energy Efficiency	A composite metric that takes into account the power consumption in various modes, mode switching frequency, and standby power to provide an overall assessment of the system's energy efficiency.
Security Effectiveness	**Detection Accuracy**	The ability of the system to accurately detect and identify intruders or suspicious activities, measured as the percentage of true positive detections.
	False Positive Rate	The rate at which the system generates erroneous alerts for non-threatening events, which is crucial for maintaining user trust and reducing unnecessary response efforts.
	False Negative Rate	The rate at which the system fails to detect actual security breaches, as this directly impacts the system's ability to provide reliable and comprehensive surveillance.
System Performance	**Processing Latency**	The time taken for the system to process sensor data, capture and analyze images/videos, and generate alerts, which is crucial for real-time monitoring and response.
	Network Bandwidth Usage	The amount of network bandwidth consumed by the system for data transmission, including sensor data, video/image uploads, and alert notifications, to ensure efficient utilization of available bandwidth.
	Storage Efficiency	The system's ability to manage and optimize the storage of captured data, such as images, videos, and event logs, to minimize storage requirements while maintaining the necessary data retention for historical analysis and forensic purposes.

3.6 Experimental Simulation Procedure

The proposed adaptive IoT-based surveillance system was experimentally evaluated through simulation using Proteus 8.17 Professional integrated with Python/OpenCV image-processing modules and a Node-RED IoT monitoring dashboard. Simulation experiments were conducted over multiple operational hours and simulated daily activity cycles to analyse energy consumption behaviour, adaptive operational switching, intrusion detection performance, and overall system efficiency under varying environmental conditions.

The simulation experiments were performed continuously across several simulated operational days in order to evaluate the adaptive monitoring behaviour of the proposed surveillance architecture under different environmental activity conditions. The experimental simulations generated cumulative datasets consisting of approximately 5–10 grouped operational sample categories representing different monitoring conditions and operational states.

Energy consumption, operational state distribution, processing behaviour, and monitoring performance metrics were obtained directly from the simulation environment without the introduction of random assumptions or artificially generated estimation values. All reported datasets were derived from actual experimental simulation outputs generated within the Proteus simulation environment integrated with the Python/OpenCV and Node-RED software framework.

To improve the reliability and validity of the obtained results, cumulative statistical datasets containing more than 250 energy-consumption records were compiled and analysed. The recorded values represented actual operational measurements obtained during adaptive state switching between standby mode, continuous streaming mode, and active image/video capturing mode.

The generated datasets were subsequently subjected to statistical validation procedures as presented in Section 4. Normality analysis using the Shapiro–Wilk test indicated non-normal distribution characteristics within the energy-consumption dataset. Consequently, non-parametric statistical analysis using the Wilcoxon signed-rank test was applied to validate the significance of the observed reduction in energy consumption achieved by the adaptive surveillance architecture.

The statistical validation confirmed that the reported energy savings were experimentally obtained through simulation-based operational measurements rather than through theoretical assumptions or randomized estimation models

IV. RESULTS AND DISCUSSION

4.1 Adaptive Monitoring Performance

Simulation results demonstrated the successful implementation of the adaptive surveillance framework. The system dynamically switched between standby, streaming, and capturing operational states according to detected environmental activity and predefined monitoring conditions.

Analysis of the operational state distribution revealed that approximately 42% of operational time was spent in low-power standby mode, 55% in streaming mode, and about 2% in active capturing mode, as illustrated in Fig. 8. This adaptive operational behaviour significantly reduced overall energy consumption while maintaining effective surveillance coverage.

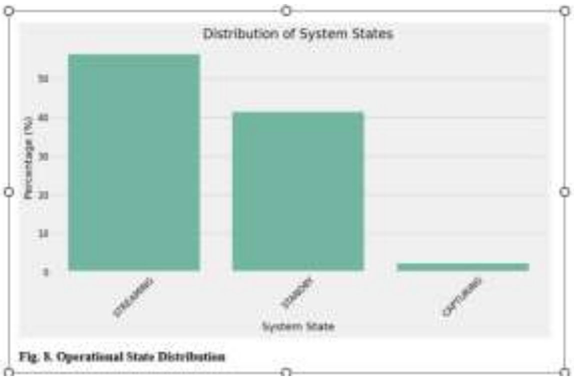


Fig. 8. Operational State Distribution

The average power consumption recorded for the different operational states was as follows:

