INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

Securing Smart Farms: An Integrated IoT-Based Security System with Arduino and SIM Module

Ome U.K[1], Eke J[2], Elufidodo G[3]

[1]*Dept. of Computer Science, University of Nigeria, Nsukka, Nigeria.*

[2]*Department of Electronics and Electrical Engineering, Faculty of Engineering (ESUT), Nigeria*

[3]*Dept. of Computer Science, University of Nigeria, Nsukka, Nigeria*

DOI: https://doi.org/10.51583/IJLTEMAS.2024.130304

Received: 18 December 2023; Revised: 28 December 2023; Accepted: 01 January 2024; Published: 30 March 2024

Abstract: The rise of smart farming, driven by technologies like the Internet of Things (IoT), has opened up new possibilities in agriculture. However, it has also brought about significant security challenges. This study aims to address the need for a comprehensive security system designed specifically for smart farms. The authors developed this system using camera technology, Arduino microcontrollers, vibration sensors, and the SIM900A SIM module. It enhances intrusion detection, provides precise location tracking, and enables real-time incident reporting through Multimedia Messaging Service (MMS) alerts and Short Message Service (SMS). By capturing visual data and leveraging vibration sensors, it offers an effective means of identifying security threats. Importantly, the SIM900A module ensures swift communication, even in remote agricultural areas. This research helps fill the gap in smart farm security, offering a practical and scalable solution to protect assets and data in the evolving landscape of digital agriculture.

I. Introduction

Smart farming, propelled by the integration of modern technologies such as the Internet of Things (IoT), data analytics, and automation, has redefined agriculture. This digital revolution has unlocked unprecedented potential for increased productivity and operational efficiency. However, it has simultaneously exposed the agricultural sector to a critical concern: the need for robust security measures. As smart farms become more interconnected and data-driven, safeguarding both physical assets and sensitive data has become paramount for ensuring the sustainability and profitability of modern farming operations.

The significance of security in smart farming cannot be overstated. While technology has bestowed numerous benefits upon agriculture, including optimized resource utilization and improved crop yields, it has also ushered in a host of security challenges. These challenges encompass vast areas, making comprehensive surveillance and intrusion detection a complex endeavor. Furthermore, many farms are located in remote or rural areas, where immediate physical intervention during security breaches may be unfeasible. Data privacy and compliance with stringent regulations add a layer of complexity, especially concerning the capture and storage of visual data, such as images and videos. Additionally, minimizing false alarms, often triggered by environmental factors like wind and wildlife, is crucial to maintaining operational efficiency.

II. Problem Statement

Smart farming, driven by IoT and automation, holds immense promise for agricultural efficiency and productivity. However, the increasing integration of technology in agriculture also exposes farms to a range of security challenges. These challenges include ensuring comprehensive surveillance across vast areas, addressing security breaches in remote farm locations, managing data privacy and compliance, and minimizing false alarms triggered by environmental factors. Current security measures, while effective to some extent, fall short of addressing these challenges comprehensively.

In light of these challenges, there is a pressing need to develop and implement advanced security solutions that not only enhance intrusion detection but also facilitate remote monitoring, provide visual evidence for incidents, and minimize false alarms. This study aims to address this need by exploring the integration of computer vision and vibration sensors as a comprehensive security solution for smart farms. The goal is to enhance the precision of intrusion detection, improve the efficiency of security operations, and empower farmers to protect their assets and data in an ever-evolving digital agricultural landscape. Through this research, we seek to contribute to the development of practical, effective, and scalable security solutions that can ensure the security and sustainability of smart farming practices.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

Objectives of the study:

i. Precise Sensor Characterization:

Ensure accurate sensor readings through thorough calibration and sensitivity adjustments, optimizing performance for robust smart farm security.

ii. Device Integration with the Controller:

Facilitate seamless communication between smart devices and the central controller, ensuring compatibility and efficiency in data exchange for a responsive security infrastructure.

iii. Build an Animal Repellent System for Real-time Monitoring:

