Journal of Computer Science and Information Technology

DOI: 10.61424/jcsit
Journal Homepage: www.bluemarkpublishers.com/index.php/JCSIT

JCSIT
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

The Application of IoT in Grain Storage Management for the Food Reserve Agency

Robbin Mchinzi[1] ✉ and Daliso Banda[2]
[12]University of Zambia, School of Engineering, Department of Electrical and Electronics
Corresponding Author: Robbin Mchinzi, **E-mail**: robbinmchinzi@gmail.com

| ABSTRACT

The Food Reserve Agency (FRA) plays a crucial role in Zambia's food security, yet inefficiencies in manual stock management, environmental monitoring, security, and logistics hinder its effectiveness. This study proposes an IoT-based model to automate monitoring, enhance security, and optimize grain storage management through real-time data collection. The IoT prototype integrates DHT11 (temperature and humidity), PIR motion, rain, flame, gas, and light sensors with an ESP32 NodeMCU, SMS-based alerts, and SSL encryption for secure data transmission. Experimental results from the storage facility detected temperature spikes of 32.8°C, indicating potential pest infestation risks, while motion sensors identified object movements. Additionally, database performance analysis showed the non-aggregated data insertion algorithm (4.44 records/sec) outperformed the aggregated approach (0.29 records/sec), emphasizing the need for optimized data handling in IoT implementations. These findings confirm that the proposed IoT-driven storage system effectively mitigates FRA's operational challenges by automating stock tracking, improving environmental monitoring, enhancing security, and optimizing logistics, contributing to IoT-based agricultural advancements and sustainable food security solutions.

| KEYWORDS

Food security, grain storage, IoT, data aggregation, real-time monitoring

| ARTICLE INFORMATION

ACCEPTED: 21 March 2025 **PUBLISHED:** 11 April 2025 **DOI:** 10.61424/jcsit.v2.i1.238

1. Introduction

Ensuring food security for a global population projected to reach 9 billion by 2050 presents a formidable challenge. Food production must increase significantly to meet demand, yet post-harvest losses remain a major obstacle. According to the Food and Agriculture Organization (FAO) [1], approximately 30% of global food production is lost annually due to inadequate storage, poor transportation, and inefficient handling practices.

In many developing countries, traditional grain storage methods lack effective environmental monitoring and control, making them highly susceptible to pest infestations, Mold growth, and humidity fluctuations, leading to significant losses [2]. The Food Reserve Agency (FRA) maintains the national food reserves in Zambia. Still, it faces challenges managing its storage facilities due to limited technological adoption and reliance on manual monitoring systems [3].

The Internet of Things (IoT) offers a promising solution by enabling real-time monitoring, automation, and data-driven decision-making in grain storage. IoT sensors can track critical environmental parameters such as temperature, humidity, and air quality, reducing spoilage and ensuring optimal storage conditions [4]. Various studies highlight IoT's effectiveness in agricultural applications, including precision farming, irrigation management, and supply chain optimization [5]. However, the specific application of IoT in grain storage management, particularly in Zambia, remains underexplored.

The adoption of IoT in grain storage management can significantly reduce post-harvest losses by enabling continuous environmental monitoring, automated responses to adverse conditions, and predictive analytics for early detection of spoilage risks [6]. Additionally, advanced data analytics and cloud computing enhance storage efficiency through predictive maintenance, automated stock tracking, and real-time alerts [7]. This study is the first to experiment with the environmental conditions in the Food reserve storage facilities.

1.1 Grain Storage and Food Security

Food security is a major global concern, particularly in developing nations where post-harvest grain losses account for 20–30% of production due to inadequate storage conditions [1]. The Food and Agriculture Organization (FAO) defines food security as the availability, accessibility, and stability of food supply, with effective storage playing a pivotal role in achieving this goal. Ensuring proper grain storage minimizes losses, maintains quality, and extends the shelf life of staple foods.

1.2 Post-Harvest Losses

Post-harvest losses represent a significant challenge in grain storage, impacting food availability and economic stability. These losses occur at multiple stages, including harvesting, storage, processing, distribution, and marketing. During harvesting and handling, mechanical damage caused by poor handling techniques reduces grain viability and overall yield [1]. Storage and processing losses arise from inadequate aeration, poor moisture control, and pest infestations, which lead to Mold growth, aflatoxin contamination, and grain deterioration [2]. In the distribution and market phase, spoiled grains often fail to meet safety standards, resulting in financial losses for farmers and supply chain actors [3]. Addressing these issues requires efficient storage management systems integrating real-time monitoring and automated control mechanisms to detect and prevent spoilage.

1.3 The Role of IoT in Agricultural Storage Management

The Internet of Things (IoT) has revolutionized agricultural storage management by enabling automation, remote monitoring, and predictive analytics for improved efficiency [4]. IoT-based solutions have been widely implemented in various agricultural applications, including precision farming, supply chain traceability, and smart warehousing. In precision farming, IoT technology is used to monitor soil moisture, irrigation, and crop health, allowing farmers to optimize resource use and increase productivity [5]. For supply chain traceability, RFID and blockchain technologies improve grain tracking from farms to warehouses, ensuring transparency and reducing losses due to mismanagement [6]. In smart warehousing, sensor-driven climate control systems maintain optimal storage conditions for perishable crops, thereby extending their shelf life and preventing spoilage [7]. These applications demonstrate the potential of IoT to enhance grain storage through real-time monitoring and automated responses to environmental changes.

1.4 IoT-Based Environmental Monitoring in Grain Storage

IoT technology allows for real-time tracking of key environmental factors such as temperature, humidity, and air quality, thereby reducing spoilage risks and improving storage efficiency. Several key components facilitate IoT-based monitoring in grain storage. DHT11 temperature and humidity sensors detect fluctuations that could affect grain moisture content and lead to spoilage. MQ-2 gas sensors monitor CO_2 and methane levels, which are indicators of spoilage and pest infestations within storage units [8]. PIR motion sensors enhance security by detecting unauthorized access to storage facilities and alerting storage managers to potential security threats [9]. Automated aeration systems utilize smart fans to maintain airflow and prevent the accumulation of excess moisture, thereby reducing the risk of fungal growth and maintaining optimal storage conditions [1]. Research has shown that

IoT-based grain storage solutions can reduce losses by up to 20% through continuous monitoring, early detection of spoilage, and automated climate control [4].

