Development of Channel Encryption Model based on AES-128 and Cipher Block Chaining Encryption Mode for Local Smart Yam Farm

Lateef Caleb Umoru[1,2], Joseph Adebayo Ojeniyi*[3], John Kolo Alhassan[4], Solomon A. Adepoju[5], Bello L. Yunusa[6], Abdulkadir Onivehu Isah[7]

[1,3,4,5,6&7]Federal University of Technology, Minna, Nigeria
[2]Confluence University of Science and Technology, Osara, Nigeria

* Corresponding Author: Joseph Adebayo Ojeniyi

Author Contributions
L.C.U.: Conceptualization, methodology, investigation, writing—original draft.
J.A.O.: Data curation, formal analysis, writing—review and editing.
J.K.A.: Validation, visualization, writing—review and editing, Supervision.
S.A.A.: Supervision, project administration, writing—review and editing.
B.L.Y.: Supervision, writing—review and editing.
A.O.I.: Supervision.

Funding Source
This research received no external funding.

Acknowledgement
The authors sincerely acknowledge the contributions of colleagues, technical staff, and institutional support of TETFund Nigeria that facilitated the successful completion of this research.

Abstract
Smart farming systems increasingly depend on Internet of Things (IoT) technologies to monitor field conditions and support timely decision-making. However, when communication channels are not properly secured, sensitive agricultural data can be intercepted, altered, or exposed, undermining both privacy and system reliability. In this study, a secure channel encryption model is designed, implemented, and experimentally evaluated for an IoT-enabled smart yam farming environment. A real-world smart farm testbed was deployed at the Federal University of Technology, Minna, Nigeria, where microcontroller-based sensor nodes were used to collect soil and environmental data and transmit them to cloud infrastructure. The proposed security framework applies AES-128 encryption with Cipher Block Chaining (CBC) mode and incorporates initialization vectors, salting, padding, and message authentication to safeguard device-to-cloud communication. Performance evaluation compared CBC and ECB cipher modes using different key generation mechanisms. The results show that AES-128/CBC increased the data size from 110 bytes to 176 bytes (approximately 60% overhead), while producing more randomized ciphertext and eliminating the pattern leakage observed with ECB mode. Although CBC required about twice the encryption time of ECB (average encryption time of 3.2×10^8 ns), decryption remained efficient, with times below 1.3×10^8 ns. Overall, the findings confirm that the proposed approach enhances data confidentiality and integrity with a level of computational overhead that is acceptable for periodic smart farming data transmission. The key contribution of this work is the delivery of a practical, deployable, and security-focused channel encryption solution validated using live farm data rather than simulations, demonstrating that strong cryptographic protection can be realistically achieved in resource-constrained agricultural IoT environments.

Keywords: Channel, data exchange, cryptosystem, integrity, internet of things, smart farm.

Introduction

Agriculture is considered as a key industry since human's creation because of its capability to offer essentials such as fibre, food, energy, and medicine [1]. It stands as the backbone of human civilization and the sustenance of economy of societies worldwide [2]. Both developing and developed economies continue to emphasize on ways to increase the effectiveness, productivity and produce. Farm mechanization is gradually complemented by information and communication technologies further automate, monitor, control and manage conditions of atmosphere, soils, and farms more effectively [3,4].
Smart farms, as a component of high-tech agriculture, accumulate enormous amount of data from IoT devices concerning various conditions of plants, animals, and the environment to enhance the production processes of complex farming systems [5] [6]. IoT's real-time data transfer imposes new cybersecurity burdens [7] [8].
Cyberattacks target smart systems, like smart farming, could cause significant disruptions, data breaches, and even physical damage to critical agricultural infrastructure. Therefore, protecting the security and integrity of smart farming systems has become a crucial priority for both researchers and practitioners [9]. IoT vulnerabilities arise from inadequate security measures, such as inadequate authentication protocols, unencrypted communication, insufficient access controls and delayed firmware updates. Adversaries exploit vulnerabilities to access devices without authorization, interrupt services, and/or exfiltrate critical data [10].
The process of designing and developing smart farms are usually met with security breaches and risks from its data collection, data storage, data broadcast, and data manipulations. Low network connectivity issue has aggravated the security of smart farming and its components in terms of logical as well as physical disruptions. To this end, there is the need to have reliable security framework in place to safeguards farms, farmers and their valuable assets (data) to reel from the benefits of technological and devices driven agriculture [11].
Data attacks, and equipment/network attacks in IoT are around communication layer for smart farms [12]. Several new cybersecurity vulnerabilities reported since the deployment of thousands of IoT devices in open fields. Attackers break into the smart farming system and network through a variety of techniques for the purpose of interfering with the normal operations of IoT-based setups or equipment [1]. Though, the basic safeguards for IoT rely on monitoring data flow and encryption of critical data [11]. There is the need to have effective information security by means of access controls, authentication, and integrity procedures, which safeguards smart farming cyber-physical systems from being altered, tampered with, damaged or accessed by third-party [6], and reduce personal data privacy leaks [13].
The specific objectives of the paper include:

i. setup smart farm testbed for generating farm data.
ii. formulate channel encryption model-based AES-128 and CBC encryption mode.
iii. evaluate the performance of the cryptosystem time complexity, computational cost, communication overhead, efficiency, and privacy.

