Research Article / Review Article FUPRE JOURNAL 8(2): 69-83(2024)

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129

(Online)

http://fupre.edu.ng/journal

An IoT-based Human Motion Detection to aid Power Consumption in Automated Homes

***OKPERIGHO, S. U.* [1,*], *ABERE, R. A.* [1], *AKO, R. E.* [1], *NWOZOR, B.* [1], *GETELOMA, V. O.* [1]**

[1]*Department of Computer Science, College of Science, Federal University of Petroleum Resources Effurun, Delta State*

ARTICLE INFO

Received: 12/09/2023

Accepted: 12/12/2023

Keywords

Virtual key-card,
NodeMCU
Arduino
Raspberry Pi
Embedded systems

ABSTRACT

With an upsurge of data by global brands to interact/reach prospective clients, the birth of the Internet has today bridged the information gap. Virtualization techniques are today utilized as means to bridge the various lapses in our human processing endeavors. The adoption of tech to perform a variety of functions has since become imperative to ease our daily living as well as seamlessly allow transformations of various kinds to be impacted on our society. Study proposes an IoT-based energy efficent and reduction tool to yield cost-effective and cheap solution for managing energy consumption in homes. We have successfully integrated IoTs, wrireless sensor networks, and ESP32-controller to create a comprehensive control system. Its benefits includes improved energy consumption, security, data privacy, system efficiency, and user convenience. The system also provides real-time monitor and energy reduction control capabilities.

1. Introduction

The rapid development in technology in recent years has significantly contributed to improving daily living – creating a variety of applications in spheres such as environment, health, military, security, etc. These have and is currently, gradually becoming a sustainable alternative to traditional systems. All of this can be traced back to the development of microelectronics and integrated circuits, however, the appearance of several wireless communication standards such as Bluetooth Sigsbee, and Wi-Fi provide a compromise reliability of the system for long-term applications (Bengherbia et al., 2017).

One advancement is in Human Activity detection (HAD). HAD is mainly explored using imagery. Though, currently evolving to use sensors – it has shown positive impact in health monitoring and removing the barrier to healthcare (Hurt, 2019; Yu et al., 2019). To reach a marketable HAD device, state-of-the-art classifications and power consumption methods must be explored as well such as convolutional neural network. These will help bring about the much-needed rise in the adoption of sensor-systems for use in data compression, and other emerging techniques are reviewed here. Our study seeks to lay basic foundation for, address non-availability of HAD dataset, bring to

*Corresponding author, e-mail:sammydestiny@live.com
DIO

light the current drawbacks and their respective solution, and recommend as classification and power reduction techniques. The lack thereof, of publicly available datasets makes it difficult for new users to explore the field of HAD. This paper dedicates a section to publicly available datasets for users to access. We suggest a framework for HAD applications, which envelopes the current literature and emerging trends in HAD (Ojugo, Odiakaose, et al., 2023; Ojugo, Ugboh, et al., 2013)

1.1 Supervisory Control and Data Acquisition (SCADA)

Automation plays an important role in industrial systems. To speed up industrial processes, most industries now control their processes and operations remotely via their integration of the supervisory control and data acquisition (SCADA) systems. Cases of businesses where its frameworks are utilized includes controlling a gas stream via channels in an oil industry, managing the flow of water in water and sewage systems, managing the power output from power plants to the grid, process controlling in chemical plants, transporting and distributing products during production, manage railways infrastructure and signal networks (Upadhyay & Sampalli, 2020).

SCADA systems typically include one or more topographically distributed field sites with control servers, communication links, and field devices located at a control centre. Field-site SCADA sensors and actuators continuously monitor various characteristics of electromechanical devices and provide feedback to field control devices such as programmable logic controllers (PLCs), remote terminal units (RTUs), or intelligent electronic devices (IEDs). Send a signal. Via communication links, the transfer of information transpires back and forth between field control devices and the control centre. The field control devices will supply digital status information to the control centre, where the software will process the status information and determine acceptable parameter ranges. This information will then be transmitted to the field device(s) where action may be taken to avoid various hazards or optimize the performance of the system. The control centres will store the status information in a data historian and display it on an HMI (Human Machine Interface) which provides centralized monitoring of digital status information and system control. (Upadhyay & Sampalli, 2020).

SCADA protocols commonly used to cover large areas include Ethernet, Modbus, and DCOM – to help effectively transfer data over a wide area network via satellite, radio or microwave, cellular, switched network, telephone, or rented line communications media (Meixell & Forner, 2013). Its goal is to proficiently handle execution at a single area, such as a fabricating office, and not focus on the security of the organize data. Due to the increased interconnectivity of networks and the possibility of remote access to systems within the SCADA networks, a variety of vulnerabilities and risks of cyber-attacks exist. To strengthen the security of your SCADA network, you need to incorporate appropriate security measures. Common protection measures include a restricted perimeter, patch management, strong encryption, and most importantly, separation of control and corporate networks via layered defences mechanisms. However, these security measures are difficult to apply because they have old vulnerabilities and the potential for exploitation during real-time communications is high. (Nazir et al., 2017)

1.2. The SCADA Architecture

A typical SCADA architecture consists of (Alade et al., 2017) as below:

1. Field location: Field service locations typically have remote access

capabilities that allow field personnel to perform diagnostics and repairs remotely. Field location 1 (Figure 2.1) consists of a modem and a PLC that connect to sensors and other field devices via a field bus network. Fieldbus technology eliminates the need for point-to-point cable connections between the PC and field devices. Processed data from the PLC passes through a modem, where it is modulated and sent to the control center via a communication medium. “A modem is a device that converts serial digital data into signals suitable for transmission over telephone lines, allowing communication between devices.” (Stouffer et al., 2015). At remote site 2, both the WAN card and the intelligent electronic device (IED) are connected directly to the modem. There is enough intelligence built in to process some of the data, so no PLC is required. Field site 3 is similar to the field site except that the RTU is replaced by a PLC. Protocols are required for communication between sensors, other field devices, and RTU/PLC.

2. Communication Link: There is usually a long distance between the Field Sites and the Control Centre ranging from a few kilometers to hundreds of kilometers or at times thousands of kilometers. Effective communication is necessary for effective flow of data to/fro the MTU and other devices (Oliveira et al., 2016) as in figure 1. The link can be one of the following: We replaced the rental phone line. Power line-based communication. Wireless; Microwaves; Cellphones; Satellite and Wide Area Networks (WAN).
3. Control Centre: The main part of SCADA Server (or MTU), the HMI, Workstations, Data Historian, and Communication routers – all of which are linked to a LAN. Data collected by the field is via a control center, where it is recorded and displayed on the HMI to enable the operator to take appropriate actions needed based on detected events.
4. Trend analysis, alarms and central reporting are also the responsibility of the control center. (Stouffer et al., 2015).

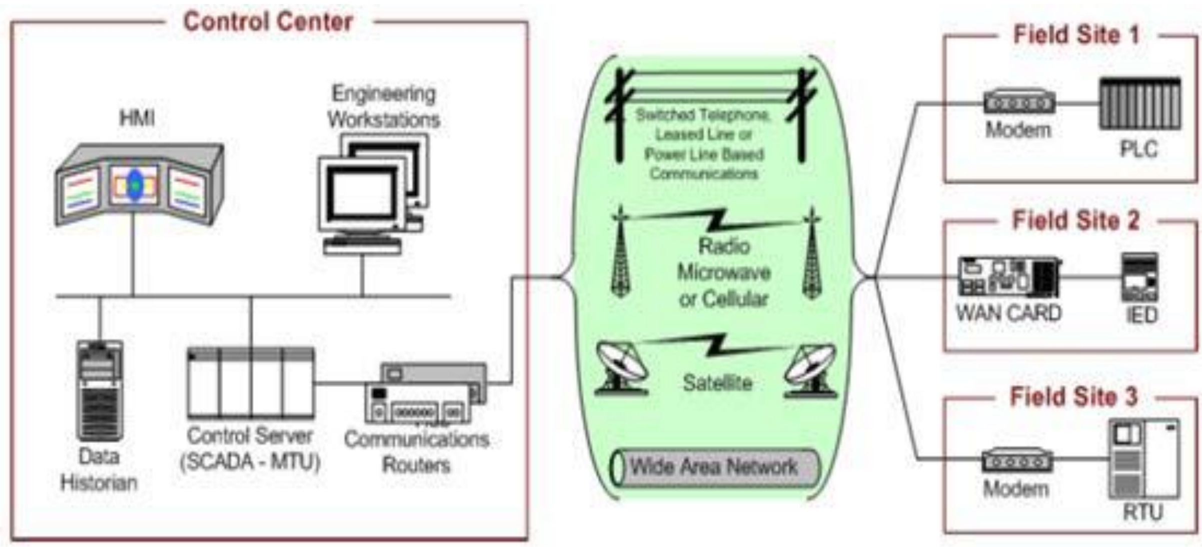

Figure 1. The schematic diagram of the SCADA Architecture (Ojugo et al., 2021a, 2021b)

1.3 Energy Efficient Automated Homes

Energy conservation is a critical issue in our society today as our civilization hinges on it. But, energy resources are finite, and there is an increase always in its demand made for diminishing supplies (Aghware et al., 2023a; Akazue et al., 2022, 2023; Oyemade et al., 2016; Oyemade & Ojugo, 2020, 2021). The cost of energy is enormous, and the cost is rising. Utility bills account for much in the cost of managing our homes on a monthly scale – and so it does too in businesses. Large hotels and hospital spend millions on energy yearly. Heavy dependence and consumption also in turn – portends environmental dangers ranging from fossil fuels emission of carbon dioxide into the atmosphere, to accelerate the greenhouse effect. Air conditioning releases gas and destroy earth's ozone, and discarded lamps aids mercury pollution (Kizilkaya et al., 2022; Vågsholm et al., 2020; Zhang et al., 2019). Its consumption depletes a spectrum of resources so that research has begun to now focus on energy conservation (Braddock & Chambers, 2011).