1.5 Security and Automation in Grain Storage

The IoT technology in grain storage presents significant benefits but also introduces cybersecurity challenges that must be addressed to ensure data integrity and prevent unauthorized access. Cybersecurity risks in IoT-based storage systems include data breaches, hacking threats, and data integrity issues. Unauthorized access to IoT devices can result in the manipulation of sensor readings, leading to deliberate spoilage or theft of stored grains [10]. IoT networks, which primarily rely on wireless communication protocols, are vulnerable to cyberattacks that could compromise system functionality and data security [9]. False sensor readings can be introduced into storage records without encryption and authentication, leading to mismanagement and financial losses.

1.6 IoT-Based Security Enhancements

Modern IoT frameworks incorporate advanced security measures such as SSL/TLS encryption, blockchain-based data integrity mechanisms, and role-based access control to mitigate security risks. SSL/TLS encryption protects data transmission between IoT devices and cloud servers, ensuring that sensor data remains secure and inaccessible to unauthorized users [11]. Blockchain technology enhances data integrity by maintaining tamper-proof stock records, thereby preventing fraudulent activities such as inventory manipulation or misreporting [12]. Additionally, role-based access control (RBAC) restricts unauthorized data access within the FRA storage network by ensuring that only authorized personnel can modify or retrieve sensitive storage information [9]. Implementing these security enhancements strengthens the reliability of IoT-based grain storage systems and ensures long-term operational efficiency.

1.7 Business Process Optimization for Grain Storage

Studies on grain storage logistics highlight inefficiencies in inventory tracking, stock dispatch, and quality control, particularly within the FRA [13]. The reliance on manual stock management results in inconsistencies in records, leading to discrepancies between reported and actual stock levels [6]. Additionally, the absence of real-time environmental tracking causes delays in fumigation and aeration, increasing the risk of spoilage. Security vulnerabilities further exacerbate storage inefficiencies, as FRA warehouses lack automated surveillance systems, making them susceptible to theft and fraud [9].

1.8 Proposed Business Process Optimization Framework

The introduction of RFID and QR code-based stock monitoring reduces human errors in inventory tracking and ensures accurate stock records [12]. Automated pest and spoilage alerts utilize IoT sensors to trigger SMS notifications, enabling proactive fumigation and pest control interventions [8]. Furthermore, real-time dashboard analytics provide predictive maintenance and supply chain optimization, allowing storage managers to respond swiftly to environmental changes and logistical requirements [11].

2. Methodology

2.1 Research Setting

The study was conducted at the Mwembeshi FRA depot on Manda Road, Light Industrial Area, Lusaka, Zambia. The site map is shown in Fig. 1.

Fig. 1. FRA Mwembeshi Satellite Depot

2.2 Data Collections

The baseline study provided essential insights into FRA's grain storage operations, integrating qualitative and quantitative methods. A literature review explored best practices, challenges, and research gaps in IoT-enabled storage management [14]. Field observations at FRA depots assessed inventory management, environmental monitoring, and storage capacity, bridging theoretical knowledge with real-world operations [15]. Semi-structured interviews with key stakeholders highlighted operational challenges and opportunities for improvement while ensuring ethical considerations such as consent and confidentiality [16]. These findings informed the development of an IoT-based storage system tailored to FRA's needs, and the data obtained from the prototype was analysed using Excel.

2.3 Functional requirements

The IoT-based grain storage monitoring system incorporates stakeholder-defined needs and research-driven functional specifications. Stakeholders emphasized the necessity of temperature and humidity monitoring to prevent grain spoilage, leading to the specification of DHT11 sensor thresholds (15-25°C for temperature, 30-65% for humidity). Similarly, concerns over unauthorized access and theft informed the inclusion of the HC-SR501 PIR sensor, set to detect movement within 3-7 meters.

Where stakeholders lacked precise technical details, the research provided industry benchmarks. For instance, the MQ-2 gas sensor thresholds (CO_2 > 600 ppm, ammonia > 25 ppm, methane > 1000 ppm) were established based on safety and environmental standards. Fire detection specifications, including the flame sensor's wavelength sensitivity (760-1100 nm) and range (100 cm), were derived from fire hazard research. Additionally, the LDR light sensor threshold (>200-300 lux) was specified based on security research to detect unexpected light exposure, indicating potential entry.

This combination of stakeholder input and research-backed specifications ensures a comprehensive and scientifically validated IoT system for grain storage management (FAO, 2021) [49].

2.4 Materials

The following hardware and software materials were selected for the study based on the stakeholders' input and research.

2.5 ESP32 NodeMCU 32s
The ESP32 NodeMCU 32s, manufactured by Shenzhen KEYES Robot Co. Ltd, was used as the development board. This microcontroller served as the central processing unit, handling sensor integration, real-time data processing, and communication. It operates on 5V power, Wi-Fi (ESP-WROOM-32), Bluetooth 4.2, and has a dual-core ESP32-D0WDQ6 processor, making it ideal for IoT applications. Its compact dimensions (48.26mm × 25.4mm) allow for easy integration into embedded systems.

2.6 Sensors
This study used sensors, such as the DHT11, to measure temperature (0-50°C) and humidity (20-90%) with an accuracy of ±5% RH and ±2°C. The HC-SR501 infrared motion sensor, with a range of 3-7 meters, was used for security monitoring, detecting object movements within the facility. A rain sensor operating at 3.3V-5V was included to detect raindrops, alerting managers to possible water damage risks. A flame sensor capable of detecting infrared wavelengths (760-1100 nm) within 100 cm was integrated to provide fire hazard detection, ensuring early warnings. Additionally, the MQ-2 gas sensor monitored LPG, smoke, CO_2 (>600 ppm), Ammonia (>25 ppm), and Methane (>1000 ppm), helping to prevent air contamination and potential hazards. The light-dependent resistor (LDR) sensor, operating at 3.3V-5V, was used to detect light exposure (>200-300 lux), which is critical for identifying open storage areas that could compromise security.

2.7 Connectivity
Connectivity tools were employed to ensure seamless integration and communication among components. A breadboard was used for circuit prototyping, allowing easy sensor testing without permanent connections. Jumper wires from Micro Elektronika, with a length of 15cm, facilitated modular connectivity between components, while a micro-USB cable was used for uploading the firmware from the Arduino IDE to the ESP32, for supplying power to the ESP32, rated at 20mVAC voltage and 1.8A current capacity.

2.8 Actuators
The Sunon EEC0251B2-000U-A99 is a 120x120x25mm DC axial fan designed for efficient cooling. It operates at 12V DC, consuming 3.4W of power with a current draw of 0.279A. The fan delivers an airflow of 93.0 CFM (158 m^3/h) at a speed of 2700 RPM, producing a noise level of 40.5 dB(A). Built with ball bearing technology for enhanced durability, it features an auto-restart function and has a lifespan of 70,000 hours at 40°C. The frame and blades are made from polybutylene terephthalate (PBT) and operate at 6 to 13.8V DC.