Theoretical Considerations

Smart farms rely on dense IoT sensor networks, UAVs, and cloud platforms, making wireless channels a prime target for eavesdropping, tampering, and device impersonation. Majority of research focus on balancing confidentiality and integrity with low energy, memory, and bandwidth use in constrained devices.
Lightweight Symmetric Encryption on IoT Links: AES (often with MQTT) secures sensor–broker links with modest overhead; combining Huffman compression + AES optimizes bandwidth and security in agricultural IoT [14]. The Expeditious Cipher (X-cipher) creates encrypted MQTT channels in smart irrigation, outperforming AES and PRESENT in power, time, and memory on constrained nodes [15]. New lightweight designs such as Ascon AEAD for Raspberry-Pi–based farms [16] and the dedicated LightAgriCrypt stream cipher show higher throughput and strong randomness with low power and memory [17]. Simple Base64 encryption has been used but only obfuscates data and is not cryptographically secure [18].
Public-Key, Authentication, and Key Exchange: Elliptic-curve-based protocols provide mutual authentication and session keys for sensors, UAVs, gateways, and servers, with formal proofs (BAN logic, ROR) and resistance to replay, MITM, and impersonation. [19] [20] [21]. Homomorphic signcryption over hyper-elliptic curves offers confidentiality, integrity, and privacy with sharply reduced computation and communication vs. earlier RSA/ECC schemes [22]. Some frameworks integrate

public-key encryption into NB-IoT + blockchain or energy-aware aggregation protocols to secure long-range field links [23] [24].

Blockchain and Secure Transport Layers: Private / permissioned blockchains secure drone–sensor links and UAV networks with ECC keys and SHA-256, providing tamper-evident logs and integrity for wireless channels [25] [26] [27] Wu & Tsai, 2019). For rural farms, TLS/SSL is recommended as the base secure transport between IoT and cloud, with emphasis on efficient encryption in low-infrastructure settings [28]. Smart farm channel encryption is moving from basic AES or ad-hoc schemes toward lightweight AEAD ciphers, ECC/HECC-based authentication, and blockchain-backed key and integrity management. The main design goal is strong protection against eavesdropping and tampering while keeping energy, memory, and latency low for field devices.

Related Work

Ref.[29] proposed a distributed ledger technology known as PrivySec framework to preserve the privacy of personal and non-personal information during exchanges on smart farms. The semi-homomorphic encryption and Corda framework offers higher privacy assurances, throughput, and commit time than Hyperledger Fabric, and Ethereum. The authors setup a testbed for validating the concepts, but more approaches could be introduced to increase analytics and stop PII leaks especially encryption techniques. The proposed scheme is distinct from existing strategies in many aspects. The data privacy is preserved by dividing the blockchain network into various channels, where every channel comprises a finite number of authorized organizations and processes a specific type of data such as health, smart car, smart energy or financial details. Moreover, access to users' data within a channel is controlled by embedding access control rules in smart contracts. Also, data within a channel is further isolated and secured by using private data collection and encryption respectively. Likewise, the REST API that enables clients to interact with the blockchain network has dual security in the form of an API Key and OAuth 2.0. There was no practical implementation of the protocol scheme.

Ref.[22] addresses security vulnerabilities and performance deficiencies in smart agriculture frameworks caused by an overreliance on resource-intensive cryptographic methods like RSA and bilinear pairing. The authors proposed a novel privacy-preserving homomorphic signcryption scheme based on Hyper-Elliptic Curves (HEC), which balances robust security with reduced processing complexity for resource-constrained IoT devices. The methodology was validated using the Scyther tool for formal security verification and subjected to a comparative performance analysis against existing literature. Empirical results show a 95.08% reduction in computational costs and an 89.28% reduction in communication overhead, while successfully resisting known attacks such as replay, modification, and impersonation. A primary weakness of the scheme is the potential for key escrow issues due to the centralized role of the Trusted Third Party (TTP), alongside scalability concerns in very large-scale deployments.

Ref.[21] aimed to protect user privacy and mitigate security risks such as impersonation and data alteration in smart agriculture Wireless Sensor Networks (WSNs). The researchers developed a three-factor key agreement framework utilizing Elliptic Curve Cryptography (ECC), hash functions, biometrics, and fuzzy extractors to ensure secure communication. The protocol's accuracy was demonstrated through BAN logic, while its security was simulated using the Scyther tool and compared to similar protocols regarding computation and communication overheads. The results indicate a low computation cost of 6.7217ms and a communication cost of 1152 bits, outperforming existing frameworks in terms of efficiency. However, the study notes weaknesses such as limited coverage area of WSNs, reliability issues due to technical interference, and the potential high cost of implementation for small-scale farmers.

Ref.[27] wanted to safeguard sensitive environmental farming indices and protect against Distributed Denial-of-Service (DDoS) attacks by applying dark web technology to hide blockchain and server locations. The methodology employs an identity authentication mechanism using ID-based cryptography (IBC), symmetric encryption for data privacy, and the establishment of private blockchains. Experimentation involved testing with IoT development boards and servers to realize bilinear pairings and private blockchain environments. Results showed that the system improved authentication speeds through lightweight encryption and effectively concealed server IP addresses to lower DDoS risks. A notable weakness is the requirement for a mediator (the dark net mechanism), which could potentially introduce a single point of failure if the Trusted Authority (TA) is compromised.

[24] addressed the challenge of incorporating high security while maximizing energy retention in resource-constrained on-field sensors. The authors proposed a synchronized framework utilizing a unique public-key encryption method that does not store private keys and a noniterative algorithm for secure data aggregation with parallel validation. The logic was implemented in MATLAB, simulating 1000 sensors and comparing the results to existing schemes like secure LEACH. Empirical results demonstrate that the scheme offers 35% more alive nodes, 32% higher retention of residual energy, and 52% faster execution than existing standards. A potential weakness is the reliance on preapproved information about adversaries, and the authors noted the need for more complex adversarial models in future work to account for multiple dynamic attackers.

Ref.[26] attempted to establish trust and secure communication between sensors and drones in a farm field while enhancing agricultural production through automation. The methodology utilizes a secure blockchain-based framework employing ECC asymmetric key exchange, SHA-256 hash functions, and off-chain IPFS storage to manage data efficiently. Experimentation was conducted via a proof-of-concept on the Ethereum blockchain using smart contracts, with performance analyzed through Hyperledger Caliper. The results indicate an average Read throughput of 32.54 TPS and a Write throughput of 19.37 TPS, confirming the system's ability to maintain data integrity. One weakness is the performance and scalability limitations of the Ethereum blockchain, along with potential difficulties in verifying user identity due to the openness of blockchain technology.