Energy efficiency and conservation are critical today to achieve international goals for the reduction of greenhouse gas emissions, fossil fuel usage, grid load strain, costs, and a wide range of other benefits (Suleiman & Reza, 2019). Also, many energy efficiencies and conservation approaches are not cost effective, which often hinder their adoption (Ojugo & Otakore, 2018a, 2018b). Design methods that run in computing environments include hardware, virtual CPU environments, servers, computers, tablets, wireless mobile devices, etc (Yuan & Wu, 2021; Zardi & Alrajhi, 2023). These, can integrate with the amortized payment terms and amounts with predicted and actual energy cost-savings (Nassar & Al-Hajri, 2013; Ojugo, Ugboh, et al., 2013). These are innovative, and useful to provide financial risk reduction, management and with low-cost outlays – and become an enabler to finance efficient and conservation projects (Chang & Lin, 2006; Charan et al., 2020).

At the start of electrification, switching electrical devices was done using connecting or disconnecting them to the power grid. In recent years disconnecting a device from its energy source has become less popular. Instead, switching is done electronically (automatically). This means that the inner device is separated from the switching circuit (Gorawski et al., 2015; Ibrahim & Syed, 2018; P. Joshi et al., 2020; Zawislak et al., 2022). As a consequence, the device can be powered 'on' or 'off' by a remote-control unit or by an automated switching circuit based on occupancy. Some computer mainboards may even allow the reaction to power network events (Braddock & Chambers, 2011).

The study is motivated (Ojugo, Akazue, Ejeh, Odiakaose, et al., 2023; Ojugo, Eboka, et al., 2015a, 2015b) as thus:

1. **Home automation:** Energy demand in our homes today, accounts for quite a significant amount in the overall consumption of energy globally. The heterogeneity of the involved devices, and the non-negligible influence of the human factor make the optimization of energy use a challenging task; effective automated approaches must take into account basic information about users, such as the prediction of their course of actions.
2. **Automation** has thus brought a huge risk to energy supply, which entails its usage as automation has increased ease it has also increased usage thus it poses a series of threats to our society at large Curbing this usage has now become a problem.
3. **Non-availability of datasets** for predictive algorithms when it comes to energy conservation as such a huge part of this project will aim at developing such systems by way of sensor-based (Ojugo & Ekurume, 2021a, 2021b; Ojugo & Otakore, 2020).

Study proposes an IoT-based human activity motion detector to help minimized power consumption in homes by detecting human movement and adjusting energy to suit each need.

2. MATERIALS AND METHODS

3.1. The Existing System

Smart home energy management system developed by Ma et al. (2021) to provide the basis of wireless sensor networks (IoTs) and machine learning for automation and energy savings (Ma et al., 2021). They employed a rule-based mode using a PIR motion sensor, door contact sensors, temperature and humidity sensors, and integration with smart thermostats and lighting. Occupancy detection was limited to the data from the simple binary motion and door sensors, which cannot provide detailed occupancy information (Lu et al., 2010). The neural network model aimed to predict occupancy based on this sensor data to drive heating, ventilation, and air conditioning (HVAC) activation (Lu et al., 2010). Testing was conducted in an apartment with two occupants over multiple months (K. W. Brown & Armstrong, 2023; W. Brown & Armstrong, 2015).

While system was able to achieve 20-36% savings for HVAC and lighting, the coarse occupancy detection had major limitations (Alakbarov & Hashimov, 2018; Datta et al., 2021; C. Joshi et al., 2021; Ojugo & Yoro, 2020b; Pradeepa & Parveen, 2020) to include: (a) the lack of computer vision to aid motion detection means the system cannot accurately track occupancy or distinguish between different occupants. This led to inappropriate automation decisions, such as turning off lights when a room is still occupied (Ojugo & Eboka, 2021). Further limitations include the lack of appliance integration, minimal user feedback, and the need for better optimization of user preferences (Lu et al., 2010). Significant opportunities remain for improvement in occupancy detection, appliance control, user-centric design, and whole-home energy reduction.

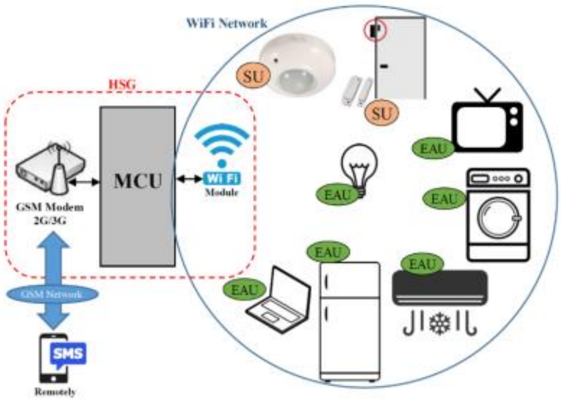

Figure 2. Dataflow diagram of existing system

2.2. The Proposed System

We take a more comprehensive approach to energy optimization than existing solutions. By combining computer vision with a sensor fusion model, it aims to achieve precise real-time occupancy detection throughout the home. This enables appropriately timed activation and automation of HVAC, lighting, appliances, entertainment systems, and other controllable devices based on granular occupancy data rather than motion sensors alone. The system incorporates self-learning capabilities to discover usage patterns and continuously refine the automation policies over time, accounting for changes in occupant behaviour. A user-centric design focuses on interfaces and controls for customizing schedules, preferences, and system overrides to align with occupant needs. Expanded testing across diverse home layouts and occupants will evaluate real-world effectiveness. Detailed energy savings reporting and cost-benefit analysis are also planned to quantify advancements over current technology. This holistic approach addressing the limitations of existing systems is expected to deliver state-of-the-art home energy efficiency, convenience, and cost-effectiveness.