2.9 Power Supply
Due to the lack of electrical power in the storage facility and the load shading the country has been experiencing, a solar-powered energy system was implemented. A 12V, 60Ah Exide battery provided backup power, while a 200W solar panel ensured continuous operation. A charging controller was included to prevent battery overcharging, and an inverter (12V to 220V AC) converted DC power from the battery to AC, enabling power supply to computing devices and network components.

2.10 Computing Devices
The computing devices were employed. An HP laptop served as the central hub for database storage and system integration, featuring 16GB RAM, a 2.90GHz Core i7 (13th Gen) processor, and running on Windows 11 Home with a Realtek RTL8822CE 802.11ac wireless adapter. A Dell laptop was used for client-side monitoring, debugging, and testing, equipped with 4GB RAM and a 1.60GHz processor supporting 802.11/g/n wireless connectivity. Additionally, an Infinix mobile phone with an octa-core processor, 4GB+1GB RAM, 64GB ROM, and a 6000mAh battery provided mobile access to the IoT dashboard, allowing storage managers to monitor environmental conditions remotely.

2.11 Software Tools

Several software tools were used for system development, network security, and data analysis. XAMPP (v3.3) hosted the MySQL database and Apache web server, enabling real-time data storage and retrieval. Arduino IDE (v2.3.4) was used for writing, compiling, and uploading firmware to the ESP32 microcontroller. Wireshark monitored network traffic and data security, ensuring secure communication between IoT devices and the server. Creately was used to design UML diagrams for IoT architecture and workflow mapping, while Mendeley managed research references and citations. An SMS API was integrated into the system to send real-time alerts to storage managers when anomalies were detected. Microsoft Excel (MS365) was used for data analysis and visualization.

2.12 IoT Architecture

The IoT architecture in this study follows a Six-layer model consisting of the Sensor Layer, Control Layer, Network Layer, Data Processing Layer, Security Layer, and Application Layer, as shown in Fig 2. IoT Architecture.

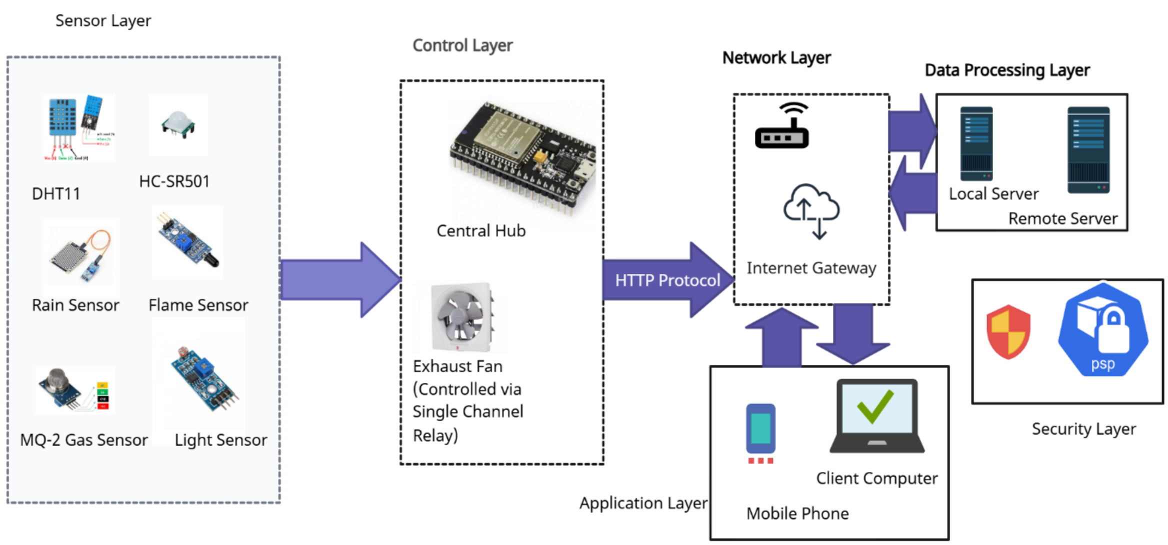

Fig 2. IoT Architecture

Before physically assembling the components, it is essential to first design a schematic circuit diagram to verify and test the connections. This approach ensures that all components function correctly and interact as expected before physical implementation. The schematic diagram in Fig 3. IoT Schematic Circuit Diagram serves as a blueprint for the actual hardware setup, minimizing errors and improving system reliability. According to [17], creating a schematic diagram allows for early detection of wiring issues and prevents potential hardware failures. Additionally, IEEE standards for circuit design emphasize the importance of simulation and validation before physical assembly to enhance system efficiency and durability [18].