Ref.[20] aimed to provide a truly efficient but robust security solution for resource-limited precision agriculture devices to protect against threats like DoS and man-in-the-middle attacks. The researchers deployed a scheme using efficient cryptographic primitives such as hashing, exclusive OR (XOR), and random number generators, verified through BAN logic. Experimentation was performed on a standard laptop to benchmark computation overheads and energy consumption against ten other related protocols. The empirical results revealed the proposed protocol to be highly efficient, consuming the lowest computation overhead (2.94ms) and energy (0.019mJ) while supporting all 19 identified security features. A weakness of this approach is that it incurs relatively higher communication costs (1664 bits) compared to some specific high-latency schemes in its comparison set.

Ref.[18] attempted to secure communication in oyster mushroom cultivation to prevent hacking or rival interference. The methodology involves the application of Base64-based data encryption and decryption on NodeMCU ESP8266 sensor nodes and Raspberry Pi sink nodes. Experimentation was conducted by simulating attacks with the Wireshark tool to scan network traffic and determine if sensor readings remained unreadable. Results showed that once the encryption was implemented, data scans yielded only unreadable strings, effectively securing information during the transfer process. The main weakness is that Base64 is an encoding method rather than a complex cryptographic algorithm; the authors acknowledge that future research is needed to implement more robust digital signatures for full data integrity.

Ref.[25] dealt with the vulnerabilities of centralized Agri-IoT solutions by introducing a multi-tiered blockchain technology (BCT) personalized for agricultural data security. The model utilizes a Quantum Neural Network combined with Bayesian Optimization (QNN + BO) and an ECC-Chaotic Map (EC^3) algorithm for secure data flow across Edge, Fog, and Cloud levels. Experimentation used the ToN_IoT dataset on a high-performance computing setup to evaluate accuracy and cryptographic time. Empirical results showed significant performance gains, including a 46.7% and 54.6% reduction in encryption and decryption times, respectively, and 16.8–33% lower memory usage than baseline models like CNN and LSTM. A weakness of the work is that it assumes homogeneous edge device participation, which may not reflect real-world scenarios where edge nodes vary significantly in computational power.

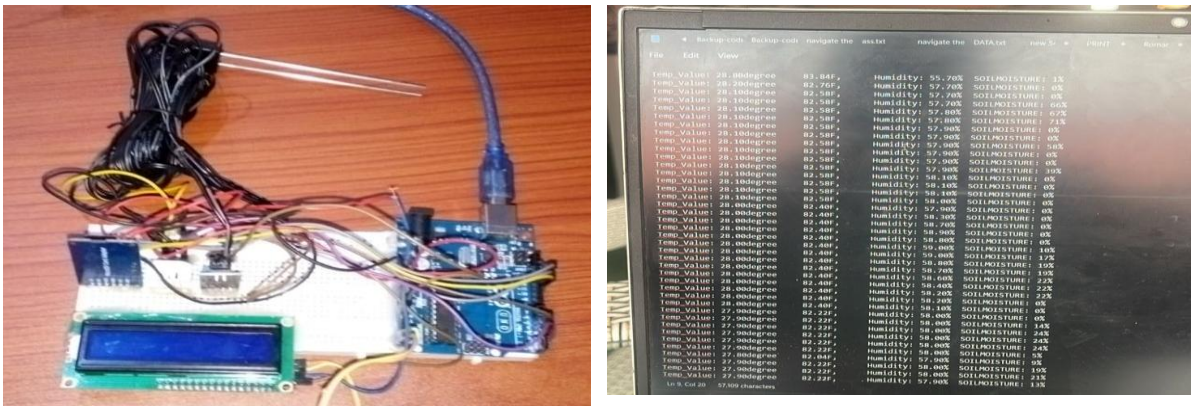
[15] aimed to secure smart irrigation systems by protecting sensor data and decision-making information from eavesdropping and alteration. The researchers investigated the adoption of the Expeditious Cipher (X-cipher), a high-throughput lightweight encryption protocol, to create secure channels within the MQTT protocol. The model was evaluated through simulations using a Raspberry Pi emulator and compared against AES and the PRESENT cipher in terms of power, time, and memory. Empirical results revealed that X-cipher required less power and memory than AES and outperformed the PRESENT cipher in throughput (164 KBps vs 140 KBps) and memory efficiency. A primary weakness is the trade-off between security and resources, as X-cipher achieves an "adequate" level of security compared to the higher security standard provided by AES.

Ref.[14] optimized data transmission in agricultural IoT to minimize traffic while ensuring data security, particularly for devices in areas with unstable connectivity. The methodology focuses on combining compression algorithms (Huffman coding) and encryption (AES) within the MQTT protocol. Experimentation used real messages from agrometeorological stations, evaluating the amount of data generated at different MQTT Quality of Service (QoS) levels. Results indicated that Huffman coding was the most effective, achieving a 32.9% reduction in data size, and the combined approach reduced annual data traffic by several megabytes while maintaining confidentiality. A weakness noted by the authors is that they prioritized widely used standards like TLS and AES rather than the "most advanced" or specialized security options.

Materials and Methods

Data Collection

This paper setup a smart yam farm for the collection of farm environmental and soil parameters data across the communication layer. The proposed smart yam farming will leverage on data-driven management based on spatial- and time- data measured from soil, plant and other parameters generated from sensors, and storage attacks data infrastructure deployed. The setup for testbed was in Federal University of Technology, Minna farm site. The sensors data include temperature, moisture, humidity, illumination and movement data of the yam crop on the field site specificity. The complete setup for the smart yam farming conceptual structure is shown in Fig. 1.



(a) The microcontroller setup for the field unit. (b) The user output monitoring unit.

Fig. 1. The setup of the smart farm field unit.

The specifications of the sensors to be deployed for the smart yam farming system: Grove Air quality sensor, Grove light sensor (v 1.2), Grove Capacitive moisture sensor, and Grove Barometer sensor (BME 280). The Microcontroller is Arduino UNO, ESP8266 Wi-Fi. The cloud service is to be provided by Microsoft Azuri. Fig. 1(a) shows the microcontroller setup for collecting farm site parameters using various sensors and display modules. Again, Fig. 1(b) illustrates the console component of the output from the field unit of the smart farming system for the different readings and precise measurements of selected farming parameters as monitored by the user from the computer PC.