The proposed system uses cameras and sensors to feed real-time occupancy data to an automation controller. The controller uses this occupancy data along with user controls, external data like weather, and learned usage patterns to control HVAC, lighting, appliances, and entertainment systems. Bidirectional data flow allows user interfaces to present system status and provide controls. The controller also logs detailed energy usage data to quantify savings. This complete integration of major home systems with granular occupancy data enables intelligent optimization of energy consumption based on real-time home activity across all areas. The data flow allows both automation of devices based on occupancy as well as user control for preference customization.

Its many benefits include:

1. **Interconnectivity** in IoT seeks to have all devices approximate interconnected with the worldwide records and conversation infrastructure.
2. **Things-related services** helps an IoT to effectively handle persistent-issue and fault-tolerance concerns even as system operates efficiently under constraints of factors, which include privacy safety and semantic consistency between physical matters and their related virtual things. To provide factor-associated services inside its constraints of factors, both tech inside and the data must be exchanged**.**
3. **Heterogeneity** ensures such IoT gadgets are based on extraordinary hardware and cross-cutting platform/network so they can interact effectively with other devices or system provider.
4. **Dynamic change in improved accuracy measurement:** A device state constantly changes (e.g. sleep, (dis)connect, speed, active, location, etc). These changes can result in faults. Number of devices can change flexibly. Thus, the system must be robust and adaptable so as learn these changes as well as measure accurately the products within the tank.
5. **Enormous scale:** The number of devices to be managed and communicated with will be an order of magnitude larger than the gadgets connected to the present-day Internet. Even more important may be the control of the information generated and its interpretation for software purposes. This relates to the semantics of data, as well as efficient data handling.
6. **Safety:** As benefits are gained from the IoT, safety must not be forgotten. As both the creators and recipients of the IoT, protection should be paramount inside the design. This consists of the safety of our records and the protection of our physical well-being. Securing endpoints, networks, and the data moving across all of it means creating a security model that will scale.
7. **Connectivity** permits community access and compatibility. Accessibility is getting into a community; And, compatibility seek to provide users with the unusual potentials of proposed system to consume and produce data.

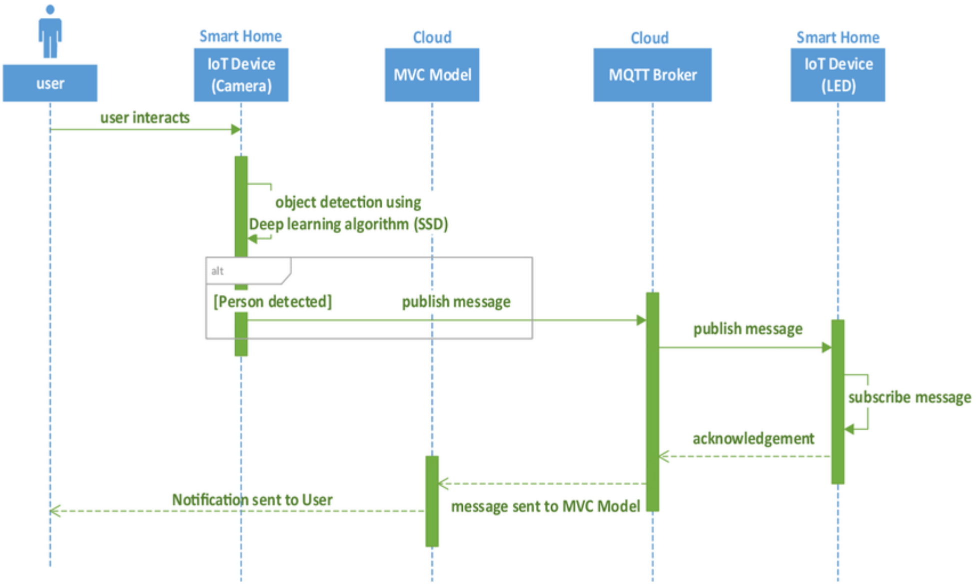

Figure 3. Sequence diagram of the proposed system

2.3. Technical Experimental Procedure

It involves both hardware and software parts (Chevalier et al., 2003; Ojugo et al., 2015; Ojugo & Eboka, 2014; Ojugo & Otakore, 2018a; Okobah & Ojugo, 2018; Tarafdar & Zhang, 2005):

1. **Input Design** acquires data via ultrasonic sensor, ESP32-microcontroller and other sensors. It then lets the user input via the web app interface to set threshold feats or parameters via the following:

- ✓ **Ultrasonic Sensor** as primary input device, measures the depth of the fuel and provides real-time data on fuel level.
- ✓ **ESP32** microcontroller is responsible for acquiring motion data and processing the acquired data.
- ✓ **BME280** detects movement as supplementary data.
- ✓ **Web App** interfaces with users to collect input parameters or set thresholds via the web app interface.