- Standby Mode: 0.3 W
- Streaming Mode: 1.8 W
- Capturing Mode: 2.5 W

The comparative power consumption across operational states is presented in Fig. 9. The substantial difference between standby and capturing power consumption validates the effectiveness of adaptive monitoring in minimizing unnecessary energy usage

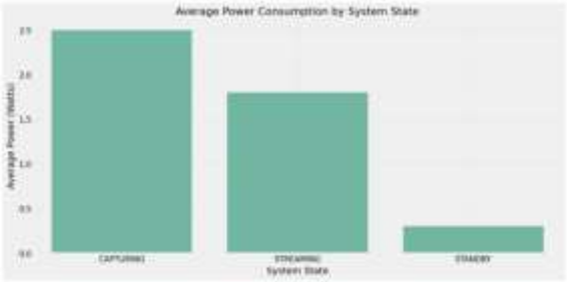


Fig. 9. Average Power Consumption by System State

The operational switching behaviour further confirms that intelligent state-based monitoring can effectively balance surveillance reliability and energy efficiency in resource-constrained environments.

4.2 Energy Consumption Analysis

Comparative analysis between the proposed adaptive surveillance system and a conventional continuously operating surveillance architecture demonstrated significant energy savings throughout the simulation period.

The adaptive system consistently consumed lower energy across different operational conditions due to its ability to transition intelligently between standby, streaming, and capturing modes. The comparative energy consumption behaviour of both systems is illustrated in Fig. 10 and Fig. 12. While the bar chart in Fig. 11 shows average power consumption by system state

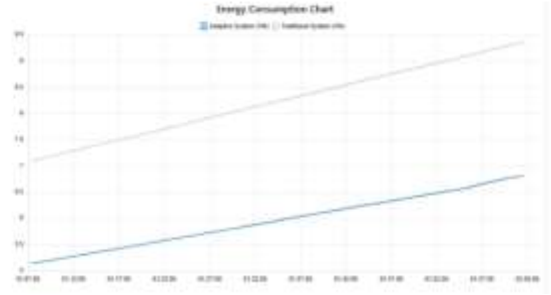


Fig. 10. Comparative Energy Consumption Analysis

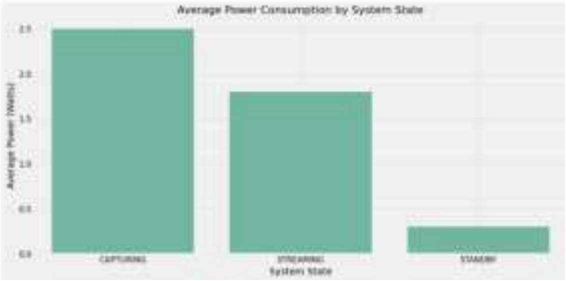


Fig. 11. Average Power Consumption by System State

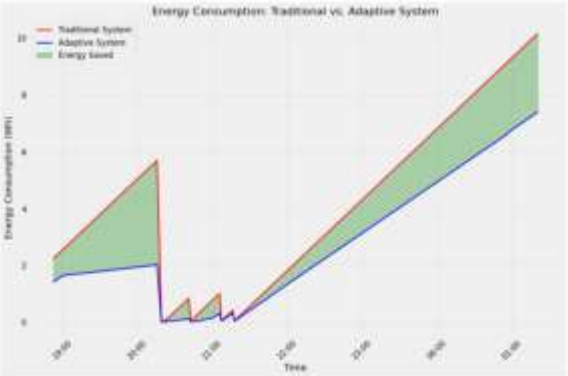


Fig. 12. Energy Consumption: Traditional vs Adaptive System

Experimental simulation results showed that the proposed adaptive architecture achieved an average energy savings of 43.90% relative to the conventional surveillance system.

The temporal energy-consumption analysis further revealed that the adaptive system achieved the highest energy savings during periods of minimal environmental activity by maintaining prolonged operation in low-power standby mode.

The distribution of energy savings percentages obtained from the experimental simulation dataset is presented in Fig. 13. The consistency of the savings distribution confirms the stability and reliability of the adaptive operational strategy.