Architecture of the Proposed Model

The architecture of the proposed secure cyber intelligent model for preventing threats and preserving smart sensor data using data encryption scheme as shown in Fig. 2.

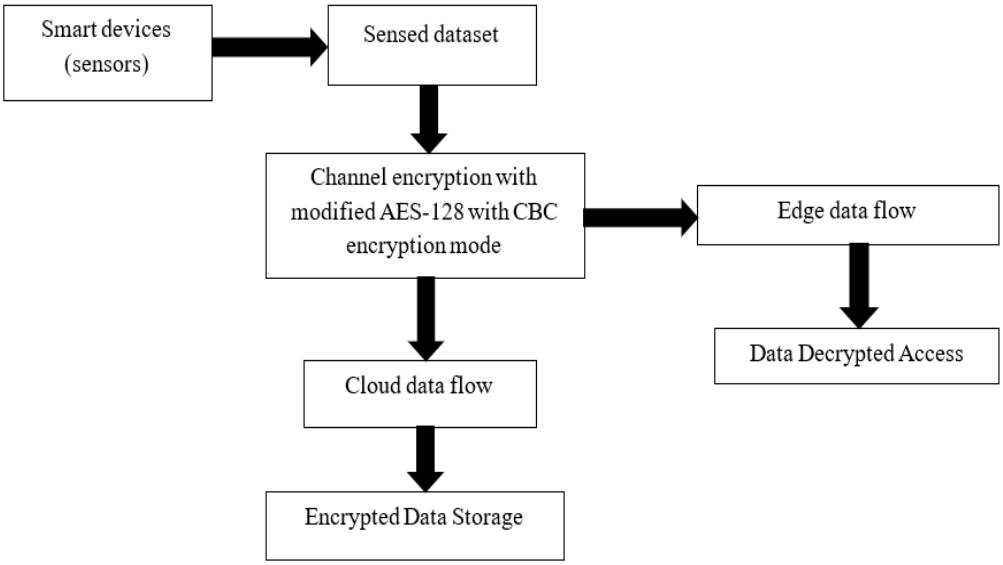


Fig. 2. The architecture of the encryption model for smart farm channels.

From Fig. 2, the main components of the architecture of the proposed model include the smart devices (sensors) and sensed dataset as the input to the proposed model. And the output component provides data encryption using modified AES-128 with Chain Block Cipher encryption mode.

Problem Definition

Definition 1. Sensor data encryption is a component in the proposed model for the protection of sensor data acquired from the smart yam farm field. The encryption algorithm required is the symmetric cryptography for the channel encryption while safeguarding the sensor parameters broadcast from the field to the cloud for further analysis. The AES encryption algorithm is used to safeguard the sensor data as given by Eq. 1:

$$C = E_k(M) \quad \ldots (1)$$

where,
C = the encrypted message or ciphertext.
M = the plaintext sensor data,
k = the secret key (or private key),
E_k = the encryption function.

Definition 2. The cyber-physical model for the smart yam farming security against attack encrypt sensor data using AES-128 encryption algorithm improved with CBC encryption mode prior to transmission from the field to the cloud.

Encryption procedure

Input: plaintext P, master_secret S, associated_data A (optional)
1. K_enc = HKDF(S, salt, info="enc", length=32)
2. K_mac = HKDF(S, salt, info="mac", length=32)
3. IV = SecureRandom(16)
4. P_padded = PKCS5Pad(P, 16)
5. C = AES_CBC_Encrypt(K_enc, IV, P_padded)
6. # compute MAC over version||IV||C||A (Encrypt-then-MAC)
7. T = HMAC_SHA256(K_mac, version || IV || C || A)
8. Output message = concat(version || IV || C || T)

Decryption and Verification Process

Input: message = version||IV||C||T, master_secret S, associated_data A (optional)
1. Parse version, IV, C, T

2. K_enc = HKDF(S, info="enc", length=32)
3. K_mac = HKDF(S, info="mac", length=32)
4. T_expected = HMAC_SHA256(K_mac, version || IV || C || A)
5. If not ConstantTimeCompare(T, T_expected): REJECT (authentication failed)
6. P_padded = AES_CBC_Decrypt(K_enc, IV, C)
7. P = PKCS5Unpad(P_padded) # if padding invalid -> REJECT
8. Return P.

Experimental Setup

Sensors, microcontrollers, and other data capturing devices were deployed on yam farm field to collect and transmit soil and environmental parameters (such as humidity, moisture and temperature) as are contained in Table 1. The Federal University of Technology, Minna, farm site was used for deployment of the developed wireless sensor network.

Table 1. The experimental tools and values.

Parameter	Value
Processor	13th Gen Intel(R) CORE(TM) i7-1355U, Intel iRISx Graphics 1.70 GHz
RAM	16.00 GB
Hard Disk Drive	1 Tera Byte
System Type	64-bit Operating System, x64-based processor
Operating System	Windows 11 Home Single Language
Application programming interface	Visual Studio Code 16
Cryptosystem	AES-128, base64code, Cipher Block Chaining (CBC), Electronic Code Book (ECB)
Key exchange protocol	Diffie and Hellman algorithm
Arduino UNO software	1.8.15
Soil moisture sensor	DHT22
SD Card reader	32GB
LCD	12C Module
Power source	5000Ahr Lipo Battery
Energy conversion	DC-to-DC converter

Performance Evaluation Parameters

The proposed model and algorithm realised from objectives two and three are to be evaluated to ascertain the level of intelligence, security and resilience using the attacks data collected from the smart yam Testbed [6]. The main evaluation metrics include: Encryption time, decryption time, message size, and ciphertext size [30].

Results and Discussion

Farm data capturing mobile app

The real-time data capture from farm field was achieved through the developed Onrender Platform API at: https://soil-mon-api.orender.com. It requires login credentials to be generated for the user's authentication to the secure field sensors data capture for temperature, humidity, and moisture. The interface for the user login and subsequent authentication is shown in Fig. 3.