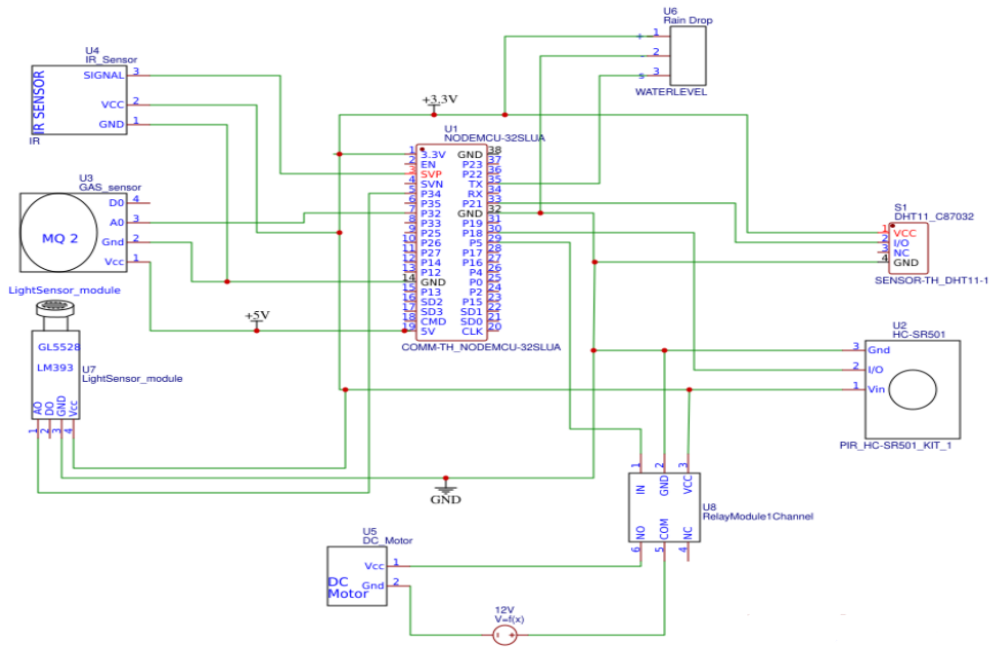

Fig 3. IoT Schematic Circuit Diagram

The method used to develop the IoT prototype is shown in Fig 4. IoT Method

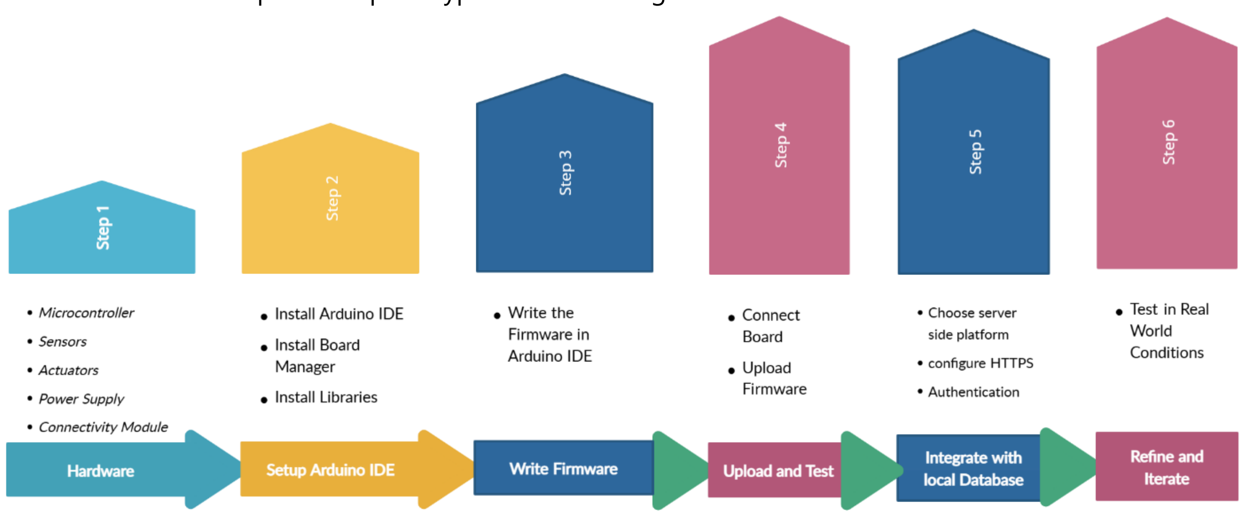

Fig 4. IoT Method

3. System Design

3.1 Algorithms

In this study, two IoT algorithms, aggregated and non-aggregated, were developed and tested using an ESP32 microcontroller, interfacing with multiple sensors. These algorithms were designed to collect and transmit environmental data to a database for real-time monitoring and analysis. The aggregated algorithm in Fig 5. Aggregated Algorithmfocused on optimizing data transmission by selectively adding only sensor readings that met or exceeded predefined threshold values to the payload. When the DHT11 sensor reads the temperature and humidity, the ESP32 will only add readings to a payload when they exceed critical thresholds, and the ESP32 triggers alerts when the PIR sensor detects an object. ESP32 continued to analyze data from all the sensors and allowed only data beyond or within the threshold. This method significantly reduced the amount of data being transmitted, conserving bandwidth and processing power [19]. Studies have shown that selective data aggregation in IoT systems improves system efficiency and reduces energy consumption in wireless sensor networks [20]. focused on optimizing data transmission by selectively adding to the payload only sensor readings that met or exceeded predefined threshold values.

In contrast, the non-aggregated algorithm continuously collected and transmitted sensor data, regardless of whether the values exceeded any threshold. Every reading from DHT11, PIR sensor, rain sensor, flame sensor, MQ-2 gas sensor, and light sensor was added to the payload and sent to the database, as shown in **Error! Reference source not found.**. In contrast, this approach ensured a complete dataset for historical analysis and the database [21]. Previous research highlights that non-aggregated IoT systems provide high data granularity but can overwhelm networks with redundant or non-actionable information [22].

3.2 Implementation of SSL

HTTPS was implemented on the XAMPP server to enhance security by enabling encrypted communication. The process began with generating self-signed SSL certificates using OpenSSL through a batch file. The batch script created necessary directories for storing certificates and keys defining the Subject Alternative Names (SAN) to include localhost, local domain, and the static IP xxx.xxx.xx.xxx. The script then executed OpenSSL commands to generate certificates and keys for each domain and IP. After generating the certificates, the Apache configuration in XAMPP was updated to enable SSL by modifying the httpd-ssl.conf file. This included specifying the paths to the SSL certificate and key files, binding the server to the appropriate IP address and ports, and defining virtual hosts for HTTPS. Once the configuration was complete, the Apache server was restarted to apply the changes, and HTTPS functionality was successfully tested on the local environment, ensuring secure access to the specified localhost domain and IP addresses.

3.3 Data Replication

The replication method employed in this study involved creating a robust and efficient mechanism for synchronizing data between a client-side database and a central server database. The client-side system logged data locally into a MySQL database, capturing essential fields such as thing_id, description, value, and date_created. To ensure seamless data synchronization, a PHP script was developed to identify unsynced records by querying a sync_log table. These records were packaged into JSON format and transmitted to the server using HTTP POST requests facilitated by cURL.

On the server side, a dedicated script was designed to handle incoming data. It validated the JSON payload, checked for the presence of required fields, and inserted the data into the server database using prepared statements to enhance security and prevent SQL injection. Acknowledgments were sent back to the client, indicating the success or failure of each transaction. For automation, the Windows Task Scheduler was configured to execute the synchronization scripts at predetermined intervals, reducing the need for manual intervention.

This replication method was tested for reliability, with error-handling mechanisms integrated to manage scenarios such as invalid data formats, connection failures, and duplicate entries. Debug logs and a dedicated sync_log table were used to monitor synchronization activities and address issues promptly. This method ensured accurate and timely data replication, maintaining data consistency and supporting real-time decision-making in the system.