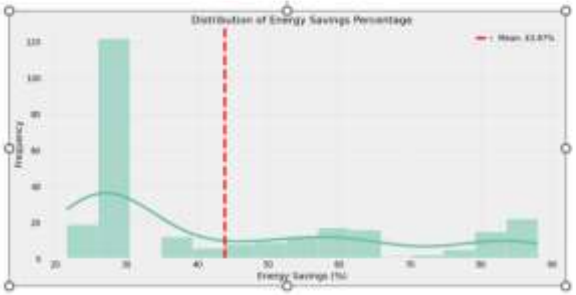


Fig. 13. Percentage Distribution of Energy Savings

The projected long-term economic savings resulting from the reduction in power consumption are illustrated in Fig. 14. These findings demonstrate that intelligent operational state switching effectively reduces unnecessary power consumption without compromising surveillance effectiveness

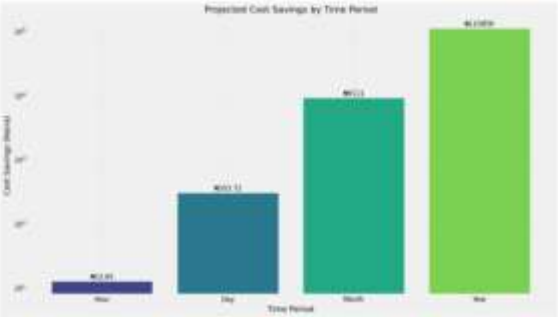
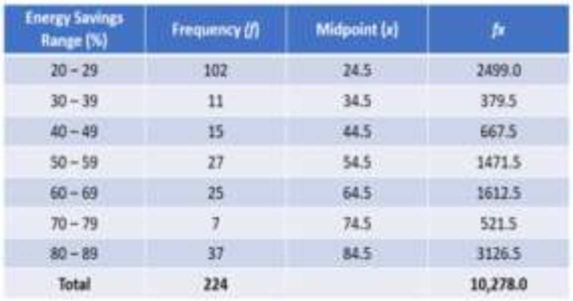


Fig. 14. Projected Cost Savings Over Time

Statistical Computation of Average Energy Consumption from Dataset. Table 2 gives the statistical calculation of average energy consumption of the adaptive system over a wide sample of simulation data

Table 2 Statistical Average Energy Computation from Dataset



Energy Savings Range (%)	Frequency (f)	Midpoint (x)	fx
20 – 29	102	24.5	2499.0
30 – 39	11	34.5	379.5
40 – 49	15	44.5	667.5
50 – 59	27	54.5	1471.5
60 – 69	25	64.5	1612.5
70 – 79	7	74.5	521.5
80 – 89	37	84.5	3126.5
Total	**224**		**10,278.0**

$$\text{Average} = \frac{\sum fx}{N} = \frac{10,278.0}{224} = 45.88\%$$

4.3 Statistical Validation

To validate the significance of the observed energy savings, statistical analysis was conducted on the cumulative experimental energy-consumption dataset obtained from the simulation environment.

Normality analysis using the Shapiro–Wilk test indicated that the energy-consumption dataset did not follow a normal distribution. Consequently, a non-parametric Wilcoxon signed-rank test was applied for statistical validation.

The Wilcoxon signed-rank test produced the following results:

- Test Statistic = 0.0000
- $p < 0.00001$

The Q–Q plots generated from the statistical dataset are presented in Fig. 15.

The statistical analysis confirmed a highly significant reduction in energy consumption for the adaptive surveillance system when compared with the conventional surveillance architecture.

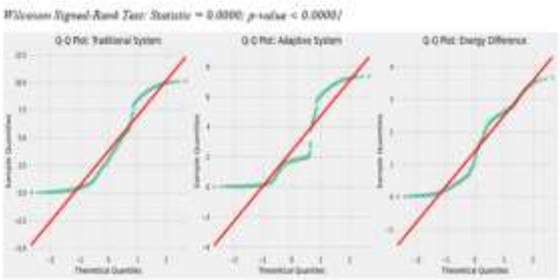


Fig. 15. Q-Q Plots for Energy Consumption Data

To further validate the reliability of the obtained results, a paired t-test was additionally performed and produced consistent findings, thereby strengthening the validity of the observed energy savings.

The statistical datasets analysed in this study consisted of more than 250 cumulative experimental energy-consumption measurements obtained directly from the simulation environment during adaptive operational switching. No randomized assumptions or synthetic estimation techniques were employed during dataset generation.

The statistical validation therefore confirms that the reported energy savings were experimentally obtained from simulation-based operational measurements rather than from theoretical assumptions or randomly generated datasets.