.

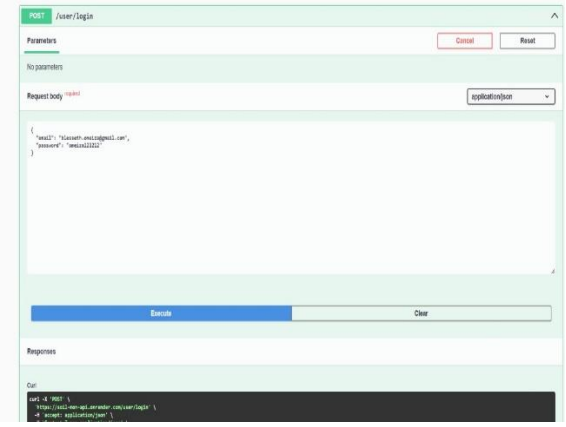
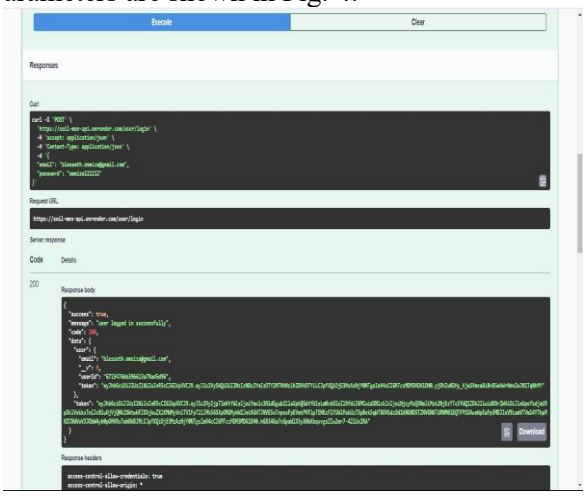
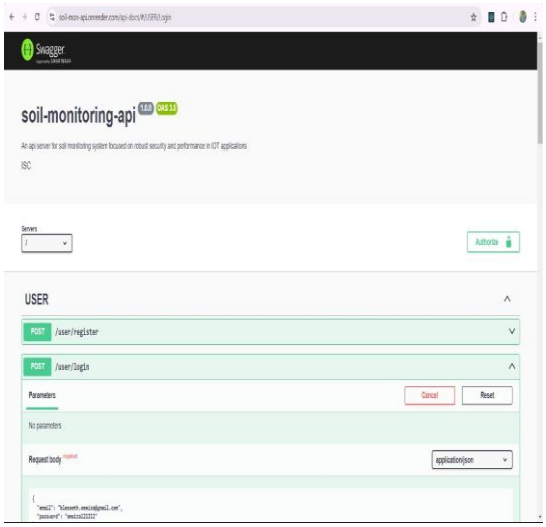


Fig. 3. The user login and authentication interface.

From Fig. 3, the system users are required to register their username (email), and password to gain access to the functionalities and datasets collected from the farm field. The Orender setup for the sensor devices and API token for controlling and monitoring of the farm and communication devices parameters are shown in Fig. 4.



(a) Orender API and sensors monitoring setup interface.



(b) User device configuration interface.

Fig. 4. Orender API and data collection control interface.

From Fig. 4(a), upon successful login of the user's credentials (username and password), the Orender API generates and allocates session Token for manipulation of the system functions and datasets collected and transmitted to the cloud infrastructure. Fig. 4(b) shows the soil-monitoring-api interface in real-time for the POST and GET operations of the user. The user is required to supply correct login credentials to be able to access and download datasets and add and configure sensor devices accordingly.

The sample of the data collected from the Orender API soil-monitoring-api system showing the timestamp, voltage level of the battery, temperature value, humidity value, soil moisture value, and charging indicator are presented in Table 2.

Table 2. Sample of data collection from the smart farm setup.

Time	Battery Voltage	Temperature	Humidity	Soil Moisture	Charging
2025-01-06T09:07:31.000Z	3.738095	32	21	4095	FALSE
2025-01-11T14:19:58.000Z	4.061905	31	29	4095	FALSE
2025-01-11T14:22:29.000Z	4.028572	31	25	4095	FALSE

2025-01-11T14:24:59.000Z	3.990476	32	24	4095	FALSE
2025-01-11T14:27:29.000Z	3.966667	32	23	4095	FALSE
2025-01-11T14:30:00.000Z	4.009524	33	23	4095	FALSE
2025-01-11T14:32:30.000Z	3.961905	33	23	4095	FALSE
2025-01-11T14:35:00.000Z	4.028572	33	23	4095	FALSE
2025-01-11T14:37:30.000Z	4.014286	33	23	4095	FALSE
2025-01-11T14:40:01.000Z	3.966667	33	23	4095	FALSE

Channel encryption for smart farm device-to-cloud communication was carried out using AES with salting, padding and encryption modes as presented in the next subsection.

Channel Data Communication Encryption Approach

This paper experimented secure component of the developed smart yam setup by encrypting the channels for devices data exchanges from the field to the cloud. Two approaches were of interest, the secret key factory generation of PBKDF2WithHmacSHA256 (CK1) and SHA-1+AES (CK2), and the cipher modes of AES/CBC/PKCS5Padding (CEM1), and AES/ECB/PKCS5Padding (CEM2) respectively. Table 3 presents the channel encryption of the smart farm data using AES with the secret key factory generation of PBKDF2WithHmacSHA256 (CK1) and the cipher modes of AES/CBC/PKCS5Padding (CEM1).

Table 3. AES with secret key factor: CK1, cipher mode: CEM1.