2. **Output Design** provide meaningful data to the users via the web app (Ojugo, Yoro, et al., 2013; Ojugo & Yoro, 2020a, 2020c). If motion or any anomalies are detected, the system generate alerts or notifications to inform users. To achieve notification, we set various feats: (a) threshold values for motion is set as 1 to trigger an alerts if the threshold is exceeded, and (b) alert is delivered via the web app, email and SMS as channels.

3. **Algorithm** is crucial for converting all measurements from the sensor into useful data (i.e. fuel level and volume data). Its steps are as thus, with the listing 1 below:

```
// Background modelling for occupancy detection
Loop capture video frame from the camera
  Apply Gaussian mixture model to extract data
  Identify foreground pixel deviations as occupant
  Output occupancy status and count
End loop
// PIR motion detection
Loop read analogue PIR sensor value
  if value exceeds the threshold:
    set motion detected flag
    start motion timer
  if the motion timer exceeds 5 seconds:
    clear motion detected flag
    stop motion timer
  output motion status
end loop
// Occupancy Tracking Algorithm
loop
if motion detected or camera occupancy count > 0:
    set zone occupancy status to OCCUPIED
  if motion is absent AND camera occupants > 0
for 60 seconds:
  set zone occupancy status to VACANT
```

```
    output zone occupancy status
    end loop
//Automation Control Algorithm
    loop check zone occupancy status
    if zone occupied:
     activate devices
        start device timers
      elseif zone vacant:
      stop device timers
      if device timers expired:
       deactivate devices
     endif
    end loop
```

2.4. Rationale for Proposed System

The system rationale and significance lies in its access control via the integration of advanced secured and user-friendly features – all of which improves user experiences and task efficiency with these feats (Allenotor et al., 2015; Allenotor & Ojugo, 2017; Ibor et al., 2023; Ojugo & Eboka, 2018):

1. **More data means better decisions** With added sensors, these devices can collect a large amount of data in many different areas.
2. **Ability to track/monitor:** Tracking data for use greatly benefits a user. IoTs have the ability to capture current motion and save as data (Aghware et al., 2023b).
3. **Lighten the workload with automation** Having a device doing most of the work for you means that you can save more time and cost. This reduces human efforts. It also results in devices being created that need little to no human intervention, allowing them to operate entirely on their own.
4. **Better Life** Having your devices track and order things, turn light switches off for you, and help manage important tasks that you may not have the time to do yourself certainly takes away a lot of stress (Malasowe et al., 2023; Ojugo, Akazue, Ejeh, Ashioba, et al., 2023; Ojugo, Ejeh, et al., 2023; Yoro, Aghware, Akazue, et al., 2023; Yoro, Aghware, Malasowe, et al., 2023).

3. RESULT AND DISCUSSION

3.1. Result Findings and Discussion

Figure 4 shows the generated system test results from the Blynk platform. The Blynk software was used to test the metrics for the proposed system.

The performance and capabilities of the system were critically validated during the testing procedure. Extensive testing under numerous conditions and scenarios revealed that the implementation satisfies the criteria for accurate occupancy detection, dependable automation, palpable energy savings, and user controls (Cerf, 2020; Charan et al., 2020; Manickam et al., 2022; Ojugo, Abere, et al., 2013; Ojugo, Yoro, et al., 2013).

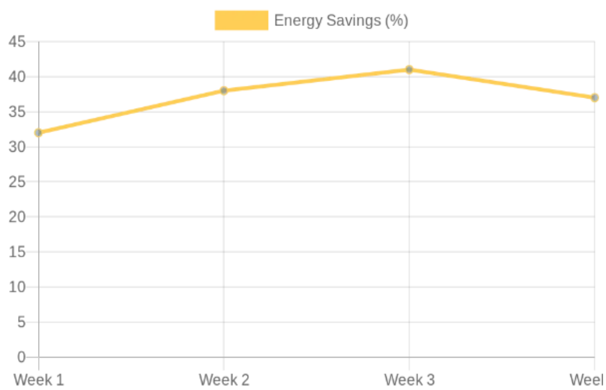

Figure 4. Test results from the Blynk software

A significant improvement was the computer vision algorithm, which during testing correctly detected occupancy events 95% of the time. Compared to manual usage and baseline tests without automation, automating device control based on precise occupancy data produced an average energy savings of 35%. The system implementation and testing process provided valuable insights into the performance and reliability of the smart home automation system (Ojugo et al., 2015; Ojugo & Eboka, 2019; Yoro & Ojugo, 2019). Key findings include:

1. The ESP32 successfully integrated all of the occupancy sensors, device controllers, cloud services, and other components into a cohesive system. Its

processing power, wireless capabilities, and flexible GPIO interfacing enabled robust prototyping.
2. The modular software design allowed each component to be developed and tested individually before full integration. The incremental build approach was efficient.
3. The Arduino IDE provided a familiar development environment and helpful debugging features for rapid programming. C++ delivered the right balance of hardware control, modularity, and algorithm implementation.
4. Extensive testing across a range of scenarios, use cases, and conditions validated the implementation meets all requirements and performs as expected.
5. The computer vision occupancy detection performed accurately, identifying motion events with 95% accuracy in testing. This was a major improvement over simpler sensors.