Introduce an animal-repellent mechanism integrated with real-time monitoring, utilizing sensor data to detect and deter animals. Incorporate an alarm system specifically for unauthorized animal access, triggering immediate repellent measures when the threshold value is exceeded.

iv. Real-time Environmental Monitoring:

Implement dynamic real-time monitoring with strategically placed sensors and proactive alarm thresholds, responding in real-time to environmental anomalies for effective security measures.

v. Build Security of Transmitted Data Using AES and Transmit to the Cloud:

Strengthen overall security by applying AES encryption to sensor data before transmission. Introduce an alarm system for potential security breaches during data transmission, adding an extra layer of protection.

vi. Timely Feedback Mechanism to Farmers:

Implement a responsive feedback mechanism for farmers, delivering timely alerts through multimedia messages and short media messages. Optimize data usage for efficient communication, empowering swift responses to security events in the smart farm.

III. Literature review:

The literature review provides a logical exploration of smart farming technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), and their impact on agriculture. Various studies contribute to a comprehensive understanding of this emerging field. Gupta et al.'s (2020) research emphasizes the urgency of addressing cybersecurity concerns in agriculture, while Shabadi and Biradar's (2018) study on IoT-based smart security in Indian farming acknowledges the potential of IoT for soil monitoring but notes limitations. Evan et al.'s (2021) review categorizes security threats in Smart Farming (SF) and Precision Agriculture (PA), offering mitigation strategies. Mohamed et al.'s (2021) paper explores the broader role of technology in agriculture, integrating AI, IoT, and mobile internet. Ahmad Latif et al. (2020) provide a comprehensive overview of smart farming, emphasizing ICT integration but suggesting a deeper exploration of challenges faced by autonomous vehicles and drones.

Amiri-Zarandi et al.'s (2022) paper focuses on IoT and AI integration in smart farming, proposing a platform approach for efficient data integration. Foster, Szilagyi, Wairegi, et al.'s (2023) article critically examines the impact of precision agriculture, smart farming tech, and AI in East Africa, advocating for inclusive and decolonial tech management approaches.

A crucial component in this technological integration is the widespread use of sensors, as demonstrated by studies from Suresh et al. (2020) and Valerio et al. (2020). These wireless soil moisture sensors optimize irrigation, conserve water, and enhance crop yield. Real-time data empowers farmers to make informed decisions on irrigation, fertilization, and planting, as highlighted by Gholamifard et al. (2021). IoT's positive impact on water management is further underscored by studies like Kamble et al. (2020), which demonstrate efficient resource utilization.

Beyond soil parameters, environmental monitoring through IoT includes sensors measuring temperature, humidity, wind speed, and air quality. This data forms the basis for predictive models anticipating fire risks, as explored by Santos et al. (2021). Proactive measures in response to early warnings are discussed by Al-Otaibi et al. (2020). IoT extends to disease and pest management, as showcased by Mahato et al. (2020), with sensors offering early detection capabilities. Data-driven insights from IoT assist farmers in optimizing practices, leading to increased yields, as evidenced in studies like Zhang et al. (2020). Collectively, these studies contribute to a holistic understanding of the challenges, opportunities, and socio-cultural implications of integrating technology, particularly IoT and AI, into agriculture.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

Research Gap

The existing research gaps in secure systems for smart farms center on issues such as false alarms, challenges in remote locations, and data security. The current literature lacks adequate focus on mitigating false alarms coming from environmental factors, addressing security issues in remote farm locations, and ensuring privacy and compliance in data handling within the area of smart farming. Bridging these gaps is crucial for developing targeted and effective security solutions tailored to the unique needs of smart agricultural practices

IV. Materials and Methods

Materials:

The materials used for the proposed system and their respective purposes are shown in Table 1. Below

Material	Purpose
Transducer	Converts physical signals into electrical signals for monitoring environmental parameters.
Arduino Uno	Serves as the central controller for device integration and data processing.
GSM/GPS Module	It enables communication through SMS and MMS and provides location data for enhanced security.
Arducam	Captures visual data for surveillance and monitoring purposes.
Solar Power	Provides a sustainable and renewable energy source for continuous system operation.
AES Encryption	Ensures the secure transmission of data for confidentiality and integrity.
Cloud Repository	Facilitates centralized storage, accessibility, and analysis of sensor data.
MMS and SMS	Enable multimedia and text message alerts for communication with farmers.
Soil Moisture and Temperature Sensors	Monitor soil conditions for optimized farming practices.