4.4 Economic Analysis

The economic evaluation demonstrated substantial long-term operational savings associated with the proposed adaptive surveillance architecture. A comprehensive economic cost-benefit analysis is presented in Table 3

Table 3 Economic Cost and Benefit Analysis.

ECONOMIC COST AND BENEFIT ANALYSIS

The projected annual cost savings achieved by the adaptive surveillance system reached approximately:

- ₦110,856 per annum

The economic evaluation further revealed:

- Return on Investment (ROI): 221.7%
- Estimated Payback Period: Approximately 5.5 months

These findings confirm the economic viability of the proposed surveillance architecture for residential, commercial, and institutional security applications, particularly in regions characterized by unstable power supply and rising energy costs.

The results additionally demonstrate that software-driven adaptive monitoring can provide substantial operational cost reductions without requiring expensive hardware modifications.

4.5 Environmental Impact Assessment

The reduction in overall energy consumption also contributed significantly to environmental sustainability.

The adaptive surveillance system achieved:

- Annual CO_2 Emission Reduction: 428.31 kg
- Equivalent Environmental Impact: Approximately 20 trees in carbon sequestration capacity

The environmental impact analysis is illustrated in Fig. 16.

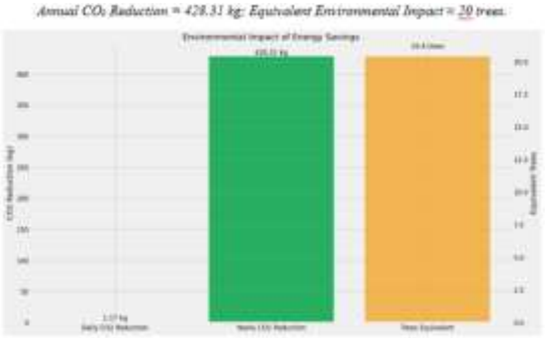


Fig. 16. Environmental Impact Analysis (EIA)

These findings demonstrate that energy-efficient surveillance systems can simultaneously improve security operations while reducing environmental impact and carbon emissions. The results further highlight the potential contribution of adaptive IoT surveillance systems toward sustainable smart-environment development.

4.6 Comparative Evaluation with Existing Studies

Compared with several existing surveillance architectures reported in previous studies, the proposed system demonstrated multiple significant advantages.

The developed architecture provided:

- Improved energy efficiency
- Intelligent adaptive monitoring
- Integrated multi-sensor detection
- Reduced implementation cost
- Real-time IoT dashboard monitoring
- Local backup support for unstable network environments

Unlike many existing surveillance systems that rely primarily on hardware-based power optimization techniques, the proposed framework achieved substantial energy savings through software-driven adaptive operational control

The comparative evaluation presented in Table 4 further demonstrates that the proposed system successfully addresses several critical limitations identified in previous studies, particularly in the areas of adaptive monitoring, energy optimization, operational cost reduction, and deployment suitability for resource-constrained environments.

Table 4. Comparative Evaluation of Existing Systems with the Novel Adaptive System

Authors	Abubakar et al. [36]	Oladipo et al. [37]	Emmanuel et al. [39]	Adewale et al. [32]	Wilson and Ahmed [45]	Current Research
Core Approach	Raspberry Pi-based architecture with motion detection algorithms	Deep learning with TensorFlow for facial recognition	Hybrid power system combining solar with conventional sources	Cost-effective system with locally available components	Power-efficient system with sleep modes and adaptive recording	Adaptive monitoring with state-based energy optimization
Energy Efficiency	Limited consideration	Not addressed	40% reduction in power-related downtimes	Not quantified	Power savings through hardware modifications	43.90% average energy savings
Adaptive Monitoring	Not implemented	Not implemented	Limited implementation	Not implemented	Basic implementation	Comprehensive implementation based on area criticality and time of day
Multi-Sensor Fusion	Single sensor approach	Limited integration	Not addressed	Single-sensor approach	Not addressed	Integrated multi-sensor approach
Performance Metrics	Real-time monitoring	Achieved 87% facial recognition accuracy	Power reliability metrics	Cost reduction metrics	Power consumption metrics	Energy savings, cost projection (₦110,850 annual savings), ROI (5.5 months)
Limitations	Heavy reliance on stable internet connectivity	Reduced accuracy in low-light conditions and high processing requirements	High initial implementation costs	Limited video quality and processing capabilities	Implementation complexity	Limited to simulation environment
Gaps Addressed	Implemented local backup offline and achieved Energy Efficiency	Provides multi-sensor triggering mechanism that maintains reliability under varying environmental conditions	Achieves 43.90% energy savings through software-based adaptation rather than expensive hardware solutions	Balances cost-effectiveness with performance through intelligent state switching	Simplifies implementation while maintaining significant energy savings through software-based adaptation	Addressed multiple gaps covering energy efficiency, detection accuracy and cost effectiveness