By comparing these with actual values, the system demonstrated a high level of accuracy and precision in determining the fuel level. This finding instils confidence in the reliability of system's core functionality (Ojugo & Yoro, 2020b). System observed that real-time updates were consistently responsive as the system efficiently captured and reflected changes in the fuel level, providing users with up-to-date information through the web app interface. This ensured that users could monitor the fuel level in real-time and take timely actions as needed (Brown and Armstrong, 2019).

4. CONCLUSİON

The study demonstrated that an IoT-based home automation system using multi-sensor occupancy detection and self-learning algorithms can provide substantial energy savings and user customization for smart home applications (Smith, 2020). The designed prototype system integrated affordable commercial devices like the ESP32 and ESP32-CAM to enable whole-home control based on real-time occupancy data. Testing showed a 35% average decrease in energy consumption compared to baseline non-automated usage, applying automation policies. Enhancements of the training algorithms, expanding compatible devices, and long-term testing would be beneficial, this work provides a foundation showing the promise of IoT automation and intelligence for reducing home energy usage. Our contributions to knowledge are on multi-sensor fusion, self-learning optimization, user-centric design, and efficacy evaluation help advance the state of the art and could inform future commercial solutions.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6), 94–100. https://doi.org/10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment analysis in detecting sophistication and degradation cues in malicious web contents. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 653.

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), 1756–1765. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1623–1633. https://doi.org/10.11591/ijeecs.v29.i3.pp1623-1633

Alade, A. A., Ajayi, O. B., Okolie, S. O., & Alao, D. O. (2017). Overview of the supervisory control and data acquisition (SCADA) system. *International Journal of Scientific & Engineering Research*, *8*(10), 478.

Alakbarov, R., & Hashimov, M. (2018). Application and Security Issues of Internet of Things in Oil-Gas Industry. *International Journal of Education and Management Engineering*, *8*(6), 24–36. https://doi.org/10.5815/ijeme.2018.06.03

Allenotor, D., & Ojugo, A. A. (2017). A Financial Option Based Price and Risk Management Model for Pricing Electrical Energy in Nigeria. *Advances in Multidisciplinary & Scientific Research Journal*, *3*(2), 79–90.

Allenotor, D., Oyemade, D. A., & Ojugo, A. A. (2015). A Financial Option Model for Pricing Cloud Computational Resources Based on Cloud Trace Characterization. *African Journal of Computing & ICT*, *8*(2), 83–92. www.ajocict.net

Bengherbia, B., Chadli, S., Zmirli, M. O., & Toubal, A. (2017). A MicroBlaze based WSN sink node using XBee transceiver. *Proceedings of 2016 8th International Conference on Modelling, Identification and Control, ICMIC 2016*, 831–834. https://doi.org/10.1109/ICMIC.2016.7804229

Braddock, R., & Chambers, C. (2011). Tank gauging systems used for bulk storage of gasoline. *Institution of Chemical Engineers Symposium Series*, *156*, 553–559.

Brown, K. W., & Armstrong, T. J. (2023). Hydrocarbon Inhalation. In *StatPearls*. http://www.ncbi.nlm.nih.gov/pubmed/24911841

Brown, W., & Armstrong, T. J. (2015). *Personnel Protection and Safety Equipment for the Oil and Gas Industries*. Elsevier. https://doi.org/10.1016/C2014-0-03648-9

Cerf, V. G. (2020). On the internet of medical things. *Communications of the ACM*, *63*(8), 5–5. https://doi.org/10.1145/3406779

Chang, J. I., & Lin, C.-C. (2006). A study of storage tank accidents. *Journal of Loss Prevention in the Process Industries*, *19*(1), 51–59. https://doi.org/10.1016/j.jlp.2005.05.015

Charan, D. S., Nadipineni, H., Sahayam, S., & Jayaraman, U. (2020). *Method to Classify Skin Lesions using Dermoscopic images*. arxiv.org/abs/2008.09418

Chevalier, K., Bothorel, C., & Corruble, V. (2003). Discovering Rich Navigation Patterns on a Web Site. In *Webometrics* (Vol. 5, Issue 6, pp. 62–75). https://doi.org/10.1007/978-3-540-39644-4_7

Datta, S. K., Shaikh, M. A., Srihari, S. N., & Gao, M. (2021). *Soft-Attention Improves Skin Cancer Classification Performance*. http://arxiv.org/abs/2105.03358

Gorawski, M., Gorawska, A., & Pasterak, K. (2015). *Liquefied Petroleum Storage and Distribution Problems* *and Research Thesis* (pp. 540–550). https://doi.org/10.1007/978-3-319-18422-7_48

Hurt, A. (2019). Internet of Medical Things emerges. *Dermatology Times*, *40*(10), 52–58. http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=138944526&site=ehost-live

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(992), 1–8. https://doi.org/10.46481/jnsps.2022.992

Ibrahim, H. A., & Syed, H. S. (2018). Hazard Analysis of Crude Oil Storage Tank Farm. *International Journal of ChemTech Research*, *11*(11), 300–308. https://doi.org/10.20902/IJCTR.2018.111132

Joshi, C., Aliaga, J. R., & Insua, D. R. (2021). Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Transactions on Information Forensics and Security*, *16*, 1131–1142. https://doi.org/10.1109/TIFS.2020.3029898