Tab. 1: Materials used and their respective purposes

i. Methods

The technical approaches and techniques used in this study are as follows:

a. Analysis of Existing Systems:

The analysis of the existing systems shows that existing solutions do not adequately protect physical assets or data from security threats, and they lack features to prevent false alarms. These shortcomings highlight the need for a more robust and secure system.

b. Analysis of Proposed System:

This paper proposes a novel solution that utilizes an Arducam, a vibration sensor, and a SIM900A cellular communication module to capture and send images of intruders, as well as their location, in MMS and SMS formats to the farmer's phone. This solution provides a robust and secure solution that addresses the shortcomings of existing systems.

ii. **System Architecture**:

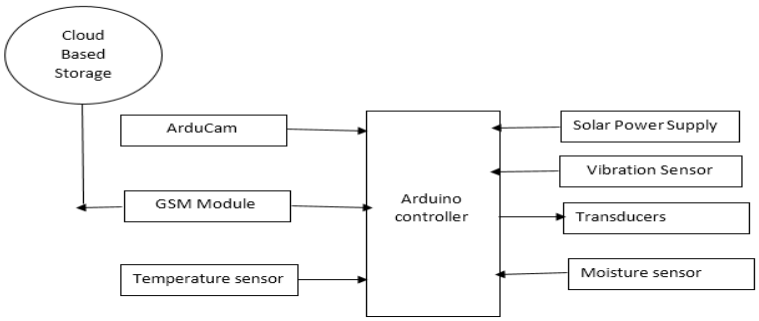

Fig. 9: Block diagram of a proposed system

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

The following outlines the descriptions of the components within the proposed system architecture:

a. **Digital Camera**

A digital camera is incorporated into the system to capture images of any intruders. When force is applied to the system that is greater than the threshold, the camera is triggered and begins capturing images. Once captured, the images are transmitted to the farmer via the SIM900A communication module. These images can be used by law enforcement to investigate and identify intruders.

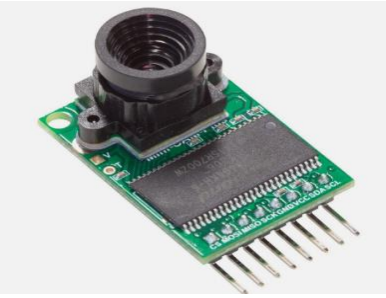

Fig. 1: Arducam Mini Module Camera Shield with OV2640 2 Megapixels

b. **Microcontroller**

The microcontroller is a programmable device that provides the computational capabilities for the system. It acts as the central processing unit, controlling the other components by sending and receiving data. It has a specific set of input and output pins, registers, and memory, all of which work together to perform the microcontroller's functions. It receives image data from the camera and vibration data from the vibration sensor, and it uses this data to determine if there is an intruder. It also communicates with the SIM900A module to send and receive data.

Fig. 2: Genuine Arduino Uno R3

c. **Transducer:**

The sound transducer is specifically designed to serve as an effective deterrent for deterring animals from targeted areas. By emitting ultrasonic waves, it creates an uncomfortable auditory environment for certain animals without causing harm, addressing the need for a humane and non-lethal method of animal repellent.

Fig. 3: Dayton Audio TT25-8 Puck Tactile Transducer Mini Bass Shaker, 8 Ohm

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

d. **Vibration Sensor**

The vibration sensor is a transducer that converts mechanical vibrations into an electrical signal using the piezoelectric effect. When the sensor is subjected to vibration, a voltage proportional to the acceleration of the vibration is generated. This voltage is then sent to the microcontroller, which uses it to detect if the vibration level exceeds the specified threshold. The microcontroller can then trigger the appropriate response, such as sending an alert or taking other action.