Sensor Data	Size (byte)	Ciphertext size (byte)	Encryption time (ns)	Decryption time (ns)
2025-01-06T09:07:31.000Z, 3.738095, 32, 21, 4095, FALSE	110	176	457599500	153796600
2025-01-11T14:19:58.000Z, 4.061905, 31, 29, 4095, FALSE	110	176	237910700	109812300
2025-01-11T14:22:29.000Z, 4.028572, 31, 25, 4095, FALSE	110	176	507455300	104518000
2025-01-11T14:24:59.000Z, 3.990476, 32, 24, 4095, FALSE	110	176	207907900	79347900
2025-01-11T14:27:29.000Z, 3.966667, 32, 23, 4095, FALSE	110	176	596193100	218587200
2025-01-11T14:30:00.000Z, 4.009524, 33, 23, 4095, FALSE	110	176	221641000	78100700
2025-01-11T14:32:30.000Z, 3.961905, 33, 23, 4095, FALSE	110	176	263960200	160886700
2025-01-11T14:35:00.000Z, 4.028572, 33, 23, 4095, FALSE	110	176	231430800	96045900
2025-01-11T14:37:30.000Z, 4.014286, 33, 23, 4095, FALSE	110	176	276042400	145514800
2025-01-11T14:40:01.000Z, 3.966667, 33, 23, 4095, FALSE	110	176	215557200	85663900

Table 4 provides the channel encryption of the smart farm data using AES with the secret key factory generation of PBKDF2WithHmacSHA256 (CK1) and the cipher modes of AES/CBC/PKCS5Padding (CEM1).

Table 4. AES with secret key factor: CK1, cipher mode: CEM1.

Sensor Data	Size (byte)	Ciphertext size (byte)	Encryption time (ns)	Decryption time (ns)
2025-01-06T09:07:31.000Z, 3.738095, 32, 21, 4095, FALSE	110	176	128046300	888000
2025-01-11T14:19:58.000Z, 4.061905, 31, 29, 4095, FALSE	110	176	147544200	866800

2025-01-11T14:22:29.000Z, 4.028572, 31, 25, 4095, FALSE	110	176	140850900	981700
2025-01-11T14:24:59.000Z, 3.990476, 32, 24, 4095, FALSE	110	176	149026300	827800
2025-01-11T14:27:29.000Z, 3.966667, 32, 23, 4095, FALSE	110	176	168377500	913300
2025-01-11T14:30:00.000Z, 4.009524, 33, 23, 4095, FALSE	110	176	153084600	900800
2025-01-11T14:32:30.000Z, 3.961905, 33, 23, 4095, FALSE	110	176	138616000	1111400
2025-01-11T14:35:00.000Z, 4.028572, 33, 23, 4095, FALSE	110	176	152990500	935600
2025-01-11T14:37:30.000Z, 4.014286, 33, 23, 4095, FALSE	110	176	157082700	1065900
2025-01-11T14:40:01.000Z, 3.966667, 33, 23, 4095, FALSE	110	176	145002300	850700

Table 5 presents the channel encryption of the smart farm data using AES with the secret key factory generation of AES+SHA1 (CK2) and the cipher modes of AES/CBC/PKCS5Padding (CEM1).

Table 5. AES with secret key factor: CK2, cipher mode: CEM2.

Sensor data	Size (byte)	Ciphertext size (byte)	Encryption time (ns)	Decryption time (ns)
2025-01-06T09:07:31.000Z, 3.738095, 32, 21, 4095, FALSE	110	176	98971800	762500
2025-01-11T14:19:58.000Z, 4.061905, 31, 29, 4095, FALSE	110	176	124178700	832000
2025-01-11T14:22:29.000Z, 4.028572, 31, 25, 4095, FALSE	110	176	156182200	908100
2025-01-11T14:24:59.000Z, 3.990476, 32, 24, 4095, FALSE	110	176	125887100	899800
2025-01-11T14:27:29.000Z, 3.966667, 32, 23, 4095, FALSE	110	176	135784500	918300
2025-01-11T14:30:00.000Z, 4.009524, 33, 23, 4095, FALSE	110	176	132625400	1112200
2025-01-11T14:32:30.000Z, 3.961905, 33, 23, 4095, FALSE	110	176	136868900	846300
2025-01-11T14:35:00.000Z, 4.028572, 33, 23, 4095, FALSE	110	176	151963200	979600
2025-01-11T14:37:30.000Z, 4.014286, 33, 23, 4095, FALSE	110	176	131208700	840800
2025-01-11T14:40:01.000Z, 3.966667, 33, 23, 4095, FALSE	110	176	142246200	977500

The summary of the various channel encryption approaches for smart farming setup because of secret key factory, cipher mode, size, ciphertext, encryption time, decryption time and security status are presented in Table 6.

Table 6. The smart farm setup's channel exchange encryptions with various secret key factors.

Secret key factory	Cipher mode	Size (byte)	Ciphertext (byte)	Encryption time (ns)	Decryption time (ns)	Security status
IV SECRET KEY GENERATOR	AES/CBC/PKCS5Padding	110	176	321569810	123227400	High
IV SECRET KEY	AES/ECB/PKCS5Padding	N/A	N/A	N/A	N/A	N/A

GEENERATOR						
AES SECRET KEY GENERATOR	AES/CBC/PKCS5Padding	110	176	148062130	934200	Moderate
AES SECRET KEY GENERATOR	AES/ECB/PKCS5Padding	110	176	132630055.6	907710	Moderate

Fig. 5 displays the ciphertext with IV and AES keys generations comparisons revealed that, IV with ECB offered the least values as against the IV with CBC, which generated longer ciphertext than the plaintext. Also, the implications of the using AES key with CBC and ECB are the same, which is larger ciphertext than the plaintext. These implies larger noise in the corresponding ciphertext for the sensor data after encryption procedures.