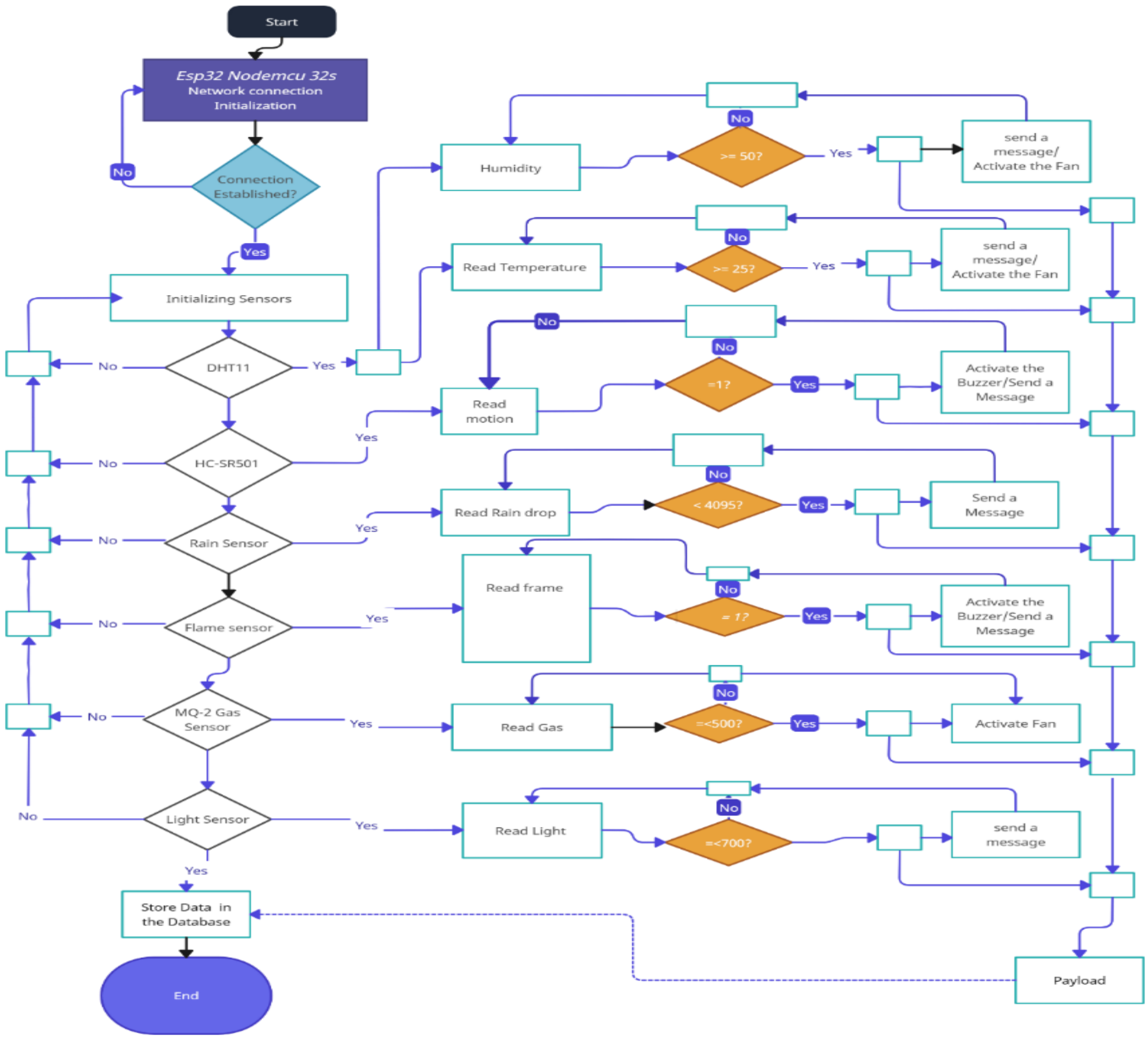

Fig 5. Aggregated Algorithm

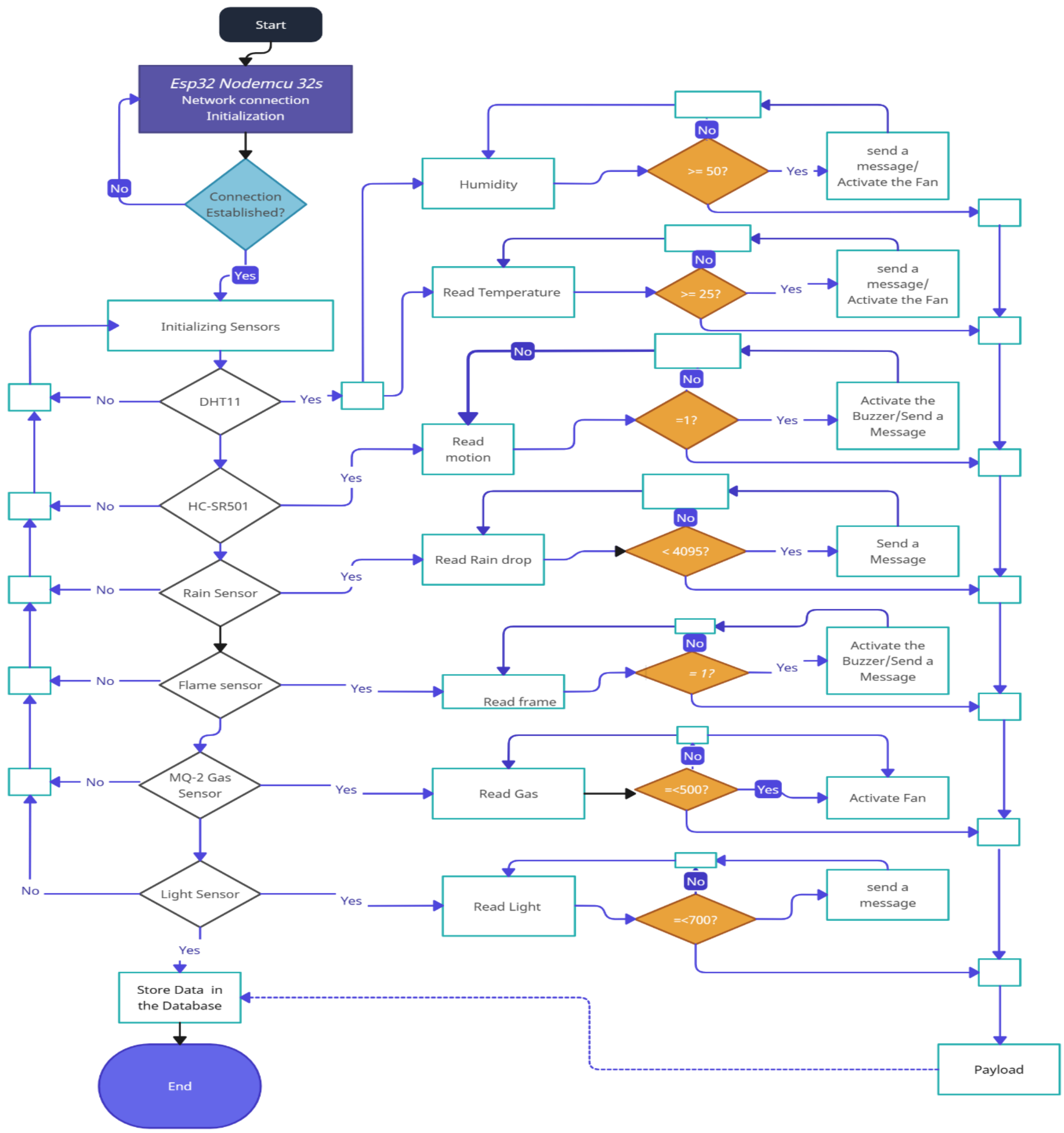

Fig 6. Non-Aggregated Algorithm

3.4 Deployment and Field Testing

Finally, the system was deployed in a real-world grain storage facility to assess its effectiveness in the target environment. This field-testing phase provided valuable insights into the system's long-term reliability, and the findings were compared with guidelines set by the Food and Agriculture Organization (FAO) on IoT-based smart agriculture.

Fig 7. Prototype Setup in the Shade

Fig 7. Prototype Setup in the Shade

3.5 Experiment Design for IoT Prototype

The prototype was deployed in section G4 of the storage facility. It contained eight-grain stack bags: six stacks, each holding 15,000 50 kg bags; one stack contained 12,000 50 kg bags; and the final stack contained 12,229 50 kg bags. The IoT prototype was strategically placed between the stack of 12,000 bags and the stack of 12,229 bags to maximize data accuracy.

A local area network was configured to facilitate communication between the system components. Two laptops, an HP and a Dell, were connected to the network. The HP laptop was designated for development and acted as a client-local server, while the Dell laptop was set up as a remote server for testing data replication. A mobile phone was included as a client device for real-time monitoring.

Since the facility lacked direct electrical power, the inverter was used, as shown in Fig 8. Prototype Setup in the Shade Once the setup was completed, the facility was sealed for 30 minutes before being reopened to assess the system performance. The data collected during the experiment was analyzed using Excel.

4. Results and Discussion