Fig. 4: Arduino Piezo vibration sensor

e. **Sim 900A Module**

The SIM900A is a GSM/GPRS module that allows the system to send and receive data via cellular networks. It supports a range of features, including SMS and MMS messaging, as well as GPS tracking and location services. The SIM900A is connected to the microcontroller, which can send and receive data using AT commands. The module uses GPRS to send and receive data and can also be used for voice calls and other functions.

Fig5. Sim 900 a Shield

f. **Solar Power:**

In our design, solar power serves as the sustainable energy source for the entire smart farm security system. Solar panels capture sunlight and convert it into electrical power, providing an eco-friendly and continuous energy supply. This design choice enables the system to operate autonomously in remote farm locations without relying on traditional power infrastructure.

Fig6. 5W Solar Panel Charge a 12V Battery

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

g. **Soil Temperature Sensor:**

In the design of the smart farming system, a soil temperature sensor is strategically integrated to capture real-time temperature data at various soil depths. This sensor, often employing thermistor technology, provides accurate measurements, enabling the system to monitor the thermal dynamics of the soil. The gathered information is crucial for understanding the environmental conditions affecting plant growth. It aids in optimizing planting times, managing nutrient applications, and implementing effective crop management strategies.

Fig7. Soil Temperature Sensor

h. **Soil moisture Sensor**:

Complementing the soil temperature sensor, a soil moisture sensor is incorporated into the system's design. These sensors, utilizing capacitance or resistive technology, measure the volumetric water content in the soil. Integrated at key locations, they offer insights into soil hydration levels. This data is instrumental in precision irrigation management, preventing both over-irrigation and under-irrigation. The soil moisture sensor enhances the system's ability to optimize water resources, contributing to sustainable and efficient agricultural practices.

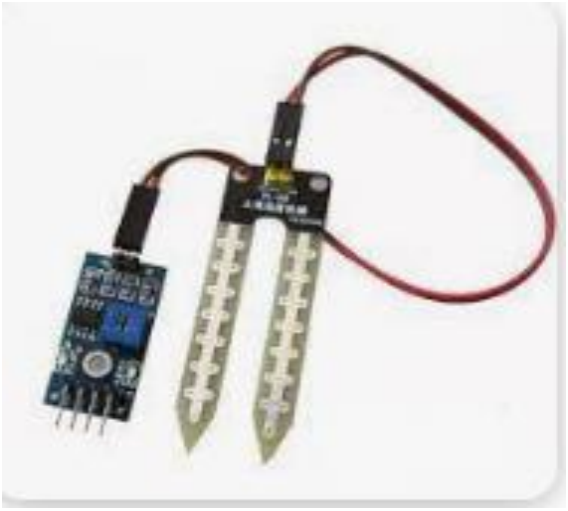

Fig 8. Soil Moisture Sensor

The system proposed in this research is based on several key technologies, including a GSM shield, an Ardu Cam camera, a vibration sensor, a transducer, a soil temperature sensor, a soil moisture sensor, and a microcontroller. The microcontroller serves as the central processing unit, interfacing with the other components to perform the system's functions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

Implementation:

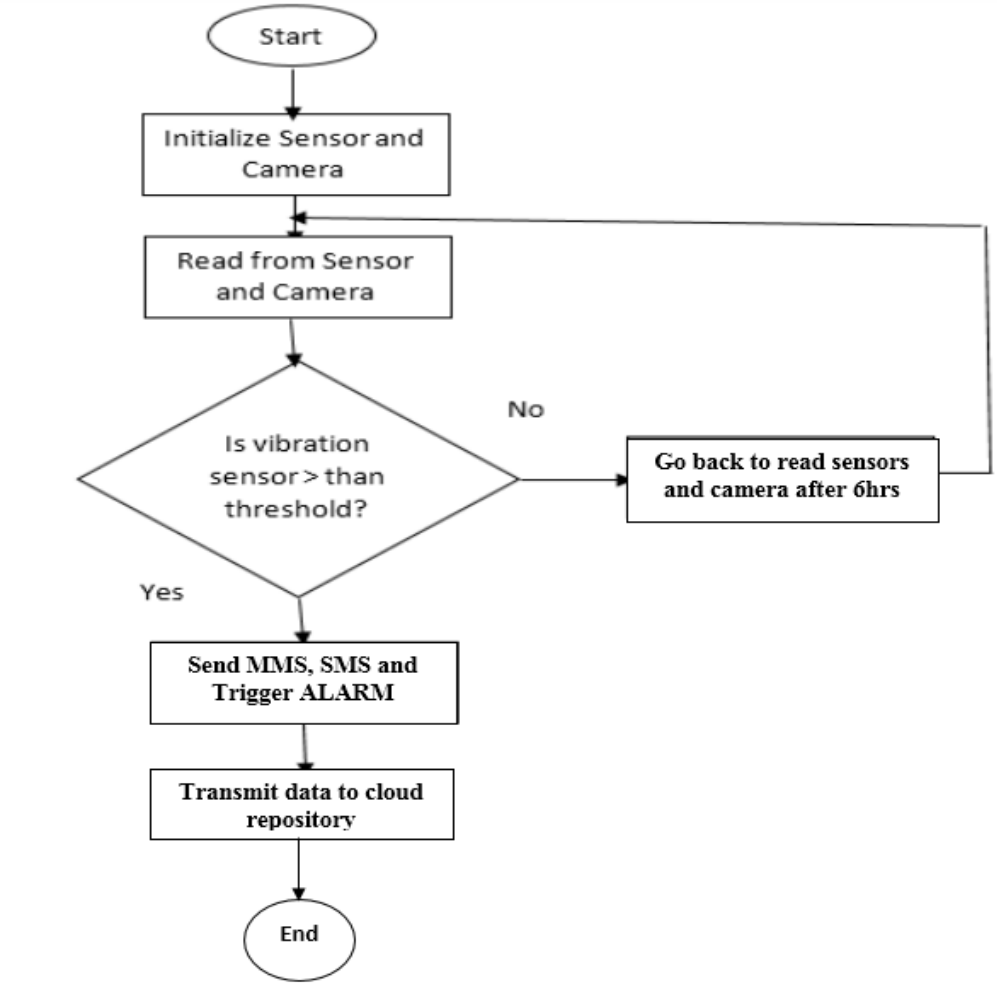

Fig9. The flow diagram of the proposed system.

The smart farm security system's development shown in fig9: above was implemented using C++ programming and the user-friendly Arduino IDE. This combination enabled seamless integration of components, ensuring efficient communication and data processing within the Arduino Uno microcontroller, the system's central brain.

The operation commenced with careful initialization of environmental monitoring sensors, initiating continuous data collection. To safeguard sensitive information, the system encrypted all collected data using AES during transmission. A critical feature involved the vibration sensor, set at a 6g force threshold. If this threshold was exceeded, signaling a potential security threat, the system sprang into action.

It swiftly dispatched multimedia (MMS) and text (SMS) alerts to the farmer, pinpointing the precise location of the disturbance. Simultaneously, an alarm triggered the animal-repellent system, enhancing security measures. The system also seamlessly transmits complete data, along with detailed alerts, to the cloud for centralized storage and comprehensive analysis.

Even in non-critical scenarios where the vibration sensor remained below the threshold, the system securely transmitted data to the cloud for future scrutiny and decision-making. Following a 6-hour wait period, intentionally pausing monitoring activities, the system re-initiated the environmental monitoring process, ensuring a continuous cycle of surveillance, alert mechanisms, and data transmission to the cloud. The code driving this proposed system is shown in Appendix 1.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