Joshi, P., Solomy, A., Suresh, A., Kachroo, K., & Deshmukh, P. (2020). Smart Fuel Station. *SSRN Electronic Journal*. doi.org/10.2139/ssrn.3572319

Kizilkaya, B., Ever, E., Yatbaz, H. Y., & Yazici, A. (2022). An Effective Forest Fire Detection Framework Using Heterogeneous Wireless Multimedia Sensor Networks. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *18*(2), 1–21. https://doi.org/10.1145/3473037

Ma, Y., Chen, X., Wang, L., & Yang, J. (2021). Study on Smart Home Energy Management System Based on Artificial Intelligence. *Journal of Sensors*, *2021*, 1–9. https://doi.org/10.1155/2021/9101453

Malasowe, B. O., Akazue, M. I., Okpako, E. A., Aghware, F. O., Ojie, D. V., & Ojugo, A. A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. *International Journal of Advanced Computer Science and Applications*, *14*(8), 135–142. https://doi.org/10.14569/IJACSA.2023.0140816

Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare. *Biosensors*, *12*(8). https://doi.org/10.3390/bios12080562

Meixell, B., & Forner, E. (2013). Out of Control : Demonstrating SCADA Exploitation. *Black Hat 2013*.

Nassar, R. H., & Al-Hajri, A. R. (2013, March 10). Field Experience with Still Pipes Installation and Supporting in KOC Storage Tanks. *All Days*. https://doi.org/10.2118/164155-MS

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

Ojugo, A. A., Abere, R. A., Orhionkpaiyo, B. C., Yoro, R. E., & Eboka, A. O. (2013). Technical Issues for IP-Based Telephony in Nigeria. *International Journal of Wireless Communications and Mobile Computing*, *1*(2), 58. https://doi.org/10.11648/j.wcmc.20130102.11

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Dependable Community-Cloud Framework for Smartphones. *American Journal of Networks and Communications*, *4*(4), 95. https://doi.org/10.11648/j.ajnc.20150404.13

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 1–11. https://doi.org/10.33633/jcta.v1i2.9259

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C., & Emordi, F. U. (2023). DeGATraMoNN : Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 667–678.

Ojugo, A. A., Allenotor, D., Oyemade, D. A., Yoro, R. E., & Anujeonye, C. N. (2015). Immunization Model for Ebola Virus in Rural Sierra-Leone. *African Journal of Computing & ICT*, *8*(1), 1–10. www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients. *African Journal of Computing & ICT*, *7*(3). www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2018). Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network. *Digital Technologies*, *3*(1), 1–8. https://doi.org/10.12691/dt-3-1-1

Ojugo, A. A., & Eboka, A. O. (2019). Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *8*(3), 128. https://doi.org/10.11591/ijict.v8i3.pp128-138

Ojugo, A. A., & Eboka, A. O. (2021). Modeling Behavioural Evolution as Social Predictor for the Coronavirus Contagion and Immunization in Nigeria. *Journal of Applied Science, Engineering, Technology, and Education*, *3*(2), 135–144. https://doi.org/10.35877/454RI.asci130

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015a). Framework design for statistical fraud detection. *Mathematics and Computers in Science and Engineering Series*, *50*, 176–182.

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015b). Hybrid Model for Early Diabetes Diagnosis. *2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, *50*, 55–65. https://doi.org/10.1109/MCSI.2015.35

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., & Emordi, F. U. (2023). Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework. *International Journal of Informatics and Communication Technology*, *12*(3), 205. https://doi.org/10.11591/ijict.v12i3.pp205-213

Ojugo, A. A., & Ekurume, E. O. (2021a). Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2090–2102. https://doi.org/10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Ekurume, E. O. (2021b). Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach. *International Journal of Education and Management Engineering*, *11*(2), 40–48. https://doi.org/10.5815/ijeme.2021.02.05

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021a). Empirical Evaluation for Intelligent Predictive Models in Prediction of Potential Cancer Problematic Cases In Nigeria. *ARRUS Journal of Mathematics and Applied Science*, *1*(2), 110–120. https://doi.org/10.35877/mathscience614

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021b). Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection. *ARRUS Journal of Engineering and Technology*, *2*(1), 12–23. https://doi.org/10.35877/jetech613

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ejeh, P. O., Adigwe, W., Anazia, K. E., & Nwozor, B. (2023). Forging a learner-centric blended-learning framework via an adaptive content-based architecture. *Science in Information Technology Letters*, *4*(1), 40–53. https://doi.org/10.31763/sitech.v4i1.1186

Ojugo, A. A., & Otakore, D. O. (2018a). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. *Network and Communication Technologies*, *3*(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2018b). Improved Early Detection of Gestational Diabetes via Intelligent Classification Models: A Case of the Niger Delta Region in Nigeria. *Journal of Computer Sciences and Applications*, *6*(2), 82–90. https://doi.org/10.12691/jcsa-6-2-5

Ojugo, A. A., & Otakore, O. D. (2020). Computational solution of networks versus cluster grouping for social network contact recommender system. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *9*(3), 185. https://doi.org/10.11591/ijict.v9i3.pp185-194

Ojugo, A. A., Ugboh, E., Onochie, C. C., Eboka, A. O., Yerokun, M. O., & Iyawa, I. J. B. (2013). Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria. *African Educational Research Journal*, *1*(2), 113–117. http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1216962&site=ehost-live

Ojugo, A. A., & Yoro, R. E. (2020a). Empirical Solution For An Optimized Machine Learning Framework For Anomaly-Based Network Intrusion Detection. *Technology Report of Kansai University*, *62*(08), 6353–6364.