The study successfully designed and assessed an IoT prototype that enhances the monitoring of FRA storage facilities. The IoT prototype successfully demonstrated its ability to automate environmental monitoring and security, and optimize data handling in FRA's grain storage facilities. The experiment confirmed that temperature monitoring is crucial in detecting conditions that could lead to pest infestations, as evidenced by the 32.8°C peak temperature recorded during testing in Fig 8. Temperature reading from the Shade That aligns with [8], which shows that pests have a developmental range for many stored grain insects of approximately 25–35°C. FRA staff, on the other hand, indicated that the Food Reserve Agency has been struggling with pest infestation and that there are no temperature reading instruments, leading to no records of temperature readings from the storage facilities.

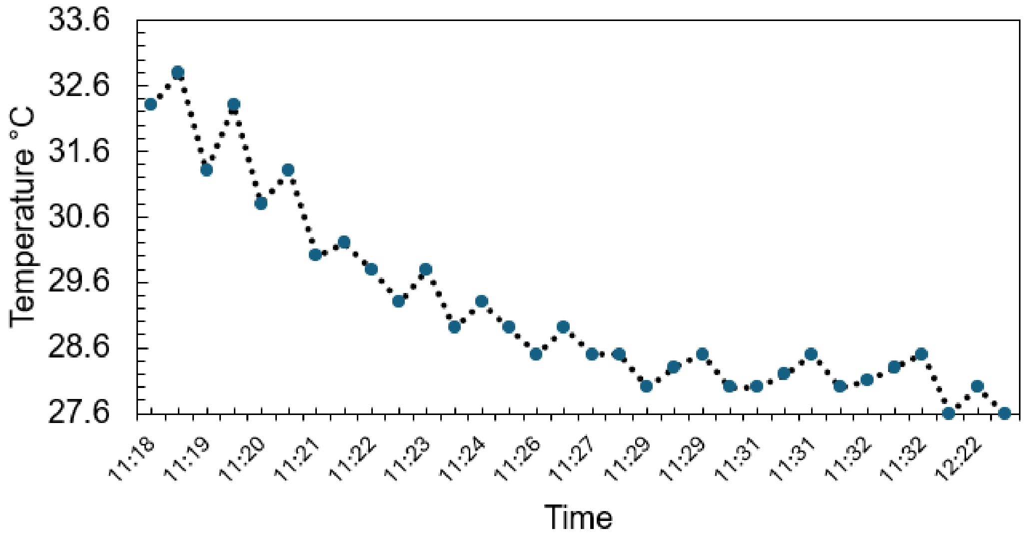

Fig 8. Temperature reading from the Shade

Additionally, motion detection was dependable, with the system successfully identifying three object movements, as shown in Fig 9. Motions Detected, all attributing to the researcher and FRA staff during deployment. This validated the system's effectiveness in detecting activity within storage areas.

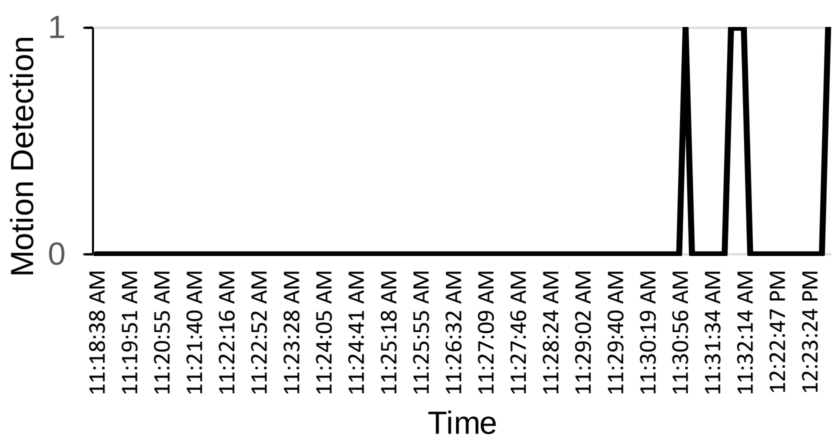

Fig 9. Motions Detected

Furthermore, real-time SMS alerts are shown in Fig 11. SMS Alerts Data encryption significantly enhanced data security and communication, ensuring immediate response to grain storage facility anomalies. The data replication improved system resilience, preventing data loss and ensuring consistent record-keeping. The throughput analysis revealed that non-aggregated data insertion provided superior performance, emphasizing the need for database optimization in IoT implementations to balance efficiency and data availability.