Figure10 Proposed System

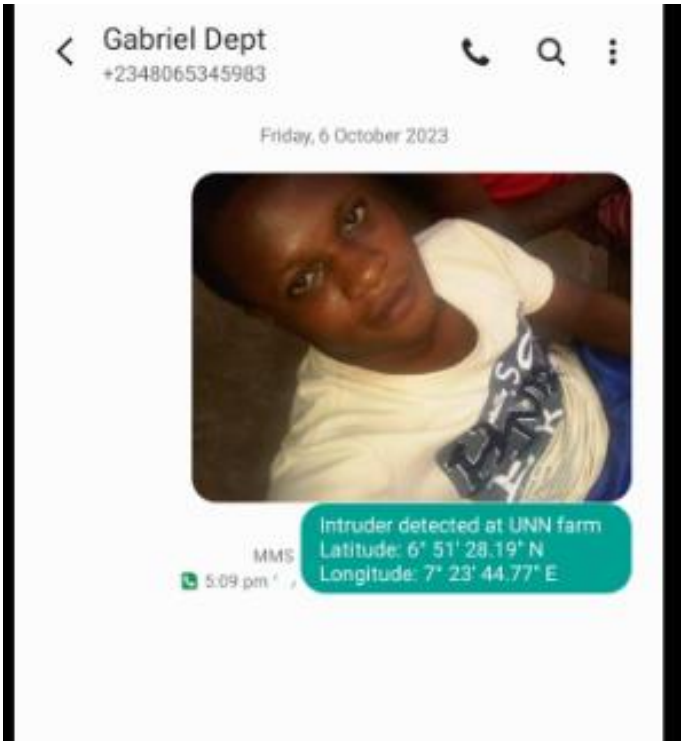

Figure11: Alert sent by the System

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

V. Discussion

In tackling the challenges of system integration, we strategically employed characterizations to streamline diverse protocols seamlessly. Addressing power consumption, solar panels were integrated for energy efficiency and sustainability. Memory constraints on Arduino were overcome through a dual strategy of code optimization and SD card utilization. The issue of false alarms triggered by environmental factors was effectively resolved by setting a discerning vibration threshold at 6g. Priority was placed on enhancing the reliability of GSM/GPS functionality through error-checking mechanisms, strategic retry protocols, and vigilant signal strength checks. This holistic approach reflects a blend of innovative solutions and meticulous problem-solving, highlighting the significance of a thoughtful strategy in overcoming intricate challenges.

VI. Conclusion

In summary, this research unites various technologies to create an advanced security system for smart farms. Cameras capture evidence and monitor for intrusions, vibration sensors increase sensitivity, and the SIM900A module transmits alerts even in remote areas. The integrated system is highly effective in detecting, tracking, and reporting incidents in real-time. This novel solution fills a vital gap in smart farm security, offering a practical and scalable option for protecting modern agricultural environments. Looking forward, future expansion of this smart farm security system will involve integrating machine learning (ML) to enhance intelligence, enabling advanced predictive analysis and proactive security measures in response to evolving challenges in smart farming.

References

1. Al-Otaibi, Y., Jarndal, A., & Alazzam, M. (2020). Internet of Things (IoT) based smart wildfire detection and prevention system. In 2020 5th International Conference on Wireless Mobile Communication and Information System (WMCAIS) (pp. 111-115). IEEE.
2. Amiri-Zarandi, M., Fard, M. H., Youse finaghani, S., Kaviani, M., & Dara, R. (2022, June 1). A Platform Approach to Smart Farm Information Processing. Agriculture (Switzerland). MDPI. https://doi.org/10.3390/agriculture12060838.
3. Foster, L., Szilagyi, K., Wairegi, A., Oguamanam, C., & de Beer, J. (2023). Smart farming and artificial intelligence in East Africa: Addressing indigeneity, plants, and gender. Smart Agricultural Technology, 3. https://doi.org/10.1016/j.atech.2022.100132.
4. Gholamifard, A., Aminzadeh, F., & Moghaddam, K. (2021). Precision agriculture technology based on IoT and cloud computing using a multi-layer perceptron neural network. Journal of the Saudi Society of Agricultural Sciences, 40(3), 359-368.
5. Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. IEEE Access, 8, 34564-34584.
6. Kamble, A. S., Gunjal, A. K., Jadhav, M. N., & Patil, D. R. (2020). Development and implementation of IoT based smart irrigation system using low-power wide area network (LPWAN) technology. Computers and Electronics in Agriculture, 176, 105605.
7. Mahato, N., De, D., & Kumar, A. (2020). IoT based crop pest and disease detection system. Wireless Personal Communications, 115(3), 1803-1818.
8. Mohamed, E. S., Belal, A. A., Abd-Elmabod, S. K., El-Shirbeny, M. A., Gad, A., & Zahran, M. B. (2021). Smart farming for improving agricultural management. The Egyptian Journal of Remote Sensing and Space Science, 24(3), 971-981.
9. Santos, D., Monteiro, J., Santos, M., & Frizzi, L. (2021). An integrative smart system for wildfire risk prediction and firebreak management in rural areas. Sensors, 2.
10. Shabadi, L. S., & Biradar, H. B. (2018). Design and implementation of IOT-based smart security and monitoring for connected smart farming. International Journal of Computer Applications, 975(8887).
11. Virk, A. L., Noor, M. A., Fiaz, S., Hussain, S., Hussain, H. A., Rehman, M., & Ma, W. (2020). Smart farming: An overview. Smart village technology: Concepts and developments, 191-201.
12. Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., & Duncan, E. (2021). A review on the security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. Applied Sciences, 11(16), 7518.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