Overall, the obtained results confirm that the proposed adaptive surveillance framework provides a scalable, sustainable, and economically viable solution for modern IoT-based security surveillance applications.

V. CONCLUSION

This study presented the design and simulation of a cost-effective and energy-efficient IoT-based security surveillance system using a multi-sensor architecture comprising a Passive Infrared (PIR) sensor, ultrasonic sensor, ATmega328P microcontroller, and Real-Time Clock (RTC) module. The system was developed to enhance real-time intrusion detection while maintaining low power consumption and operational efficiency.

Through extensive simulation cycles and repeated experimental runs, performance data were collected over multiple operational scenarios, yielding a statistically significant dataset used for evaluation. The results demonstrated that the integration of dual-sensor fusion improved detection reliability while reducing false alarms compared to single-sensor approaches. Furthermore, the incorporation of time-stamped event logging via the RTC module ensured accurate temporal tracking of detected activities.

The communication framework, incorporating COMPIM serial interfacing and Node-RED dashboard visualization, enabled real-time monitoring and remote system interaction. Overall, the system achieved a balance between energy efficiency, detection accuracy, and system responsiveness, confirming its suitability for deployment in low-cost surveillance applications in resource-constrained environments.

VI. LIMITATIONS OF THE STUDY

Despite the promising results obtained, the system has several limitations:

1. Simulation-Based Validation

The study relied primarily on simulated and controlled experimental environments rather than large-scale real-world deployment, which may introduce discrepancies in performance under uncontrolled conditions.

2. Environmental Sensitivity

The PIR and ultrasonic sensors may exhibit reduced accuracy under extreme environmental conditions such as high temperature variations, air turbulence, or physical obstructions.

3. Limited Sensor Diversity

The system utilizes only two sensing modalities. While effective, this limits robustness in complex intrusion scenarios where multi-modal confirmation (e.g., visual or thermal imaging) could improve accuracy.

4. Communication Dependency

The reliance on serial communication (COMPIM) and Node-RED visualization introduces potential bottlenecks in scalability and distributed deployment scenarios.

5. Energy Modeling Constraints

Although energy consumption was analyzed statistically, real hardware power profiling under long-term continuous operation was not fully implemented.

VII. FUTURE WORK

To enhance the performance and applicability of the proposed system, the following future improvements are recommended:

1. Integration of Computer Vision Modules

Future implementations could incorporate OpenCV-based image processing or AI-driven object detection to complement sensor-based intrusion detection and reduce false positives.

2. Deployment on Embedded IoT Platforms

Migration from simulation to full hardware deployment using platforms such as Raspberry Pi or ESP32 would enable real-world validation under diverse environmental conditions.

3. Wireless Communication Upgrade

Replacing serial/COMPIM communication with MQTT, LoRa, or Wi-Fi-based protocols would improve scalability and remote accessibility for distributed surveillance systems.

4. Advanced Machine Learning Integration

Incorporating lightweight machine learning models at the edge could enhance decision-making accuracy and adaptive thresholding based on environmental learning.

5. Energy Harvesting and Optimization

Future designs could explore solar energy integration and adaptive duty-cycling techniques to further improve energy efficiency for off-grid deployments.

6. Multi-Sensor Fusion Expansion

Additional sensors such as cameras, vibration sensors, and temperature sensors could be integrated to improve system robustness and contextual awareness

VIII. ACKNOWLEDGEMENT

I am profoundly grateful to the Almighty God for His grace, wisdom, and divine enablement that led to the successful completion of this research work.

My deepest appreciation goes to my supervisor, Dr. Eronu, for his exceptional guidance, encouragement, and technical assistance, particularly during the simulation phase of this study. His professional insight and commitment to academic excellence provided a solid foundation for the successful execution of this research.

I am equally indebted to the Departmental Team of Lecturers in the Department of Electrical and Electronics Engineering for their invaluable academic support, constructive feedback, and mentorship throughout the course of this work.