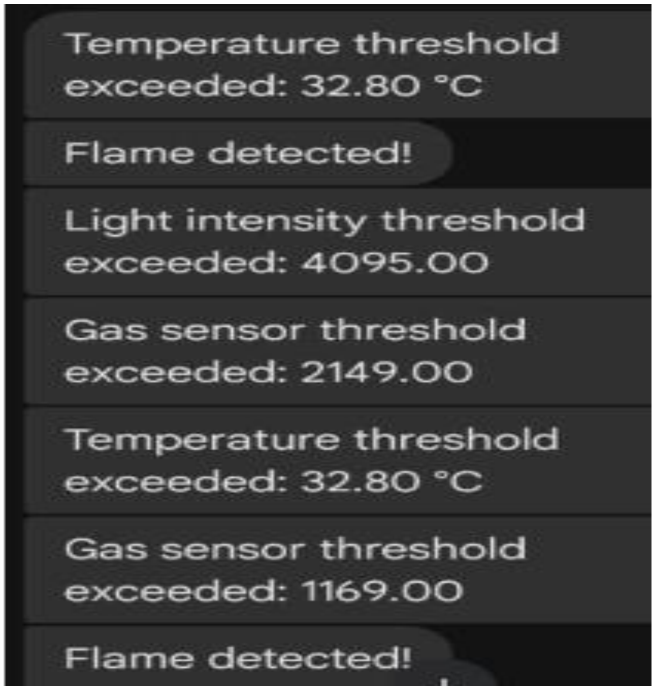

Fig 10. SMS Alerts

A comparison of database insertion algorithms in Table 1. Aggregation Algorithms Performance demonstrated that the non-aggregated algorithm (4.44 records/sec) outperformed the aggregated method (0.29 records/sec), highlighting the need for optimized data handling strategies in IoT implementations. The findings confirm that the proposed IoT model effectively automates stock tracking, enhances environmental monitoring, and improves security and logistics management, making a significant contribution to food security and modernizing grain storage practices.

Table 1. Aggregation Algorithms Performance

Algorithm	Number of Records	Duration
Non-Aggregated	*7995*	30 min
Aggregated	520	30 min

Aggregated Algorithm: A total of 520 records were inserted.

Percentage: $\frac{520}{8515} x\ 100 = 6.1\%$

Non-Aggregated Algorithm: A total of 7,995 records were inserted. Percentage: $\frac{7995}{8515} x\ 100 = 93.9\%$

Throughput comparison of aggregated and non-aggregated algorithms

$$\text{Throughput} = \frac{\textit{Number of Records Inserte}}{\textit{Time Taken for Insertion}} \qquad \text{Equation 1}$$

Converting 30 minutes to seconds = 30 x 60 = 1800 seconds

$$\text{Throughput for aggregated} = \frac{520\ \textit{Records}}{1800\ \textit{seconds}} = 0.29\ \text{records/seconds}$$

$$\text{Throughput for Non aggregated} = \frac{7995\ \textit{Records}}{1800\ \textit{seconds}} = 4.44\ \text{records/seconds}$$

The storage facility's environmental conditions were remotely monitored using a dashboard, as shown in Fig 11. Dashboard View

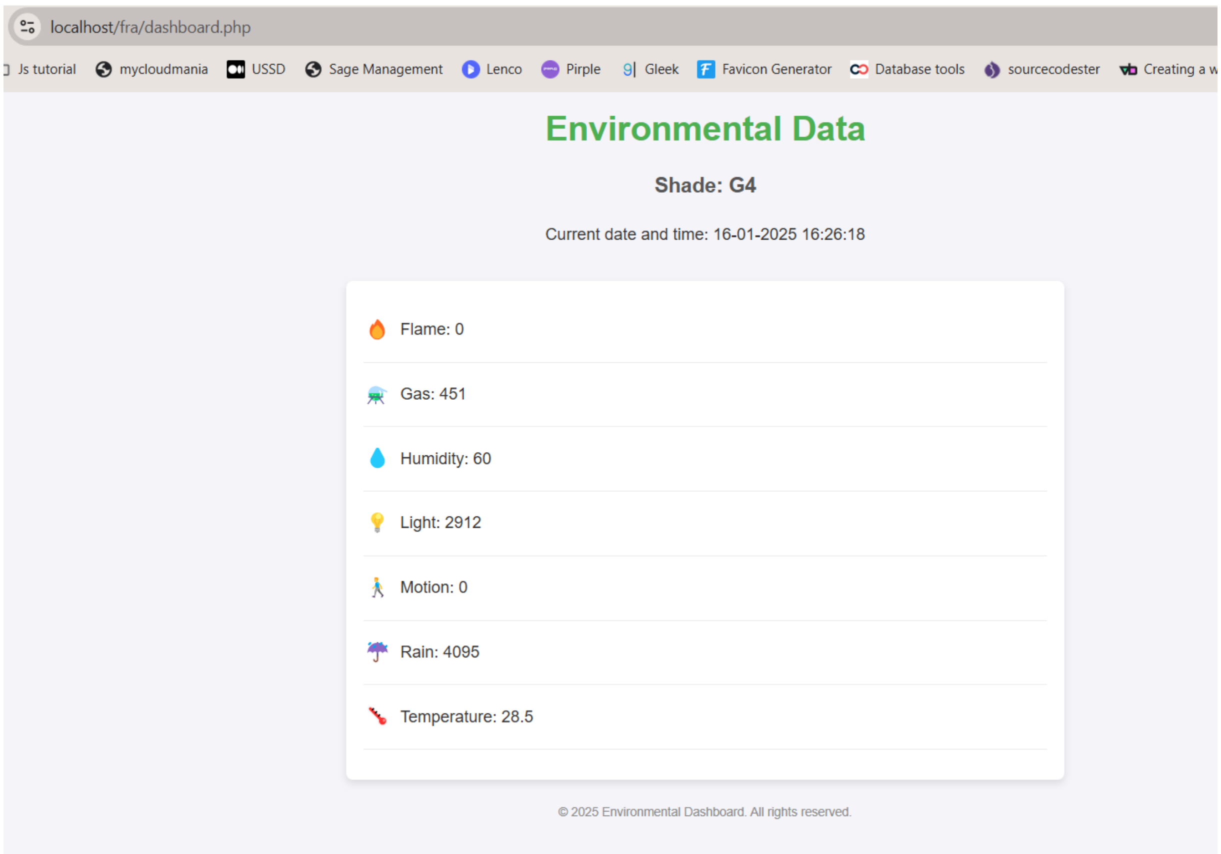

Fig 11. Dashboard View

5. Conclusion of the Study

The study explored the Application of IoT in Grain Storage Management for the Food Reserve Agency (FRA), aiming to enhance efficiency, security, and environmental monitoring. The findings revealed several inefficiencies in FRA's current storage management, including manual stock tracking, inadequate environmental monitoring, security vulnerabilities, logistical delays, and outdated fumigation methods.