Appendix 1

```
#include <Arduino. h>
#include <AESLib. h>
#include <GSM GPS Library h>
#include <SD. h>
#include <Wire. h>
#include <ESP8266WiFi.h>
#include <Thing Speak. h>
const char *ssid = "<YOUR_WIFI_SSID>";
const char *password = "<YOUR_WIFI_PASSWORD>";
const char *thing Speak Api Key = "<YOUR_THINGSPEAK_API_KEY>";
const int vibration Pin = A0;
const int arducam Pin = 10;
const int soil Moisture Pin = A1;
const int soil Temperature Pin = A2;
const int animal Repellent Pin = 7;
byte aes Key [] = {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F};
GSM gsm Access;
GSM SMS sms;
GSM GPRS gprs;
GSM GPS gps;
void setup () {pin Mode (vibration Pin, INPUT); pin Mode (a rdu cam Pin, OUTPUT); pin Mode (animal Repellent Pin,
        OUTPUT);
  Serial. begin(9600);
 // Connect to Wi-Fi
  Wi Fi. begin(ssid, password);
  while (Wi Fi. status () != WL_CONNECTED) {delay (1000);
    Serial. Print ln ("Connecting to WiFi..."); }
  Serial. Print ln ("Connected to Wi Fi"); Thing Speak. begin(client); // Initialize Thing Speak if (!SD. begin(4)) {Serial. Print
        ln("SD card initialization failed!");return; }
  // Initialize GSM module
  while (gsm Access. begin() != GSM_READY) {Serial. Print ln ("GSM initialization failed!"); delay (1000);}
  // Enable GPS gps. begin();}
void loop () {int vibration Reading = analog Read (vibration Pin);
  int soil Moisture Reading = read Soil Moisture ();
  int soil Temperature Reading = read Soil Temperature ();
```

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue III, March 2024

```
if (vibration Reading > 6) {capture Visual Data (); encrypt And Transmit Data (soil Moisture Reading, soil Temperature Reading);
  send Alerts (); trigger Animal Repellent (); send To Thing Speak (soil Moisture Reading, soil Temperature Reading);
  // Get GPS location
  String location = get GPS Location ();
  // Send MMS and SMS with location
  Send MMS("image.jpg");
  Send SMS ("Security breach detected!: " + location); } else {encrypt And Transmit Data (soil Moisture Reading, soil Temperature Reading);
  send To Thing Speak (soil Moisture Reading, soil Temperature Reading);}
 delay (6 * 60 * 60 * 1000); // Wait for 6 hours}
// ... (Existing functions remain unchanged)
String get GPS Location () {String location = ""; while (gps. Get GPS () == 0) {Serial. Print ln ("GPS data not available");
  Delay (1000);}
 location += "Lat: " + String (gps.latitude, 6) + ", Lon: " + String(gps. longitude, 6);
 return location;}
void send SMS (String message) {
 Serial. Print ln("Security breach detected!: " + message);
 sms. begin SMS ("<+2348065345983>");
 sms. Print (message);
 sms. End SMS ();}
```