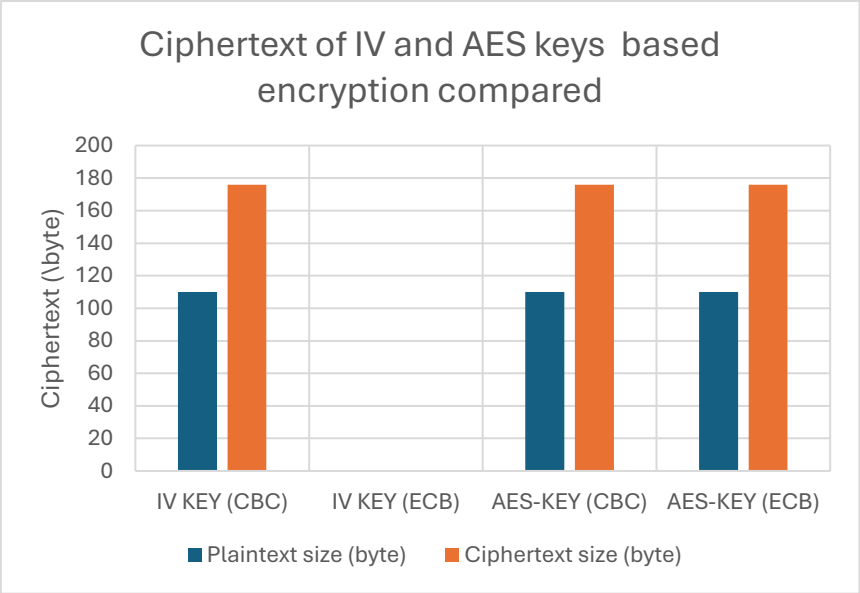
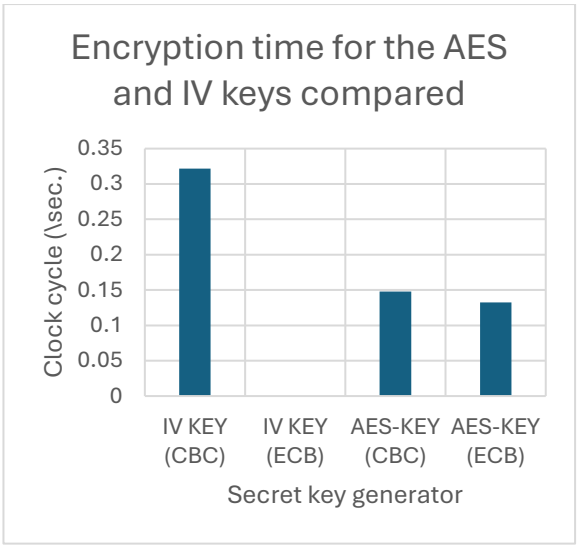
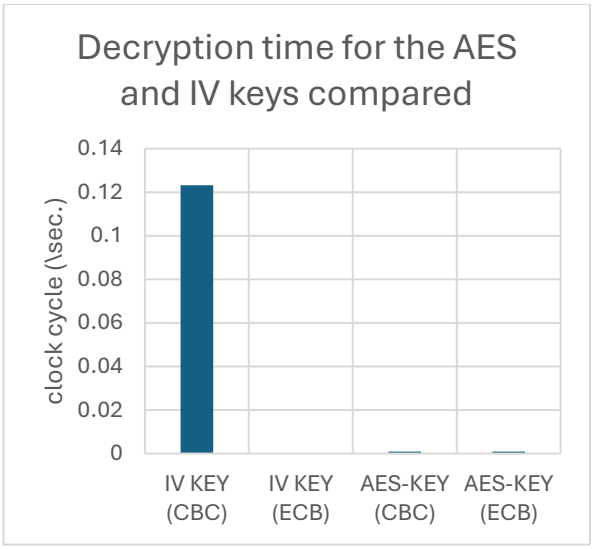


Fig. 5. The plaintexts and ciphertexts sizes with IV and AES keys-based encryption compared.

Fig. 6 considers the encryption time for the IV and AES keys generators, the IV-ECB was the fastest, followed by AES-ECB and AES-CBC respectively. While, the IV-CBC had the biggest encryption time indicating overheads of the scheme along the communication channels.



(a) The encryption time with IV and AES keys generation-based encryption compared.



(b) The decryption time with IV and AES keys generation-based encryption compared.

Fig. 6. The encryption and decryption time with IV and AES keys generation.

Fig. 6 focuses on the decryption time for the IV and AES keys generators, the IV-ECB was the quickest, tailed by the AES-ECB and AES-CBC accordingly. On the contrary, the IV-CBC was slowest in term of decryption procedure which increases overheads for the data communication along the channels.

Discussion of findings and outcomes

The findings of this study demonstrate that strong channel-level encryption can be practically deployed in smart farming systems without imposing excessive computational or communication overhead. Unlike many prior works that favour lightweight or simplified cryptographic schemes due to perceived device limitations [18] [11], the results show that AES-128 with CBC mode effectively eliminates ciphertext pattern leakage and significantly strengthens data confidentiality. This directly addresses the well-documented weaknesses of ECB mode, which remains vulnerable to traffic analysis and inference attacks [27] [14].

Although AES-128/CBC introduced approximately 60% ciphertext expansion and about a twofold increase in encryption time, the observed latency remains acceptable for periodic agricultural data transmission. This supports arguments by [14] and [25] that moderate cryptographic overhead is a reasonable trade-off for enhanced security in non–time-critical IoT applications. Therefore, prioritizing lightweight encryption at the expense of confidentiality, as adopted in several earlier studies [15] [18], appears unjustified for smart farming contexts where data integrity and privacy are critical.

From a computational perspective, the measured encryption and decryption times confirm that AES-based cryptography is feasible on resource-constrained platforms, aligning with findings reported by [21] and [24]. Despite the additional operations required by CBC mode, decryption latency remained consistently low, indicating that cloud-side analytics and real-time monitoring services are not adversely affected. This challenges assumptions in prior works that dismiss block ciphers as impractical without validating them through real-world deployment.

A key strength of this study lies in its evaluation using a real smart farm testbed rather than simulations or synthetic datasets. Many existing works rely on controlled laboratory environments [24] [22], which often underestimate practical deployment constraints. By validating performance using live farm data and operational wireless links, this study provides more realistic insights into cryptographic overhead and feasibility. Overall, the results strongly support AES-128/CBC as a balanced and deployable solution for secure smart farming communications, offering robust confidentiality and integrity with tolerable overhead.