To address these challenges, an IoT-based prototype was designed and tested. The prototype successfully integrated multiple sensors (temperature, humidity, motion, rain, flame, gas, and light sensors) with an ESP32 NodeMCU, providing real-time data monitoring and alerts. The results showed that temperature and humidity monitoring helped detect pest infestation risks, motion sensors enhanced security, and real-time data analysis improved decision-making. The system also incorporated SSL encryption to enhance security and prevent data breaches.

5.1 Future Work and Recommendations

To expand the impact of IoT in grain storage management, future research should focus on:

- Scaling IoT implementation to multiple FRA storage depots nationwide.
- Integrating AI and machine learning for predictive analytics in grain storage.
- Enhancing connectivity by combining Wi-Fi, LoRaWAN, and satellite communication.
- Implementing blockchain technology for enhanced data security and transparency.

5.2 Policy recommendations include:

- Developing a National IoT Strategy for Agriculture.
- Providing financial incentives for IoT adoption.
- Enhancing training and capacity building for FRA personnel.
- Establishing legislation for mandatory real-time storage monitoring.

In conclusion, this study demonstrated that IoT-driven innovations can transform grain storage management, reducing post-harvest losses, improving efficiency, and ensuring food security in Zambia.

Acknowledgments

I would like to express my sincere gratitude to the University of Zambia for providing the academic platform and resources necessary for the completion of this research.

I extend my deepest appreciation to my supervisor, whose guidance, patience, and insightful feedback were invaluable throughout the research process. Your expertise and encouragement played a crucial role in shaping this study.

I am also grateful to the Food Reserve Agency (FRA) of Zambia for granting me access to their facilities and allowing me to conduct field studies. Special thanks to the staff members who shared their knowledge, experiences, and valuable insights, which greatly enriched the study.

To my family and friends, your unwavering support, encouragement, and understanding throughout this journey have been my greatest source of motivation.

Lastly, I extend my appreciation to all researchers and experts in the field of IoT and grain storage management whose work served as an inspiration for this study.

This research would not have been possible without the support and contributions of these individuals and institutions.

References

[1] S. McGuire, "FAO, IFAD, and WFP. The State of Food Insecurity in the World 2015: Meeting the 2015 International Hunger Targets: Taking Stock of Uneven Progress. Rome: FAO, 2015," *Advances in Nutrition*, vol. 6, no. 5, pp. 623–624, Sep. 2015, doi: 10.3945/an.115.009936.

[2] D. W. Hagstrum, C. Reed, and P. Kenkel, "Management of stored wheat insect pests in the USA," 1999. doi: 10.1023/A:1009682410810.

[3] J. Coulter, J. Sondhi, and R. Boxall, "The economics of grain warehousing in sub-Saharan Africa," *Savings and Development*, vol. 24, no. SUPP, 2000.
[4] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. H. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2932609.
[5] S. Wolfert, L. Ge, C. Verdouw, and M. J. Bogaardt, "Big Data in Smart Farming – A review," 2017. doi: 10.1016/j.agsy.2017.01.023.
[6] L. Ruiz-Garcia and L. Lunadei, "The role of RFID in agriculture: Applications, limitations and challenges," *Comput Electron Agric*, vol. 79, no. 1, 2011, doi: 10.1016/j.compag.2011.08.010.
[7] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, "Internet of Things in agriculture, recent advances, and future challenges," *Biosyst Eng*, vol. 164, 2017, doi: 10.1016/j.biosystemseng.2017.09.007.
[8] K. E. Ileleji, D. E. Maier, and C. P. Woloshuk, "Evaluation of different temperature management strategies for suppression of Sitophilus zeamais (Motschulsky) in stored maize," *J Stored Prod Res*, vol. 43, no. 4, 2007, doi: 10.1016/j.jspr.2007.01.002.
[9] A. Sharma, "IoT Data Security in Smart Farming," *IEEE Transactions on Agriculture*, 2022.
[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," Jan. 15, 2015, *Elsevier B.V.* doi: 10.1016/j.comnet.2014.11.008.
[11] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications, and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, 2012, doi: 10.1016/j.adhoc.2012.02.016.
[12] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," *Food Control*, vol. 39, 2014, doi: 10.1016/j.foodcont.2013.11.007.
[13] C. Muyunda, J. Phiri, C. L. Muyunda, and P. G. Student, "A Wireless Sensor Network Based Grain Inventory Management System for Zambia's Food Reserve Agency," *Article in International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3297, 2007, doi: 10.15680/IJIRSET.2016.0503144.
[14] R. T. Watson and J. Webster, "Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0," *J Decis Syst*, vol. 29, no. 3, 2020, doi: 10.1080/12460125.2020.1798591.
[15] B. B. Kawulich, "Participant observation as a data collection method," *Forum Qualitative Sozialforschung*, vol. 6, no. 2, 2005.
[16] Kvale, "An Introduction to Qualitative Research Interviewing," *Qualitative Research*, 1996.
[17] J. Becker, M. Rosemann, and C. von Uthmann, "Guidelines of Business Process Modeling," 2000. doi: 10.1007/3-540-45594-9_3.
[18] S. Ali and et al., "PCB Design for IoT Sensor Nodes in Agricultural Monitoring," *Sensors Journal*, 2023.
[19] S. Patel and A. Singh, "Optimizing IoT Communication Using Data Aggregation Techniques," *Smart Systems and Applications Journal*, vol. 15, no. 2, pp. 34–48, 2021.
[20] X. Wu and et al., "Energy-Efficient Data Collection Strategies in IoT Networks," *Wireless Communication Journal*, vol. 8, no. 1, pp. 78–92, 2020.
[21] R. Kumar and et al., "Efficient Data Transmission in IoT-Based Sensor Networks," *IEEE Transactions on IoT Systems*, vol. 14, no. 2, pp. 89–102, 2022.
[22] M. Ahmed and et al., "Challenges of Data Overload in IoT Systems," *Journal of Sensor Networks*, vol. 12, no. 3, pp. 67–82, 2019.