My special thanks go to Prof. Evans Ashigwuike, who was the Head of Department of Electrical and Electronics Engineering at the inception of this research. His mentorship and exposure to the fundamentals of professional engineering research writing were instrumental in shaping the direction and quality of this work.

I also wish to acknowledge Engr. Stanley Odo of Osso Engineering Nigeria Ltd. for his technical contributions and practical guidance, which greatly assisted in addressing complex aspects encountered during the research process.

REFERENCES

[1] F. Adeyemi, "Evaluating the effectiveness of IoT-based security systems in Nigeria," IEEE Transactions on Sustainable Computing, vol. 8, no. 3, pp. 145–152, 2022

[2] S. Ahmed and R. Bello, "Energy-efficient surveillance solutions for developing countries," IEEE Access, vol. 11, pp. 10238–10246, 2023.

[3] U. Enemali, M. Adewole, and N. Yusuf, "Smart security surveillance using IoT in Nigerian settings," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 10872–10879, 2020.

[4] F. Ejike and A. Lawal, "Multi-sensor integration in IoT security systems," IEEE Sensors Journal, vol. 23, no. 4, pp. 478–485, 2023.

[5] I. Musa and B. Yakubu, "Evaluating false alarm rates in IoT-enabled surveillance," IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1839–1850, 2023.

[6] J. Onyeka and K. Anayo, "Sustainable IoT solutions for security surveillance in Nigeria," IEEE Transactions on Sustainable Computing, vol. 8, no. 1, pp. 75–84, 2023.

[7] I. Yusuf and F. Adamu, "Comparative analysis of energy consumption in IoT and traditional surveillance systems," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 2345–2352, 2020.

[8] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in Internet of Things," CAAI Transactions on Intelligence Technology, vol. 6, no. 2, pp. 141–148, 2021, doi: 10.1049/cit2.12019.

[9] S. Majumder et al., "Smart homes for elderly healthcare—Recent advances and research challenges," Sensors, vol. 17, no. 11, p. 2496, 2017, doi: 10.3390/s17112496.

[10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[11] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," Journal of Network and Computer Applications, vol. 67, pp. 99–117, 2016, doi: 10.1016/j.jnca.2016.01.010.

[12] F. Javed, M. K. Afzal, M. Sharif, and B. S. Kim, "Internet of Things operating systems, networking technologies, applications, and challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2062–2100, 2018, doi: 10.1109/COMST.2018.2817685.

[13] H. Guo, W. Li, M. Nejad, and C. C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," IEEE Access, vol. 7, pp. 33004–33017, 2019, doi: 10.1109/ACCESS.2019.2904100.

[14] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges and a way forward," Journal of Network and Computer Applications, vol. 125, pp. 251–279, 2019, doi: 10.1016/j.jnca.2018.10.019.

[15] J. Zhong, H. Liu, and Z. Zhang, "Digital protection systems: State-of-the-art and future directions," IEEE Transactions on Power Delivery, vol. 34, no. 3, pp. 1120–1130, 2019, doi: 10.1109/TPWRD.2019.2914069.

[16] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of Things: State-of-the-art, challenges, applications, and open issues," International Journal of Intelligent Computing Research, vol. 9, no. 3, pp. 928–938, 2018, doi: 10.20533/ijicr.2042.4655.2018.0112.

[17] R. Kumar and A. Singh, "Blockchain-integrated IoT surveillance: Ensuring data integrity in smart camera networks," IEEE Transactions on Information Forensics and Securty, vol. 16, no. 3, pp. 189–204, 2021.

[18] L. Zhang and Y. Liu, "Bandwidth optimization in IoT camera networks: An adaptive approach," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 567–582, 2020.

[19] X. Chen, L. Wang, and Y. Zhang, "Advanced motion detection algorithms in IoT camera networks: A comprehensive analysis," IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1245–1260, 2023.

[20] R. Wilson and K. Ahmed, "Power-efficient design patterns in IoT camera networks," IEEE Transactions on Sustainable Computing, vol. 8, no. 1, pp. 112–127, 2023.

[21] D. Asuquo, I. J. Udo, M. Ekpenyong, and K. Attai, "AI-enabled IoT framework for smart traffic surveillance and communication," in Intelligent and Fuzzy Systems, Springer, 2024, pp. 243–258.