Conclusions

The paper developed and experimentally validated a secure channel encryption model for IoT-enabled smart yam farming, addressing critical communication-layer vulnerabilities in agricultural sensor

networks using AES-128 with CBC mode. Performance evaluation shows that AES-128/CBC provides stronger confidentiality and resistance to data pattern leakage compared with ECB-based schemes. For an average plaintext size of 110 bytes, ciphertext expansion to 176 bytes resulted in approximately 60% communication overhead, while encryption latency increased by about 2× relative to ECB (average encryption time of 3.2×10^8 ns). Although CBC introduces additional computational cost, the latency remains acceptable for periodic smart farming data transmissions where security and integrity are prioritized over ultra-low delay.

This work lies in delivering a practically deployable, security-centric channel encryption framework validated on live farm data rather than simulations. Future research will explore hybrid and post-quantum encryption schemes to enhance long-term security resilience in smart agriculture systems.

References

1. Bui T-A *et al.* Edge-computing-enabled deep learning approach for low-light satellite image enhancement. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **17** (2024) 4071–4083.
2. Saadouni R *et al.* Securing smart agriculture networks using bio-inspired feature selection and transfer learning for effective image-based intrusion detection. *Internet of Things* **29** (2025) 101422.
3. Ryu M *et al.* Design and implementation of a connected farm for smart farming system. in *2015 IEEE Sensors* (2015) 1–4. doi:10.1109/ICSENS.2015.7370624.
4. Doshi J *et al*. Smart Farming using IoT, a solution for optimally monitoring farming conditions farming conditions. *Procedia Comput. Sci.* **160** (2019) 746–751.
5. Dineva K & Atanasova T. Cloud Data-Driven Intelligent Monitoring System for Interactive Smart Farming. *Sensors* **22** (2022) 6566.
6. Aldhyani T H H & Alkahtani H. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics* **11** (2023) 233.
7. Neethirajan S. Safeguarding digital livestock farming - a comprehensive cybersecurity roadmap for dairy and poultry industries. *Front. Big Data* **8** (2025) 1556157.
8. Mehmood S *et al.* Distributed Denial of Services (DDoS) attack detection in SDN using Optimizer-equipped CNN-MLP. *PLoS ONES* **20** (2025) e0312425.
9. Ileri K. A hybrid feature selection method for anomaly detection using shallow and deep ANN classifiers in smart farming. *J. Ambient Intell. Smart Environ.* (2025) 1–13. doi:10.1177/18761364251359885.
10. Ali M *et al.* Internet of Things DDoSViT: IoT DDoS attack detection for fortifying firmware Over-The-Air (OTA) updates using vision transformer. *Internet of Things* **30** (2025) 101527.
11. Riaz A R *et al.* Applying Adaptive Security Techniques for Risk Analysis of Internet of Things (IoT)-Based Smart Agriculture. *Sustainability* **14** (2022) 10964.
12. Alfa A A *et al.* Sooner Lightweight Cryptosystem: Towards Privacy Preservation of Resource-Constrained, *ICTA 2020* (Springer International Publishing) *CCIS* vol. **1350** (2021), 415–429.
13. Makhdoom I *et al.* Securing personally identifiable information: a survey of Sota techniques, and a way forward. *IEEE Access* **12** (2024) 116740–116770.
14. Has M *et al.* Efficient Data Management in Agricultural IoT: Compression, Security, and MQTT Protocol Analysis. *Sensors* **24** (2024) 3517.
15. Fathy C & Ali H M. A Secure IoT-Based Irrigation System for Precision Agriculture Using the Expeditious Cipher. *Sensors* **23** (2023) 2091.
16. Rahul R *et al.* Smart farming with improved security using ascon encryption and authentication, *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* 2024, 365–373.
17. Afzal S & Bokhari M U. LightAgriCrypt: A Novel Lightweight Stream Cipher for Enhancing Security in Smart Agriculture Systems. *Secur. Priv.* **8** (2025) e70024.
18. Wahid A *et al.* Secure Wireless Sensor Network using Cryptography for Smart Farming Systems. *IOTA* **02** (2022) 248–262.
19. Abduljabbar Z A *et al.* Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. *Sustainability* **15** (2023) 10264.

20. Kadhim T A *et al.* Lightweight Scheme for Secure Signaling and Data Exchanges in Intelligent Precision Agriculture. *Cryptography* **9** (2025) 7.
21. Itoo S & Khan A A L I. A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System. *IEEE Access* **11** (2023) 56875–56890.
22. Taji K & Ghanimi F. Enhancing security and privacy in smart agriculture: A novel homomorphic signcryption system. *Results Eng.* **22** (2024) 102310.
23. Mohammed M Y. Enhancing Energy Efficiency in IoT Wireless Sensor Networks: AI-Driven Clustering and Routing Protocols. *J. Al-Qadisiyah Comput. Sci. Math.* **17** (2025) 12–26.
24. Nagaraja G S *et al.* Novel Framework for Secure Data Aggregation in Precision Agriculture with Extensive Energy Efficiency. *J. Comput. Networks Commun.* **2023** (2023) 1–11.
25. Thiruvenkatasamy K V *et al.* An online tool based on the Internet of Things and intelligent blockchain technology for data privacy and security in rural and agricultural development. *Sci. Reports* **15** (2025) 1–12.
26. Alqarni K S *et al.* Authenticated Wireless Links between a Drone and Sensors Using a Blockchain: Case of Smart Farming. *Wirel. Commun. Mob. Comput.* **2022** (2022) 1–13.
27. Wu H-T & Tsai C-W. An Intelligent Agriculture Network Security System Based on Private Blockchains. *J. Commun. Networks* **21** (2019) 503–508.
28. Rahaman M *et al.* Privacy-Centric AI and IoT Solutions for Smart Rural Farm Monitoring and Control. *Sensors* **24** (2024) 4157.
29. Makhdoom I *et al.* PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities. *Comput. Secur.* **88** (2020) 101653.
30. Yang H. Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card. *Secur. Commun. Networks* **2022** (2022) 1–11.