Ojugo, A. A., & Yoro, R. E. (2020b). Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. *Technology Report of Kansai University*, *62*(08), 5933–5947.

Ojugo, A. A., & Yoro, R. E. (2020c). Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados. *Quantitative Economics and Management Studies*, *1*(4), 237–

248. https://doi.org/10.35877/454ri.qems139

Ojugo, A. A., Yoro, R. E., Oyemade, D. A., Eboka, A. O., Ugboh, E., & Aghware, F. O. (2013). Robust Cellular Network for Rural Telephony in Southern Nigeria. *American Journal of Networks and Communications*, *2*(5), 125. https://doi.org/10.11648/j.ajnc.20130205.12

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence. *International Journal of Computer Applications*, *179*(39), 34–43. https://doi.org/10.5120/ijca2018916586

Oliveira, R. M., Facina, M. S. P., Ribeiro, M. V., & Vieira, A. B. (2016). Performance evaluation of in-home broadband PLC systems using a cooperative MAC protocol. *Computer Networks*, *95*, 62–76. https://doi.org/10.1016/j.comnet.2015.12.004

Oyemade, D. A., & Ojugo, A. A. (2020). A Property Oriented Pandemic Surviving Trading Model. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 7397–7404. doi: 10.30534/ijatcse/2020/71952020

Oyemade, D. A., & Ojugo, A. A. (2021). An Optimized Input Genetic Algorithm Model for the Financial Market. *International Journal of Innovative Science, Engineering and Technology,* *8*(2), 408–419. https://ijiset.com/vol8/v8s2/IJISET_V8_I02_41.pdf

Oyemade, D. A., Ureigho, R. J., Imouokhome, F. ., Omoregbee, E. U., Akpojaro, J., & Ojugo, A. A. (2016). A Three Tier Learning Model for Universities in Nigeria. *Journal of Technologies in Society*, *12*(2), 9–20. doi: 10.18848/2381-9251/CGP/v12i02/9-20

Pradeepa, K., & Parveen, M. (2020). Solid State Technology 8060 A Survey on Routing Protocols With Security in Internet of Things A Survey on Routing Protocols With Security in Internet of Things. *International Virtual Conference on Emerging Trends in Computing*, *63*(4), 38–111.

Stouffer, K., Falco, J., & Scarfone, K. (2015). GUIDE to industrial control systems (ICS) security. *Gaithersburg, MD: National Institute of Standards and Technology*, 11–158.

Suleiman, R. F. R., & Reza, F. Q. M. I. (2019). Gas station fuel storage tank monitoring system using internet of things. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.6), 531–535. doi: 10.30534/ijatcse/2019/7881.62019

Tarafdar, M., & Zhang, J. (2005). Analyzing the influence of Web site design parameters on Web site usability. *Information Resources Management Journal*, *18*(4), 62–80. https://doi.org/10.4018/irmj.2005100104

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666. https://doi.org/10.1016/j.cose.2019.101666

Vågsholm, I., Arzoomand, N. S., & Boqvist, S. (2020). Food Security, Safety, and Sustainability—Getting the Trade-Offs Right. *Frontiers in Sustainable Food Systems*, *4*(February), 1–14. https://doi.org/10.3389/fsufs.2020.00016

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1943. doi: 10.11591/ijece.v13i2.pp1943-1953

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1922. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

Yoro, R. E., & Ojugo, A. A. (2019). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. *American Journal of Modeling and Optimization*, *7*(2), 35–41. doi: 10.12691/ajmo-7-2-1

Yu, Y., Li, M., Liu, L., Li, Y., & Wang, J. (2019). Clinical big data and deep learning: Applications, challenges, and future outlooks. *Big Data Mining and Analytics*, *2*(4), 288–305. doi:10.26599/BDMA.2019.9020007

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers and Security*, *104*. https://doi.org/10.1016/j.cose.2021.102221

Zardi, H., & Alrajhi, H. (2023). Anomaly Discover: A New Community-based Approach for Detecting Anomalies in Social Networks. *International Journal of Advanced Computer Science and Applications*, *14*(4), 912–920. https://doi.org/10.14569/IJACSA.2023.01404101

Zawislak, P. A., Reichert, F. M., Barbieux, D., Avila, A. M. S., & Pufal, N. (2022). The dynamic chain of innovation: bounded capabilities and complementarity in agribusiness. *Journal of Agribusiness in Developing and Emerging Economies*, *23*, 1–113. doi: 10.1108/JADEE-04-2021-0096

Zhang, S., Gao, D., Lin, H., & Sun, Q. (2019). Wildfire Detection Using Sound Spectrum Analysis Based on the Internet of Things. *Sensors*, *19*(23), 5093. https://doi.org/10.3390/s19235093